ANKARA YILDIRIM BEYAZIT UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES



IDENTIFYING CRITICAL CYBERSECURITY CONTROLS AT COUNTRY LEVEL

M.Sc. Thesis by

Burak Aydın

Department of Defence Technologies

March, 2019

ANKARA

IDENTIFYING CRITICAL CYBERSECURITY CONTROLS AT COUNTRY LEVEL

A Thesis Submitted to

The Graduate School of Natural and Applied Sciences of

Ankara Yıldırım Beyazıt University

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Defence Technologies, Department of Defence Technologies

by

Burak Aydın

March, 2019

ANKARA

M.Sc. THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"IDENTIFYING CRITICAL CYBERSECURITY CONTROLS AT COUNTRY LEVEL"** completed by **BURAK AYDIN** under the supervision of **PROF. HÜSEYİN CANBOLAT** and ASST.PROF. MEHMET ALİ ÇİNİCİ, and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Hüseyin CANBOLAT
Supervisor

Asst.Prof. Mehmet Ali ÇİNİCİ
Jury Member (Second Advisor)

Assoc.Prof. Baha ŞEN
Jury Member

Assoc.Prof. Enver ÇAVUŞ
Jury Member

Assoc.Prof. Bünyamin CİYLAN
Jury Member

Prof. Ergün ERASLAN
Director
Graduate School of Natural and Applied Sciences

ETHICAL DECLARATION

I hereby declare that, in this thesis which has been prepared in accordance with the Thesis Writing Manual of Graduate School of Natural and Applied Sciences,

- All data, information and documents are obtained in the framework of academic and ethical rules,
- All information, documents and assessments are presented in accordance with scientific ethics and morals,
- All the materials that have been utilized are fully cited and referenced,
- No change has been made on the utilized materials,
- All the works presented are original,

and in any contrary case of above statements, I accept to renounce all my legal rights.

Date: 01/03/2019 **Signature:**

Name & Surname: Burak AYDIN

ACKNOWLEDGEMENTS

Firstly, I would like to express my sincere gratitude to my first advisor, Prof. Hüseyin CANBOLAT for his guidance during my administrative issues and I also would like to appreciate my second advisor, Asst.Prof. Mehmet Ali ÇİNİCİ for his tremendous support and motivation during my study. His immense knowledge in cybersecurity and precious recommendations constituted the milestones of this study. His guidance assisted me all the time of my research and while writing this thesis. Last but not least, I would like to thank my wife, Ayşe Gül AYDIN for her patience during the writing phase of my thesis.

2019, 01 March **Burak AYDIN**

IDENTIFYING CRITICAL CYBERSECURITY CONTROLS AT COUNTRY LEVEL

ABSTRACT

All the states around the world are trying to take measures against the new actors that threaten their very existence such as terrorism, global financial crisis, and climate change. Cybersecurity is one of these actors that states try to take measures against. Whether the reason is limitations that they encounter or disagreements originated from the international environment, a new unconventional challenge has been already posing a threat to the global order.

Cybersecurity starts from the outside of state borders since cyber attacks can be committed against a particular state at any time and at any part of the world due to the nature of the Internet. In order to ensure cybersecurity, states should take some critical measures in the first place as the first line of defence.

The main objective of this study is to show how states can identify and manage their strategic cybersecurity controls without grappling with the Internet's architecture and undermining the very benefits of cyberspace.

Keywords: Cybersecurity, strategic controls, nation-level cybersecurity controls, cybersecurity strategy, cybersecurity controls

ÜLKE DÜZEYİNDE KRİTİK SİBER GÜVENLİK TEDBİRLERİNİN BELİRLENMESİ

ÖZ

Dünyadaki tüm devletler terörizm, küresel mali kriz, iklim değişikliği gibi varlıklarını tehdit eden yeni aktörlere karşı tedbir almaya çalışıyorlar. Siber güvenlik de devletlerin tedbir almaya çalıştıkları bu aktörlerden birisidir. Sebep ister karşılaştıkları kısıtlar isterse de uluslararası ortamdan doğan uyuşmazlıklar olsun, alışılmadık yeni bir aktör küresel düzeni çoktandır tehdit etmektedir.

Siber güvenlik devletlerin sınırları dışında başlar. Çünkü internetin doğası gereği siber saldırılar herhangi bir zamanda ve dünyanın herhangi bir yerinde bir devlete karşı icra edilebilir. Siber güvenliğini sağlamak için de devletler, bazı kritik tedbirleri ilk hat savunması olarak en başta almak zorundalardır.

Bu çalışmanın ana hedefi; devletlerin, siber alemin sunduğu faydalara gem vurmadan ve Internetin mimarisiyle boğuşmadan, stratejik siber güvenlik tedbirlerini nasıl belirleyeceği ve nasıl yöneteceğini göstermektir.

Anahtar Kelimeler: Siber güvenlik, stratejik tedbirler, ülke seviyesinde siber güvenlik tedbirleri, siber güvenlik stratejisi, siber güvenlik tedbirleri

CONTENTS

M.Sc.THESIS EXAMINATION RESULT FORM ii
ETHICAL DECLARATION iii
ACKNOWLEDGMENTS I
ABSTRACT..... II
ÖZ III
NOMENCLATURE VI
LIST OF TABLES VIII
LIST OF FIGURES IX

CHAPTER 1 - INTRODUCTION 1
1.1 Literature Summary 2
1.2 Aim Of The Thesis 3
1.3 Hypothesis 4

CHAPTER 2 - CYBER THREATS THAT THE COUNTRIES ENCOUNTER 5
2.1 Cybercrime 5
2.2 Cyberwarfare 6
2.3 Cyber Terrorism 7

CHAPTER 3 - SOME CYBER ATTACKS CONDUCTED AT COUNTRY LEVEL 8

CHAPTER 4 - IDENTIFYING CRITICAL CYBERSECURITY CONTROLS AT COUNTRY LEVEL 10
4.1 Establishing and Empowering a Parent Organization Liable for Nationwide Cybersecurity 10
4.2 Adopting a National Cybersecurity Strategy 13
4.3 Shaping Legal and Regulatory Framework 18
4.4 Following a Risk Management Approach 19
4.5 Partnering with Industry and Academia 22
4.6 Forming an Information Sharing Mechanism 24
4.7 Adopting Cybersecurity Standards Recognized by Industry 25

4.8 Raising Public Awareness 28
4.9 Promoting International Cooperation and Conducting Cybersecurity Exercises 29
4.10 Building Capacity and Capability with Education and R&D 30
4.11 Laying Out National Cybersecurity Contingency Plans 32
4.12 Fostering Cyber Insurance in Businesses 33
4.13 The Assessment of Turkey According to 12 Controls 35

CHAPTER 5 – THE FUTURE OF CYBERSECURITY 38

CHAPTER 6 – CONCLUSION 40

REFERENCES 42

CURRICULUM VITAE 45

NOMENCLATURE

Abbreviations

APT	Advanced Persistent Threat
CGSD	Cyber and Government Security Directorate
CEN	European Committee for Standardization
CERT	Computer Emergency Response Team
CSIRT	Cybersecurity Incident Response Team
CSP	Cyber Security Platform
DHS	Department of Homeland Security
DoD	Department of Defence
DoS	Denial of Service
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Network and Information Security
EU	European Union
EUROPOL	European Police Office
FIS	Federal Intelligence Service
GCI	Global Cybersecurity Index
IC	Intelligence Community
ICAO	International Civil Aviation Organization
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
INTERPOL	International Criminal Police Organization
IP	Internet Protocol
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
ITU	International Telecommunication Union
MELANI	Swiss Reporting and Analysis Centre for Information Assurance
MITM	Man-in-the-middle
MoD	Ministry of Defence
NCCIC	National Cybersecurity and Communications Integration Center
NCIRC	National Cybersecurity Incident Response Center
NCSS	National Cybersecurity Strategy

NIPS	Network Intrusion Prevention Systems
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OSCE	Organization of Security and Cooperation in Europe
TCP/IP	Transmission Control Protocol/Internet Protocol
UNODC	United Nations Office on Drugs and Crime
UK	United Kingdom

LIST OF TABLES

Table 4.1 Comparison of ten national cybersecurity strategies …...……... 17

Table 6.1 Issues that needed to be addressed in Turkey ..…….……..… 36

LIST OF FIGURES

Figure 1.1 Focus down research model ……..……..…. 2

Figure 4.1 Countries with established or developing a national cybersecurity agency ……13

Figure 4.2 NCSS lifecycle of ENISA …….. 16

Figure 4.3 121 of 194 ITU member states have a national cybersecurity strategy . 16

Figure 4.4 Six Steps of the Risk Management Framework of NIST ……...… 20

Figure 4.5 Contents of ISO/IEC 27002:2013 …….. 28

CHAPTER 1

INTRODUCTION

The Internet or more broadly cyberspace was not originally designed to maximize security. It was designed as a small network in order to ensure permanent connectivity. Yet, with the inclusion of e-mail and radio and satellite communications, it gave rise to ARPANET. And with the use of Transmission Control Protocol / Internet Protocol (TCP/IP) in ARPANET, the real birth of the Internet took place. In fact, TCP/IP structure used to foster networks to link with one another increasingly. The most significant one of these networks was the National Science Foundation's NSFNet whose availability to every researcher on every U.S. campus laid the foundation for the Internet's worldwide growth [1]. For this reason, it can be said that the Internet - network of the networks - was designed to allow scientists and researchers to exchange data with one another quickly rather than to maximize security. But over the course of the time, it has become increasingly accessible to everybody, the number of users and connected devices have continued to increase exponentially and with new technological supplies and services such as cloud computing, artificial intelligence, advanced robotics, internet of things and machine-to-machine communication, the number of attacks along with their constant evolution and their complexity have grown each day.

In line with the growth of attacks, the anonymity of the attackers operating from fake Internet Protocol (IP) addresses and geographically distributed servers has increased. The main reason for this is that it is very difficult to track the origin of attacks in borderless cyberspace. Defenders must always be on guard and defend all possible attacks which require high-cost solutions and investments.

Besides, cyber domain - *the fifth domain after land, sea, air and space* [2] - has transformed the traditional and symmetrical power center into asymmetric one, providing even non-state actors with an opportunity to have effective actions in times of crisis in which expertise and knowledge matter rather than size and mass. Thus some great powers around the world equate cyber attacks with military intervention.

In such an uncertain and mutable cyber domain, cyber attacks can seriously and irreversibly disrupt, paralyze or destruct states' critical infrastructures and society's vital functions. In order to be prepared for the bad, states should take some critical measures against the hazardous behaviors of this crucial domain. They have to put cybersecurity at the heart of policy and technology, and they have to secure their state infrastructures for public health, citizen welfare, economic growth and all in all for their survival.

1.1 Literature Summary

Most of the countries around the world have a National Cybersecurity Strategy (NCSS) and they continuously improve and update their strategies after expiration period of the strategy. Though these strategies have some common topics and controls, they are largely sophisticated and different from each other both in form and in content.

The difference in strategies leads to "Global Cybersecurity Index (GCI)" which measures the commitment of countries to cybersecurity. Inside this Index, there are pillars and sub-pillars that are used as indicators. These pillars are very crucial in terms of strategic controls and gave birth to the selection of the research title. Via "Focus down model" [3], a broad literature review (See Figure 1.1) was implemented in order to discover what controls the countries have and should have.

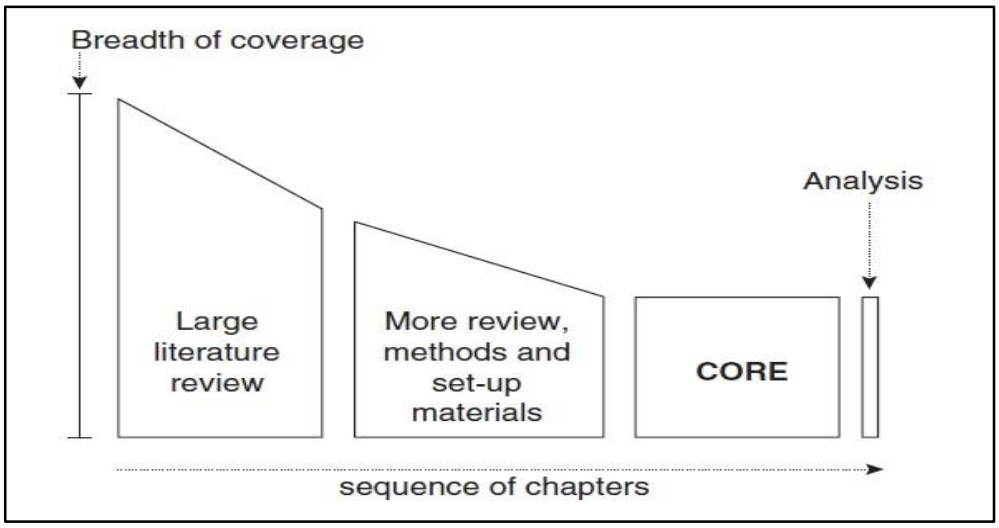

Figure 1.1 Focus down research model

With this broad literature review, 54 data collection tools were used as the basis of the research including 7 books, 17 periodicals, 1 thesis and 29 official publications.

During literature review, it is also realized that there are lots of studies with regard to cybersecurity both in national and international literature. But most of them consist of enterprise level or organization level controls rather than a strategic point of view. And these enterprise-level controls most of the time include technical controls against well-known cyber attacks such as malware, phishing, denial of service (DoS) and man-in-the-middle (MITM) attacks. The studies about strategic controls are very scarce and they usually belong to regional or international bodies like the European Union Agency for Network and Information Security (ENISA). Therefore, after the broad literature review, the related resources were put aside and the others were looked over superficially and of those, needless ones were discarded.

Finally, narrowed down resources were ready to benefit. Yet, these resources just put forward the controls that a nation should have at large. They mostly do not go into detail or they do not include real practices. Hence, the nation-level controls were first specified and once again, each listed control were elaborated with an exhaustive literature review.

1.2 Aim of the Thesis

The aim of this research is to put forward some nation-level cybersecurity controls, unlike regional or international bodies. And its scope does not depend on technical controls but strategic controls.

The research consists of six chapters in which the first chapter covers the introduction and the last chapter covers the conclusion. Apart from these chapters:

The second chapter covers the cyber threats at large that a nation might encounter. Going into details of a specific cyber threat like Advanced Persistent Threat (APT) does not make sense here as the level of the research is strategic. The aim of including this chapter is to inform readers about current cyber threats in general terms.

The third chapter covers some far-reaching cyber attacks that the countries have already encountered. The aim for including this chapter is to draw readers' attention about big scale cyber attacks. During daily routine lives, people take individual cyber attacks for granted, but what if these cyber attacks affect the whole nation or its policy?

The fourth chapter covers twelve strategic cybersecurity controls that a nation can adopt for making their citizens live in a more cyber-secure environment. These controls are supported by good examples around the world. In fact, this part is the essence of the research.

The fifth chapter covers the future of cybersecurity. The aim of putting this chapter is to show future trends in cybersecurity and to make readers think about their cyber future.

1.3 Hypothesis

The power of a state in cyberspace is territorially linked, which means it is most effective where it can control up to the physical side of the Internet. In a cyber incident, it exerts its power by seizing physical and financial assets, closing the offices, imprisoning the culprits at most. If the incident is multinational, the power of the state will probably fall short.

For eliminating or at least for reducing the restraints of the power of the state and for having a better cyber secure posture, states can adopt some organizational, legal, educational and other types of measures at nation-level.

CHAPTER 2

CYBER THREATS THAT THE COUNTRIES ENCOUNTER

Before identifying nation-level cybersecurity controls, the threats that the countries encounter today should be clarified. According to most of the scientific writings and documents in the literature about the classification of cyber attacks, cyber attacks can be broken down into three main categories. These are cybercrime, cyber warfare, and cyber terrorism.

2.1 Cybercrime

As long as there are people, there are crimes. In other words, the history of crime originates from the very existence of humankind. In ancient times, crimes were committed against one another. With the introduction of laws and punishments, the ways crimes are committed have changed which finds its place in cyberspace today.

There is no agreed international definition of cybercrime nor of cyber attacks, However, when European Commission's definition is taken, it can be said as "Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems" [4]. And when United Nations Office on Drugs and Crime (UNODC) definition is taken, it can be said as "Cybercrime can be described as having cyber-dependent offences, cyber-enabled offences and, as a specific crime-type, online child sexual exploitation, and abuse" [5]. So presumably, the best way for defining cybercrime is merging these two institution's explanations and putting cybercrimes into three categories:

- Cyber-Dependent Crimes: Crimes that require an Information and Communication Technology (ICT) infrastructure to be committed and they are often addressed as the deployment of cyber attacks on vital infrastructures or transforming a website from online to offline by overloading it with data with the intention of disrupting that website such as via a DOS attack.

- Cyber-Enabled Crimes: These types of crimes are generally traditional crimes that occur in the real world, but they are facilitated by ICT. Common examples are online frauds and forgery, money laundering online and purchases of drugs online.

- Having illegal online content: Housing illegal contents such as material related to terrorism, racism, child sexual abuse, violence, and xenophobia.

2.2 Cyberwarfare

Wars are fought with the weapons determined by prevalent technology of the age. The prevalent technology of the twenty first century is computers. Therefore, the wars during this century would be cyberwars. The characteristic of cyberwarfare is disruptive rather than destructive when compared with the traditional mass destructive wars. But its consequences would be no less serious than the traditional ones.

The definition cyberwarfare refers to actions taken by a nation state to damage and to disrupt another nation's computer and network systems. According to one general definition, "*cyberwarfare refers to a massively coordinated digital assault on a government by another, or by large groups of citizens. The term cyber warfare may also be used to describe attacks between corporations, from terrorist organizations, or simply attacks by individuals called hackers, who are perceived as being warlike in their intent*" [6].

Cyberwarfare and cybercrime are sometimes difficult to differentiate. The factors that distinguish cyberwarfare from cybercrime are generally the actors involved and the level of intensity and sophistication of the strategy of the attack.

Cyberwarfare involves the following attack methods:

- Cyber Espionage: Cyber espionage can be seen as an extension of traditional espionage. It is mostly used to steal required information from rival organizations or individuals for political, military or financial gain. Some prominent examples of cyber espionage include: Operation Buckshot Yankee (2008); Operation Night Dragon (2008-2011); Operation Aurora (2009); penetration of Lockheed Martin, BAE

Systems and Northrop Grumman (2009); Operation Shady RAT (2006); GhostNet (2009); the RSA Breach (2011) [7].

- Cyber Sabotage: It can be viewed as an extension of traditional sabotage as well. Yet, the difference is the field. The field that the cyber sabotage takes place is the cyberspace. Via cyber sabotage, military and financial computer systems can be disrupted from normal operations and equipment.

It is believed that the world's largest militaries are building cyber warfare programs. As of 2012, at least 11 nations have offensive cyber warfare capabilities. Among them, the United States, China, and Russia have publicly announced the existence of cyberwarfare units within their militaries [8].

2.3 Cyber Terrorism

Cyber terrorism can be called as the convergence of cyberspace and terrorism. And since cyberspace has emerged as the new battlefield after sea, land, air, and space, terrorists have started to use this domain as their lair.

Cyber terrorism can be viewed as unlawful attacks against computers, networks and the data stored therein to inflict terror and panic. It is qualified as cyber terrorism when the attacks result in violence or fear against people or their property. Attacks via cyberspace that lead to injury or death such as explosions or collisions would be examples.

The first known cyber terrorism against a country's computer systems can be viewed as the ethnic Tamil guerrillas who attempted to disrupt Sri Lankan embassies by sending large volumes of e-mail in 1998. The embassies received 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications" [9].

CHAPTER 3

SOME CYBER ATTACKS CONDUCTED AT COUNTRY LEVEL

Past cyber attacks against Estonia, Georgia, Iran and Ukraine serve as valuable examples in order to achieve state goals or gain an advantage in military operations. Among these:

Computer networks in the tiny Baltic country of Estonia were disabled in April and May 2007. Hackers kicked off a wave of cyber attacks that caused serious damage to dozens of government and corporate sites in Estonia. The authorities traced the so-called denial of service attacks and suggested that they had been orchestrated by Russia - a charge Russia denied -. Experts said they were coordinated attacks that were conducted by hundreds of thousands of computers against government agencies and banks. The attacks had great influences and consequences in Estonia. It was the first publicly well-known example of a nation-level cyber campaign. This case forced Estonia and NATO to reconsider the potential impact of cyber threats and the vulnerabilities of the cyber domain in general which resulted in the establishment of the NATO Cooperative Cyber Defense Center of Excellence in Tallinn in 2008 [10].

Another example is the 2008 Russia-Georgia war. The newly elected president Micheil Saakashvili tried to integrate with the West and recover the breakaway Georgian provinces – South Ossetia and Abkhazia – His attempts brought about a severe reaction from Moscow which led to the war in 2008. It was the first war which took place on the ground, on the sea, in the air and as well as in cyberspace. The first Distributed Denial of Service (DDoS) attacks against the Georgian websites took place before the outbreak of war. The similar scenario with a bigger scale coincided with the Russian troops entering South Ossetia. The attacks focused mainly on media and government websites as well as financial and educational institutions and businesses. Besides the DDoS attacks, there were also web defacement operations and massive spamming on public emails. The majority of the Georgian governmental websites were not

functional and could not communicate with the world on the Internet. Instead of normal content on the Georgian President website, there were images depicted Saakashvili as Hitler [11].

Yet another example is the deployment of Stuxnet – the malware designed specifically to target industrial control systems – The Stuxnet worm was discovered in an Iranian computer in 2010. It was later found that the malware was not designed to spy, but rather to sabotage centrifuges especially in the uranium enrichment facilities of Natanz that was involved in Iran's nuclear program. The high level of sophistication, complex architecture and all-around research effort needed to develop it caused it to be believed that the USA built Stuxnet with the support of Israel with the intention of stopping or delaying the Iranian nuclear program. The worm was probably implanted in the Natanz power plant's network by using a compromised USB drive. This technique enabled the worm to penetrate a network that is normally isolated from other networks [12].

CHAPTER 4

IDENTIFYING CRITICAL CYBERSECURITY CONTROLS AT COUNTRY LEVEL

The digital environment has the potential for states to improve public service delivery, to accelerate economic growth and social progress, to facilitate international trade and to ensure good governance. As a result, the increasing reliance on it has increased attention on cybersecurity. For instance, when governments deploy their services online - *like* e-*Government Applications* - cybersecurity incidents might occur, potentially resulting in reputational damage and disruption of services. Therefore, it can be said that while society's growing information hunger makes it vulnerable to the malicious actions on the one hand, it also compels the government authorities to fortify their cyber defense by taking some critical measures on the other hand.

Countries cannot disregard the opportunities associated with becoming connected to the Internet world. However, they have to balance the security risks regarding the proliferation of ICT-enabled infrastructure, devices and Internet applications with comprehensive national cybersecurity strategies and plans. Otherwise, they can not achieve the national security goals they are seeking.

In most cases, governments have some policy instruments at their disposal including legislation, regulation, standardization, mechanisms such as information sharing and education programmes. But, achieving a total cyber secure environment at the country level is an impossible task. In this context, cybersecurity risks cannot be entirely eliminated but they can be minimized by implementing below 12 control mechanisms:

4.1 Establishing and Empowering a Parent Organization Liable for Nationwide Cybersecurity

The first duty of a state government is to keep the nation and its people safe especially while delivering its public services to citizens. New technologies and methods for

delivering public services have unquestionably brought incredible gains for states in terms of efficiency and effectiveness. But they also have brought new vulnerabilities.

Cyber attacks are now a daily reality. State governments cannot be passive in the face of this threat. Actually, they should be proactive, rigorous, collaborative and comprehensive in their approach. In order to achieve this, they should build cybersecurity policies and take critical security decisions when they see fit. The best way for this is to establish and empower a parent and competent organization that is responsible for countrywide cybersecurity.

Whether it is called National Cybersecurity Agency or not, this parent organization should have unique authority to deal with cybersecurity directly and ensure coordination between public and private sector organizations, established regulatory authorities, national legislatures, and international partners. It is also important that the responsibilities of the parent organization should be distinct from those of other private and governmental bodies taking part in cybersecurity. This parent organization can have some internal branches responsible for planning, operations, policy developing, etc.

All in all this parent organization should:

- Prepare, direct, coordinate, monitor and evaluate the outcomes of the implementation of cybersecurity strategy (cybersecurity strategy will be explained in the next part). That is to say, it should act as the main coordinator and management body to define, specify and clarify tasks, responsibilities and decision rights to ensure the implementation of the strategy effectively.

- Report the overview of the activities, weaknesses, difficulties, proposals for improving the strategy and the cost of the application to the head of the government. With the financial, material and human resources allocated, the organization should establish a flexible system in which the benefits of centralization (a central cybersecurity authority with wide decision rights across sectors) and decentralization (the principle of subsidiarity) can be mapped and use the resources accordingly.

- Be responsible for compiling and distributing the cybersecurity situation picture - an overall cybersecurity situation assessment - and improving the cybersecurity expertise. It should operate on a 24/7 basis and oversee each administrative branch or cybersecurity incident response teams (CSIRTs) prepare its cyber risk analysis.

- Take on the main national CSIRT. This team plays a key role in coordinating incident management at the nation level. It should cooperate with other relevant national and international CSIRTs in order to report security incidents and warn related stakeholders via an early warning system. It should also behave as the main cyber offensive entity supporting military operations and/or supporting cyber espionage or cyber warfare when authorized.

When world nations are examined, most of the nations have a governmental parent organization that is responsible for nationwide cybersecurity (See Figure 4.1). United Kingdom (UK) can be given as an example. The Cyber and Government Security Directorate (CGSD) is responsible for physical, personal and information security policy across government and internationally. It works with other lead government departments and agencies like Ministry of Defence (MoD). Mainly, it delivers cybersecurity strategy and manages five-year cybersecurity programme [13]. Another example is "The National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security (DHS)" in the US. It was authorized by the Cybersecurity Act of 2015 in order to establish a mechanism for cybersecurity information sharing among the private sector and federal government entities [14]. It was further centralized by "2018 National Cyber Strategy of The United States of America". According to the strategy, DHS is to secure federal department and agency networks, with the exception of national security systems such as the Department of Defense (DoD) and Intelligence Community (IC) systems. This includes ensuring DHS has appropriate access to agency information systems for cybersecurity purposes and can take direct action to safeguard systems from the spectrum of risks [15].

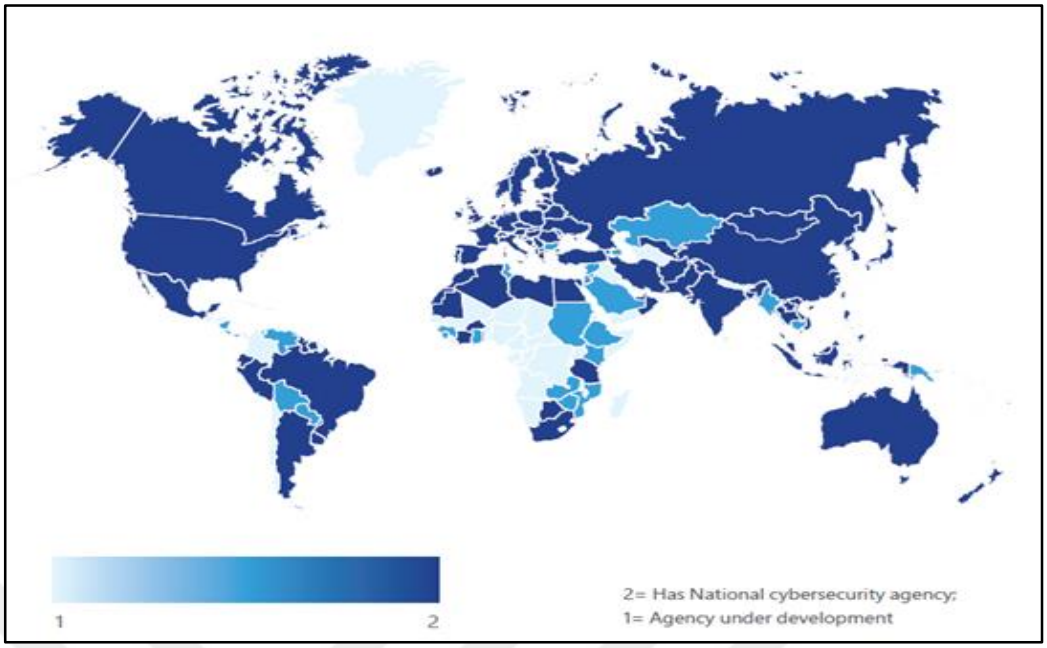

Figure 4.1 Countries with established or developing a national cybersecurity agency [16].

4.2 Adopting a National Cybersecurity Strategy

Cybersecurity includes multiple different legal, technical, operational and governance aspects. A national cybersecurity strategy should address, organize and prioritize many of these areas by providing an overview of the main components in order for a country to become cyber-prepared. By implementing a national cybersecurity strategy, a nation can improve its digital security and manage cybersecurity risks at nation-level.

A strategy can be defined as "*a plan of actions designed to achieve a long term or overall aim*" [17]. A national strategy for cybersecurity is needed in order to set a top-down and clear direction to form and improve cybersecurity for the government itself, its organizations and citizens. On the other hand, national cybersecurity plans accelerate growth and development by stimulating domestic sectors or by excluding foreign companies that are to be a national security concern in the future.

However, cybersecurity strategies can be different and assume many forms and length varying from nine pages to ninety pages with various levels of detail, depending on the particular country's goals. Therefore, there is not a commonly agreed and established definition of what forms a national cybersecurity strategy. Primarily, a national cybersecurity strategy constitutes as:

- The vision, scope, key principles and objectives, and priorities that guide a country in addressing cybersecurity,

- The current phase which indicates the state's own capabilities and shortcomings and the identification and clarification of vulnerabilities in critical infrastructures,

- The steps, programs and initiatives that a country undertakes to protect its vital functions and cyber-incident response capabilities to increase its preparedness,

- Respective roles and responsibilities of stakeholders and key entities in each sector tasked with addressing and implementing cybersecurity.

Setting out the vision, scope, key principles and objectives enables governments to address cybersecurity holistically across their national digital environment, instead of across a particular sector like finance with an atomistic approach. In other words, it allows them to be strategic. Priorities might vary, for instance, while one country might focus on addressing critical infrastructure-related risks, the others might focus on safeguarding intellectual property or improving cybersecurity general awareness of the public. In this perspective, the strategy should clearly state the key principles and the objectives the government has in mind for cybersecurity.

Indicating current capabilities and shortcomings enables governments to focus on specific areas, to allocate sufficient resources accordingly and to identify how these resources should be used. New investments might be created as well.

Putting steps, programs and initiatives in place helps governments to achieve its objectives and desired outcomes within set budget and timelines. Establishing cyber incident response capabilities also increases a country's ability to respond quickly and recover from cyber attacks swiftly.

Involving stakeholders, key entities and public advice - by means of asking related individuals and groups for inputs and views - in national cybersecurity strategy provides governments to beef up the risk management efforts in every aspect. Therefore, the strategy should be developed and implemented with the active

participation of all related stakeholders and it should be a public document to increase inclusiveness.

The national cybersecurity strategy should have the formal support of the highest level of authority in order to show how significant the country places importance in cybersecurity. Furthermore, it should focus on how to ensure vital services uninterruptedly, fighting cybercrime more effectively and improving national defense capabilities appropriately. National exhaustive monitoring, analysis and reporting system for cybersecurity should be adopted. Digital continuity of the state should be sustained by mirror and backup alternatives in virtual embassies [18].

In a nutshell, the strategy should help build a digital secure environment inside the state in which the society and businesses can completely rely on, their interests and rights are protected and the data security is always assured.

When the situation in EU is examined, 2016 adopted Network and Information Systems (NIS) Directive require EU Member States to develop and adopt a National Cybersecurity Strategy (NCSS). Parallel to this directive, ENISA prepared a guide for NCSS. According to this guide and in order for states to improve the national cybersecurity strategies continuously as well as its implementation through actions, measures, and processes, ENISA recommends a lifecycle approach (See Figure 4.2).

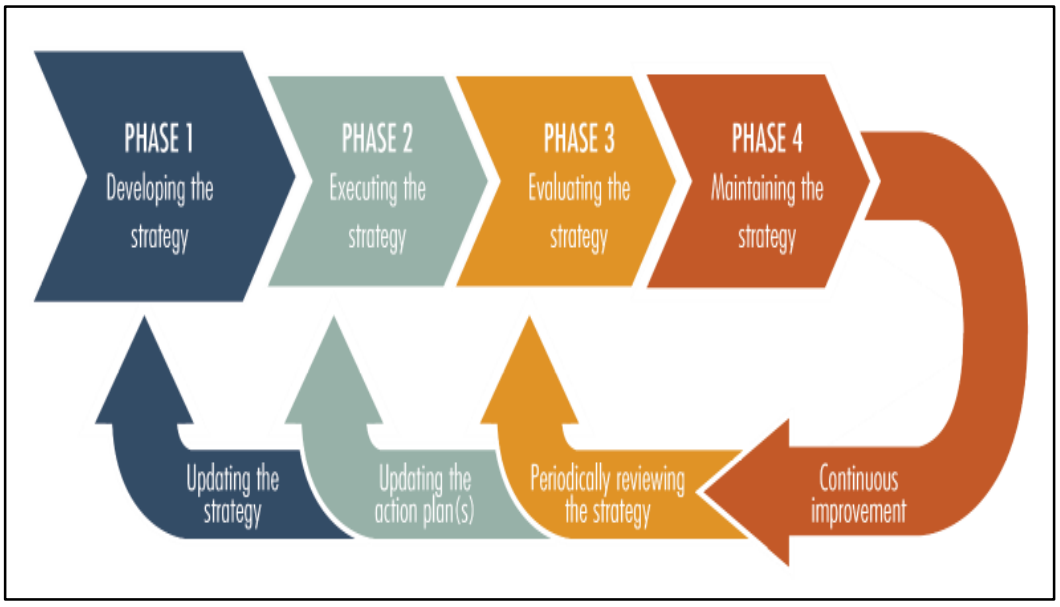

Figure 4.2 NCSS lifecycle of ENISA [19]

According to a "2017 Global Cybersecurity Index" paper published by The International Telecommunication Union (ITU), only 38% countries have a published cybersecurity strategy and only 11% have a dedicated standalone strategy; another 12% have a cybersecurity strategy under development [20]. Also, see Figure 4.3 for countries that have a cybersecurity strategy.

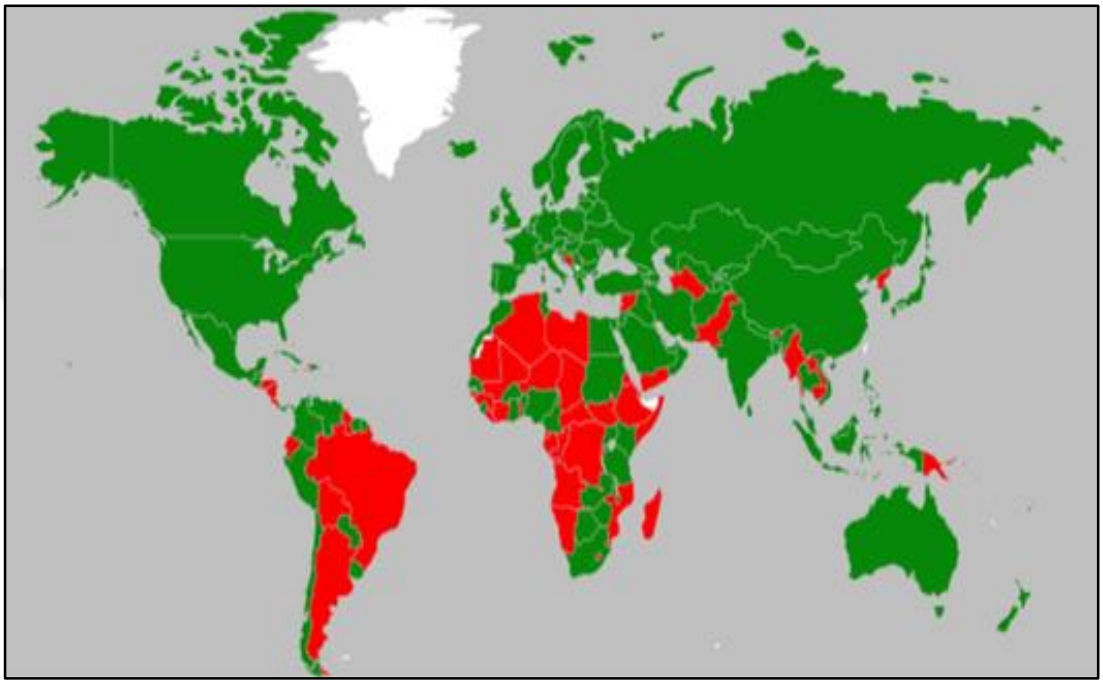

Figure 4.3 121 of 194 ITU member states have a national cybersecurity strategy [21].

When a comparison of national cybersecurity strategies is made among ten countries including Australia, France, Japan, Canada, New Zealand, Czech Republic, Germany, The Netherlands, The United Kingdom and The United States, it can be clearly noticed that no harmonization between the countries is existing. See Table 4.1 for the comparison of national cybersecurity strategies.

Table 4.1 Comparison of Ten National Cybersecurity Strategies [22].

Comparison of National Cybersecurity Strategies ●= explicitly described, ○= implicitly referenced											
		Australia	Canada	Czech Republic	France	Germany	Japan	The Netherlands	New Zealand	United Kingdom	United States
Language		English	English / French	Czech / English	French	German / English	Japanese / English	Dutch / English	English	English	English
Issued		2009	2010	2011	2011	2011	2009	2011	2011	2009	2003
Definition of Cybersecurity		definition	descriptive	no definition	definition	definition	no definition	definition	definition	descriptive	implicit
Addresses cyber threats to:	Critical Infrastructure	●	●	●	●	●	○	●	●	●	○
	Defence Abilities	●	●		○			○			
	Economic Prosperity	●	●	●		●	●	●	●	●	●
	National Security	●	●	●	●	○	●	○	●	●	●
	Public Confidence in ICT							●	○		
	Social Life of Citizens	●	●	○			●	●		●	
Addresses cyber threats from:	Activism							●	●		
	Criminals/Organised Crime	●	●	●	●	●	○	●	●	●	○
	Espionage	●	●		●	●	○	●	●	●	●
	Cyberwarfare		●	●	●	●	●	●	○	●	●
	Terrorists	●	●	●	●	●		●	●	●	●
	Large Scale Attacks		○			●	●				○

For preparing, drafting, developing, managing, implementing and reviewing a national cybersecurity strategy, *"Guide to Developing a National Cybersecurity"* guide which co-published by twelve renowned international organizations can be utilized [23]. This guide is also utilized in this study.

4.3 Shaping Legal and Regulatory Framework

Governments struggle to respond to the sophisticated threats and the prevalence of cybercrimes due to the speed of technological developments and the frequency of cybercriminal and malicious activities. In order to respond rapidly to new challenges, governments should design a legal and regulatory framework to protect their citizens against cybercrimes and ensure a safe and secure cyber space. This legal and regulatory framework should clearly define "crime", that is to say, what constitutes illegal cyber activity. It is essential that the definitions should be forward-looking enough to meet new and unforeseen tactics that cybercriminals may use. Thus, as technology continues to develop, forward-looking laws can still be applicable. This framework should also aim to reduce online crime. Most often, this framework can be achieved by amending existing laws or enacting new ones. Yet, while designing the legal and regulatory framework, protection of the privacy of personal data and freedom of expression should be safeguarded.

Another factor that the governments should place importance is to increase the effectiveness of law enforcement and its workflow, in other words how to form specialized cybercrime units and how to establish investigation. Investigative rights, search and seizure warrants while seeking access to cybercriminal contents should be clearly defined. Working together, the government and the business community should put forward the details of lawful interception of communications, digital investigation and use of electronic devices in cyber-related crimes. Record-keeping, registry and archive of cyber crimes are also essential for statistical analysis which help governments understand cybercrimes better.

Training and education of law enforcement officials such as prosecutors, judges, and lawyers and other investigators such as forensic specialists involved in combating cybercrime should be encouraged.

Collaboration with international law enforcement entities like the International Criminal Police Organization (INTERPOL) and the European Police Office (EUROPOL) is also vital to tackle cybercrime.

Another point that the governments should take into consideration is the international cybercrime agreements. This can be done by making national laws align with international ones and with bilateral agreements. For instance, The Council of Europe's Budapest Convention can be taken as a good model for cybercrime legislation that facilitates coordination and cooperation across borders. Like every state expects that, participating in cross border investigations and prosecutions and exchanging digital evidence enable governments to deal with cyber crimes efficiently.

Additionally, it should be kept in mind that legal and regulatory frameworks enforce organizations/civil sectors within the state to adopt cybersecurity measures in their respective areas of interest.

In a nutshell, with this framework, it can be ensured that the law enforcement agencies have sufficient rights and powers when it comes to preventing the planning, directing and financing of cybercrime in networks which lay the grounds for propaganda and criminal activity.

Estonia can be taken as a good example in terms of cybercrime legislation and cybercrime unit set-up. It has ratified the Budapest Convention in 2003 and included cyber crime in the penal code. It has also set up cybercrime units under the Central Criminal Police Department [24].

4.4 Following a Risk Management Approach

Risk management can be defined as the process of identifying and assessing risks and taking steps to reduce risks to the desired level. Identifying risks can be explained as having a better understanding of the risks so as to manage them most effectively. Assessing risks can be explained as focusing on dependencies. Risk management should consider the whole lifecycle of the process from procurement or development to operation and replacement. Especially, it is best achieved in the first place where it is an integral part of the design process of a service or product. Taking steps to reduce

risks can be explained as minimizing the probability or impact of unfortunate events that might put the critical services at risk.

Risk management can be conducted on different levels from the national level to the operational and to the tactical level. Risk management on a national level allows states to gain a holistic understanding of risks to the nation as a whole. Operational or tactical risk management allows considering more organization-based risks to specific infrastructures and services they provide.

For successful risk management, a framework - a standard designed to keep the confidentiality, integrity and availability of data – can be taken as a baseline. This framework helps the state with the identification and prioritization of critical infrastructures and helps what should or should not be invested to protect those assets on hand. The list of critical infrastructures should be specific enough so as to be workable when those assets need to be protected most. The parent organization liable for countrywide cybersecurity should periodically review and update the critical infrastructure list and confer liabilities to individual operators in order to hold them responsible or even accountable for not taking proper security measures. The German Cybersecurity Act **(**IT-Sicherheitsgesetz) is a good guide for defining and specifying critical infrastructures (which infrastructures are considered as critical infrastructures). Germany counts critical infrastructures as those that operate in the sectors of *energy, health, water, information technology and telecommunications, transport and traffic, nutrition, finance and insurance* [25]. Similarly, Turkey also defines critical infrastructures with her 2016-2019 National Cybersecurity Strategy as *electronic communication, energy, water management, critical public services, transportation and banking and finance.*

On the other hand, the risk management framework developed by the National Institute of Standards and Technology (NIST) is commonplace and one of the most widely known and can be taken as a guide (See figure 4.4). It helps organizations identify the risks to their information systems and take steps to reduce risks to an acceptable level.

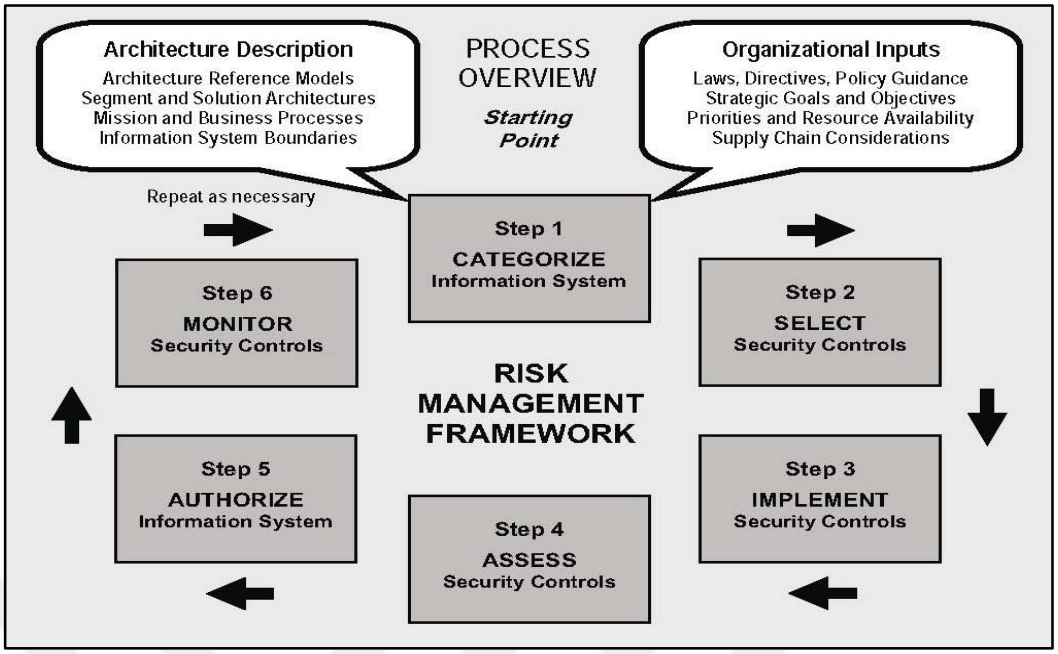

Figure 4.4 Six Steps of the Risk Management Framework of NIST

Risk management at the nation level should include deterrence, prevention, detection and recovery measures. The concept of deterrence is to discourage a potential attacker from thinking to initiate an attack. As inherently, deterrence efforts have two components. The first one is the application of effective defensive controls that make malicious activities extremely difficult to be conducted. The second one is the presence and illustration of retaliation against any performed attack and attackers. When deterrence fails, prevention is the next step. Prevention aims at preventing malicious activities in their initial delivery phase. There is one important aspect to be cautious in prevention. Too much prevention can result in reduced user productivity, whereas too little prevention can result in system compromises. When prevention fails, detection is essential in order to assess the damages and inform the affected system owner. Here, Intrusion Detection Systems (IDS) can be utilized. And last, recovery takes over once detection has occurred and recovery will seek to restore the normal state of the computer or network. This whole process is an important part of strengthening both a nation's and an organization's overall cybersecurity posture. All these four measures serve as cyber defense cycle in risk management.

As indicated above, risk management sets forth ways to determine what measures are needed for minimizing or avoiding the identified risk. Misunderstanding of a risk, or

its uncertainty, can lead to negative consequences and prevent the application of mitigation measures efficiently.

Risk management can also be addressed from a mathematical perspective. Risk equations/formulas might be used to mitigate risks. One of the commonly used risk equations in cybersecurity is :

$$RISK = (Threat \times Vulnerability \times Impact) \div Security\ Controls \quad \textbf{4.1}$$

In this equation, risk can be described as the probability that a threat will exploit a vulnerability of the system or an asset. This probability can be mitigated by security controls such as management, operational and technical controls.

If any of the three components in the numerator is zero, then the risk is also zero. For instance, if there is no threat, then there is no risk, even if high potential impact and severe vulnerabilities exist in the system. Unfortunately, the cyberspace is rife with targeted threats and innate vulnerabilities. Thus, the risk is a constant reality. The general idea of risk management is to determine potential risk and then reduce it to an acceptable level. In this perspective, cybersecurity efforts should focus on removing vulnerabilities and applying security controls. Well planned and implemented security policies, procedures and technical solutions can effectively mitigate risk [26].

4.5 Partnering with Industry and Academia

Modern life is completely dependent on a wide range of systems, services, functions, and assets which commonly referred to as infrastructures. Today, when several of these critical infrastructures such as banking, telecommunications, energy, healthcare and transportation are disrupted, a nation’s stability can severely be impacted.

In most of the countries, critical infrastructures and ICT networks are owned and operated by the private sector. The protection of these critical infrastructures is usually ensured by sector-specific regulations and by operator licenses. Therefore, in the context of cybersecurity, the private sector should be the first line of cyber defense.

Cyber threat preparedness requires swift and coordinated action from all parties in a given society. To ensure that state governments should utilize industrial and academic expertise through public-private partnerships.

Public-private partnerships are essential for boosting trust among the industry, academia and the government. Some of the partnership areas include agreement on common cybersecurity frameworks and standards, establishing effective information sharing and coordinating mechanisms, exchanging approaches, ideas and best practices for improving security and international coordination.

A good example of public-private partnership is Austrian Cybersecurity Platform (CSP). The Platform was set up in 2015 via Austrian Cybersecurity Strategy 2013 with more than 100 stakeholders from administration, science and businesses. It ensures a periodic exchange of information on cyber-related issues and provides the cooperation between the participating partners. The platform intends to bring work groups and existing activities together without changing their composition and main structure. The primary goal is to make activities in the field of cybersecurity transparent for all stakeholders and to intensify the collaboration between the public and private sector. Besides that, one of its major goals is to foster the establishment of sector Computer Emergency Response Teams (CERTs) for each critical infrastructure in Austria [27].

A similar structure can be seen in Turkey. In 2017, with the participation of all public agencies / organizations and representatives of private sector and academia, supported by the Presidency of Defence Industries and run by SSTEK Inc., Turkish Cybersecurity Cluster was generated. Companies who work in the field of cybersecurity can become a member to the cluster. The cluster mainly organizes technical and social activities in order to increase communication of members, catalog the products and services of member companies, establishes a certification laboratory and cybersecurity academy and organizes national / international activities such as conference, symposium, training, seminars, panels and fairs.

4.6 Forming an Information Sharing Mechanism

Given the complexity of cyber threats, forming a trusted information sharing mechanism among public and private stakeholders is vital for understanding a constantly changing environment all the better. Private stakeholders could share their input with public authorities on mitigating vulnerabilities, threats and emerging risks while public authorities could share only on a "*need to know*" based information. Combining both inputs produces a very powerful insight on how to deal with threat landscape. Incorporating trusted international information sharing mechanism into the national mechanism also consolidates cybersecurity.

Sharing threat and risk-based information such as hacking trend data or unexplained anomalies can be counted as examples of information sharing. If needed, coordination centers can be formed for achieving info sharing.

Operational information exchange –like those in NATO exercises - between countries is also becoming increasingly crucial in the fight against cybercrimes. A significant effort between allies and partners should be made to share the cybersecurity-related experience. Thus, exchange information and a lessons-learned environment can be forged in which all allies, partners and stakeholders can benefit.

A good example of information sharing is the Swiss Reporting and Analysis Centre for Information Assurance (MELANI) and its information sharing platform MELANI-Net. Via MELANI-Net, critical infrastructure operators can be warned via e-mail or SMS. It was set up in October 2004 for close cooperation with the private and public sectors. As soon as it was in charge, MELANI built relationships with important foreign equivalents to be able to identify emerging threats timely for its early warning system. It uses a broad national and international network, especially in close collaboration with technical experts from CERTs and with the Federal Intelligence Service (FIS). It also has contacts with law enforcement agencies in important countries by being a part of Interpol Working Groups. It can compile threat analyses, statistics, situation reports, perpetrator profiles and their background information and can make them available to the operators of critical infrastructures. In this way, for instance, a threat of economic espionage could be directly imparted to the

representatives of the private sector. Besides, with the dissemination of knowledge, MELANI works as a unit that fosters information sharing among the companies and raises their awareness against recent threats. In turn, it receives information from these companies [28].

Another example can be seen in Turkey. There are some main bodies and their affiliates that are liable for ensuring cybersecurity at national-level. The first one is the Cybersecurity Board which is responsible for taking decisions with regard to cybersecurity at national-level. It mainly determines the policies, strategies and action plans. Another body is the National Cybersecurity Incident Response Center (NCIRC). It mainly coordinates the incident response activities internationally and nationally. There are Institutional CSIRTs and Sectoral CSIRTs as well affiliated to NCIRC. Via these CSIRTs, NCIRC ensures information sharing and coordination between actors in the field of Internet, law enforcement agencies, international actors, research centers and private sector.

4.7 Adopting Cybersecurity Standards Recognized by Industry

The main objective of using cybersecurity standards is to reduce the risks. Standards provide a product, system, technology or process with establishing common security requirements needed for secure solutions. Well-established cybersecurity standards enable consistency among manufacturers and serve as a reliable measure for purchasing secure products and services. A standard must meet user needs and be practical in terms of cost and technological limitations.

Another aspect of cybersecurity standards is that they facilitate sharing of knowledge and best practices by ensuring a common understanding of terms and definitions which results in preventing errors. Using common terms and definitions saves time in the development of new standards and their interoperability. Another benefit is that their usage generally results in improvements in quality and during their development process, a wide range of experts and prototyping involve. So, products or services conforming to cybersecurity standards offer more confidence than nonstandard products and services.

When cybersecurity standards are not available, several problems often emerge. Institutions and organizations may not be aware of the inherent security weaknesses of the technology that they adopted or what additional security measures may be required to compensate for those weaknesses. This makes systems more vulnerable and likely to be exploited. Take a war platform that operates online as an example and consider that a nation's Ministry of Defence has acquired that platform. Lacking cybersecurity standards might endanger that nation's survival during a crisis.

Standards can be seen in different ways. *Company Standards* are developed by manufacturing companies with no external participation and they are unique to that company, mostly based on experience. *De facto Standards* are prevailing applications or practices that are used widely although they have no official status such as QWERTY keyboard. *Voluntary Standards* are established generally by private sector bodies and developed through consensus or agreement of stakeholders, for that reason they can also be called industry or consensus standards. *Mandatory Standards* are administered by a regulatory agency or implementing organization in which failure to comply with carries a sanction.

A standard also depends on the audience to whom that standard applies. An *International standard* is issued by an international organization and made available to the public such as International Organization for Standardization (ISO) standards and used in multiple nations. A *Regional Standard* is adopted by several nations in a particular geographic region, for example, the European Committee for Standardization (CEN) standards. A *National Standard* is a standard developed by a national standards body for use in a particular country. A national standard can also be an international standard that is adopted for use by an individual country [29].

Cybersecurity standards are useful. They bring tangible benefits and proliferate every day. Therefore, governments and businesses mandate their implementation increasingly. More suppliers and vendors manufacture and sell standards-compliant products and services. Additionally, a growing number of organizations are being involved in standards development.

Adopting minimum security standards for a given sector is important and not only all organizations in that sector should comply with these standards but also these standards should be continuously reviewed and updated. Existing international adopted standards can help governments utilize proven standards without having to create peculiar and less known security practices [30].

These standards can be adopted from specialized organizations like ISO in which ISO/IEC 27000 family of standards can be a basic example for keeping information assets secure. Among these 27000 family, 27001 contains the requirements of an Information Security Management System (ISMS) and 27002 contains information security with 11 detailed security controls.

ISO/IEC 27001 formally defines the mandatory requirements for an Information Security Management System (ISMS). It uses ISO/IEC 27002 to indicate suitable information security controls within the ISMS, but since ISO/IEC 27002 is merely a code of practice/guideline rather than a certification standard, organizations are free to select and implement other controls, or indeed adopt alternative complete suites of information security controls as they see fit. ISO/IEC 27001 incorporates a summary (little more than the section titles in fact) of controls from ISO/IEC 27002 in Annex A. In practice, most organizations that adopt ISO/IEC 27001 also adopt ISO/IEC 27002.

ISO/IEC 27002 is a code of practice - a generic, advisory document, not a formal specification such as ISO/IEC 27001. It recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information. Organizations that adopt ISO/IEC 27002 must assess their own information risks, clarify their control objectives and apply suitable controls (or indeed other forms of risk treatment) using the standard for guidance.

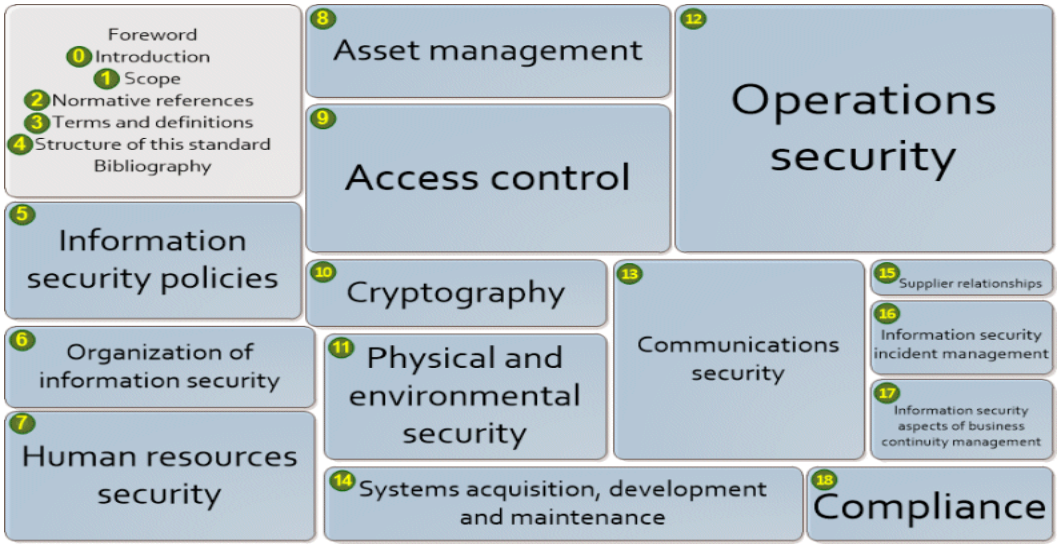

Figure 4.5 Contents of ISO/IEC 27002:2013

Another framework that can be adopted is NIST SP 800-53 rev4 which provides a comprehensive set of security controls for the industry.

4.8 Raising Public Awareness

In the first place, individuals are responsible for the safe use of ICT tools. Therefore, cybersecurity starts with individuals. In this regard, state governments should invest in training and education for their citizens to improve cybersecurity awareness in society. Through awareness raising, individuals have the opportunities to learn how to behave in the online world and protect themselves from typical risks.

In this context, the states should:

- Find ways to wage constructive campaigns in order to raise public awareness. These campaigns might be, for instance, distributing free software and installations like firewall or antivirus or by providing voluntary certification programmes and arranging cyber competitions with a reward.

- Make use of communication channels like social media for reaching out to local people in order to advertise local programs and campaigns about cybersecurity.

- Organize a national week or day (like Black Friday) in order to engage the citizens in cyber initiatives such as conferences, seminars, lectures and other means.

A good example of increasing awareness is European Cybersecurity Month. It is the EU's annual public awareness campaign that takes place each October across Europe. The aim is to promote cybersecurity among citizens and organizations and to highlight the simple steps that could be taken to protect their data, whether personal, financial or professional. In 2017 a total of 532 activities took place across 33 countries [31].

4.9 Promoting International Cooperation and Conducting Cybersecurity Exercises

Since cyber threats are transboundary and no uniform international treaty exists which binds all states and cover all cyber threats, cybersecurity can be consolidated by international cooperation with allies and partners not single-handedly. Especially the collaboration with forerunner and pioneer states/organizations is very critical. With a multilateral approach, based on the consent of all participating nations, it could be effective in decreasing the security threats posed by cyber activities because cybercrime investigation often demands international cooperation.

International civilian aviation, for instance, has been protected through many regulations and treaties adopted by numerous states acting through the International Civil Aviation Organization (ICAO) -192 member states as of 19/04/2018 [32] – It is a specialized agency, within which standards are developed by committees of experts. Like ICAO, it is a must to form an international regime in which all states can set the stage for coordination and collaboration on cybersecurity and refrain from cyber attacks. The cyber threat cannot be entirely overcome, but if cyber attacks on certain level should be treated as illegal everywhere regardless of motive, the harms could be limited [33].

Creating a global cyber secure culture and finding mutually acceptable solutions to common challenges should be a goal for all the countries. In order to reach this goal, governments should express their cybersecurity concerns at negotiation tables with their foreign policies. Something like creating cyber diplomacy. They should participate in establishing international cybersecurity norms and standards via this cyber diplomacy.

There are some international efforts that the countries might engage in the field of cybersecurity and cybercrime such as the Organization of Security and Cooperation in Europe (OSCE), the Council of Europe's Budapest Convention, the African Union's Convention, the Shanghai Cooperation Organization, the Arab Convention as well as the NATO Cooperative Cyber Defence Centre of Excellence for the Tallinn Manuals 1.0 and 2.0.

Governments should also make their workforces participate in domestic and international cybersecurity and incident response exercises. These exercises enable authorities to evaluate their existing contingency plans, to increase cooperation between different sectors, to discover specific strengths and weaknesses, to identify interdependencies, to stimulate improvements in planning processes, to develop institutional capacity in response to incidents under pressure and to improve the overall resilience and preparedness levels.

A good example of both national and international exercise participation is Sweden. Sweden conducted the National Cybersecurity Exercise "NISÖ" in 2012 with 17 organizations in total. The purpose of the exercise was to strengthen society's ability to manage national IT related crises, primarily by developing the ability to cooperate and coordinate between public and private sectors [34]. Sweden also participated in the International Watch and Warning Network Exercise in 2013 known as Cyber Storm IV which organized by the United States [35].

As for Turkey, in order to increase the skills of the participants and to improve public awareness, 3 national and 1 international cybersecurity exercises were conducted in 2015.

4.10 Building Capacity and Capability with Education and R&D

In order to ensure deterrence, prevention, detection and prosecuting of cybercrime, cybersecurity-related know-how is pivotal. The study of basic cybersecurity skills must be included at all levels of education. Especially students should be encouraged to join and prepare themselves to enter the cybersecurity field. This includes developing cybersecurity curricula across primary and secondary schools,

incorporating cybersecurity courses into computer science and IT programs and creating cybersecurity degrees and government apprenticeships as well as formal internships and traineeships. All in all, cybersecurity career paths should be fostered in every part of education.

Sustaining cybersecurity professionals are also vital based on the needs of industry and government. Hence additional accreditation and certificates should be established in the form of higher education providing master's and doctoral degrees. Experts from the best cybersecurity and information technology companies should be employed if needed by the governments.

A good example of education is Estonia's cybersecurity programs. Estonia is investing and taking several measures to increase the number of cybersecurity experts. The Ministry of Defence is providing grants to students who study PhD. In addition, cybersecurity programs at universities have been developed such as Cybersecurity MSc in Talinn University of Technology [36].

Research and development for capacity and capability building are also needed in order to develop and deliver new technologies, tools and techniques. In this regard, the state governments should:

- Advocate cybersecurity-related research and development projects by means of incentive mechanisms like grants, research funds, procurement aids, tax credits and competitions.

- Stimulate businesses providing cybersecurity solutions and contribute them to the export of these solutions.

- Encourage universities to bolster their basic research, applied research and innovation in cybersecurity. For instance, universities can establish ties with the international research communities studying on cybersecurity such as computer science, electrical engineering and cryptography.

- Establish a cybersecurity R&D center and make this center provide technical and management expertise support for the wide range of research, testing, development and evaluation activities.

A good example of R&D is The National Cybersecurity R&D Programme in Singapore. It was launched in 2013 and it supports research efforts in both technological and human science aspects of cybersecurity. It covers six themes: resilient systems; scalable trustworthy systems; threats detection, analysis and defence; effective situation awareness and attack attribution; combatting insider threats; efficient and effective digital forensics [37].

4.11 Laying Out National Cybersecurity Contingency Plans

A contingency plan is a plan that is prepared for dealing with an emergency or something bad that might possibly happen and cause problems in the future. It is the measures and practices on hand for responding to major incidents when required.

The national cybersecurity contingency plan should explain the crisis criteria and define the actions and the roles of stakeholders for handling the crisis. Especially, during the emergency situations, the plan should put forth the procedures for the media activity. It should be reviewed after every exercise from lessons learned experience.

Contingency plans should be established in close collaboration with military and civil agencies since cybersecurity contingency planning ensures the continuation of critical services in case of emergencies and crises both on civil and military facilities. Especially for the civil sector, critical manufacturing processes are increasingly dependent on automation, therefore a well-established national contingency plan surely can prevent any cyber attack from bringing a unit or plant down. They should also include cyber warfare retaliation capabilities and when needed and directed, these capabilities should be used against adversary premises or systems.

A good example of cybersecurity contingency planning is “GOVCERT.LU”. GOVCERT.LU stands for the CERT of the Government of Luxembourg. The service oversees the management of cybersecurity incidents compromising Luxembourg, its economy or its citizens and is responsible for receiving, reviewing and responding to

such reports. In case of a serious cyber attack or vulnerability affecting the public or private sector on a large scale, the national contingency plan is activated. Several managing bodies are set in motion to ensure appropriate countermeasures and immediate responses whenever and wherever required. These bodies are the Crisis Unit (CC, Cellule de crise) and the Cyber Risk Assessment Unit (CERC, Cellule d'évaluation du risque cyber). They are composed of technical experts and offer a surveillance and vulnerability analysis within the national contingency plan. In the event of a large scale cyber threat, the general public is informed about the situation by the government and by its website *www.infocrise.lu* [38].

4.12 Fostering Cyber Insurance in Businesses

Despite improvements in risk protection techniques such as antivirus and antispam software, firewalls and IDSs over the last decade, it is not possible to achieve perfect or near-perfect cybersecurity protection. Therefore, a very new need arises as an alternative method for risk mitigation in cyberspace. In this regard, some security researchers have recently identified cyber insurance as a potential means for mitigating cyber-related risks.

Cyber insurance is a kind of contract that an individual or entity can purchase to protect themselves from cyber-related risks and activities. Risks of this type are generally excluded or not specifically defined in traditional insurances.

Coverages provided by cyber insurance mostly include:

- Losses resulting from data breaches, fraud, cyber extortion and computer attacks like the virus, other malware attacks or DoS attacks;

- Defense and liability coverage associated with third-party lawsuits. For example, losses the companies caused to others by errors and omissions, copyright infringement or failure to safeguard data;

- And other coverages including regular security audits, post-incident and investigative expenditures.

Generally, potential cyber insurers are Internet service providers, cloud providers and traditional insurance organizations like Allianz. But, many insurance companies have been hesitant to take place in this market, as sound statistical and actuarial data for cyber exposure is non-existent. However, cyber insurance premiums are expected to grow from around $2 billion in 2015 to an estimated $20 billion or more by 2025 while insurers are continuing to refine underwriting requirements [39].

Within a country, the neediest sector for cyber insurance is the business sector. But many small (fewer than 250 employees) and mid-sized businesses overlook or underestimate the cyber threats when compared with the larger companies. The main reason for this is that small and mid-sized companies do not believe they will be the target of an attack and the cost of insurance is not affordable. However, they are more vulnerable to cybercrime - especially social engineering attacks - and fraud than larger ones since they also store customer information and have business banking accounts. According to Ponemon Institute, half of all small and mid-sized businesses in the U.S. experienced a data breach in 2016 and 55 % experienced a cyber attack. Globally, more than 75 % of certain large businesses but less than 5 % of small and mid-sized businesses have some cyber insurance in 2015 [40].

In cyber insurance, there is a win-win situation. The cyber insurers earn profit from premiums, network users are compensated for losses, policy makers ensure the increase in overall network security and software suppliers increase their product sales by means of forming alliances with cyber insurers.

On the other hand, a cyber insurance market helps reduce the number of cyber attacks and make the cyberspace more robust by encouraging self-defense (the efforts made by an online user to secure his overall system through technical solutions such as antivirus and antispam software, firewalls, secure operating systems and updated patches, etc.).

In addition to boosting cybersecurity directly, cyber insurance is completely beneficial in case of a large-scale security breach. Insurance guarantees a smooth funding system to all kinds of businesses for recovery from major losses, helping them return to normal and reducing the need for government support and assistance.

All in all, cyber insurance is a risk management and mitigation technique via which online risks are transferred to an insurer, in return for a fee or a premium.

4.13 The Assessment of Turkey According to 12 Controls

12 critical cybersecurity controls above are identified as a minimum requirement in order to strengthen a country's overall cyber posture. These controls are a blend and brought out from:

- NCSSs including those of Finland, Estonia, Sweden, the EU, the USA (the DOD, the DHS and the White House), the UK and Turkey,

- Guides including those of ENISA, Microsoft and a co-publication,

- Indices and reports including those of GCI by ITU, National Cybersecurity Index by Estonia Development Cooperation and Global Cybersecurity Status Report by Information Systems Audit and Control Association (ISACA),

- Relevant articles, books, thesis, official publications and periodicals.

When some of the top ten most committed countries in GCI 2017 are examined, several good practices stand out. Such as:

- Singapore stands out with child online protection since internet service providers in Singapore are required to comply with the Internet Code of Practice. They are obligated to offer filtering services with Internet subscriptions. This practice can be an example of "Shaping Legal and Regulatory Framework" control.

- The USA stands out with information sharing since government agencies such as defence, health, justice, intelligence community and energy work collaboratively to enhance information exchanges at machine speed. This practice can be an example of "Forming an Information Sharing Mechanism" control.

When the cyber situation in Turkey is examined according to 12 security controls, below recommendations can be brought forward:

Table 6.1 Issues that needed to be addressed in Turkey

ISSUES THAT NEEDED TO BE ADDRESSED IN TURKEY			
Line	**Strategic Controls**	**Situation in Turkey**	**Remarks and Recommendations**
1	Establishing and Empowering a Parent Organization Liable for Nationwide Cybersecurity	The parent and the executive organization is Ministry of Transport and Infrastructure. But critical policies, strategies and decisions are taken by the Cybersecurity Board. In other words, the executive and the decision-making bodies are different.	1. In case of a big scale cyber attack, crisis or incident management might be a problem. The decision-making and the executive authority should be strong and unique to deal with cybersecurity directly and ensure coordination between public sector, private sector and related CSIRTs. To avoid confusion, the authority can be single under the Presidency so as to ensure better governance in cybersecurity. 2. As a cyberwarfare entity, the parent organization should also have an offensive capability in addition to defence capability against the adversaries when authorized.
2	Adopting a National Cybersecurity Strategy	2016-2019 National Cybersecurtiy Strategy is in force	-
3	Shaping Legal and Regulatory Framework	Legal Framework is established with articles between 243 and 246 under the Penal Code.	-
4	Following a Risk Management Approach	-	A nation-level risk management and mitigation approach can be adopted by the parent organization in order to gain a holistic understanding of risks as a whole and can be reflected to the National Cybersecurity Strategy.
5	Partnering with Industry and Academia	Partnership is provided by the Cybersecurity Cluster which is supported by the Presidency of Defence Industries and organized by a company named SSTEK Inc.	1. The cybersecurity platform should be standing and it should be organized and coordinated under the parent organization as a technical working group in order to bring business, science and administration groups together. 2. The representatives of civil sector such as industry and academia should be a part of the Cybersecurity Board.
6	Forming an Information Sharing Mechanism	Information sharing mechanism is established via NCIRC and related institutional and sectoral CSIRTs	-

ISSUES THAT NEEDED TO BE ADDRESSED IN TURKEY			
Line	**Strategic Controls**	**Situation in Turkey**	**Remarks and Recommendations**
7	Adopting Cybersecurity Standards Recognized by Industry	No uniform or nationally agreed terminology in cybersecurtiy exists	The terminology and related terms and definitions about cybersecurity such as cybercrime and cyber space should be established in the Turkish Language Association database.
8	Raising Public Awareness	There are some initiatives in order to raise public awareness, but a national cybersecurity date is not clear.	A national day/week/month can be determined as the national cybersecurity day/week/month in order to engage the citizens' interest or become a part of European Cybersecurity Month and wage national campaigns every October.
9	Promoting International Cooperation and Conducting Cybersecurity Exercises	National and international cybersecurity exercises are being conducted.	Efforts can be made to shape international cyberspace policy and to establish an international cyber diplomacy or regime like Missile Technology Control Regime.
10	Building Capacity and Capability with Education and R&D	Education of cyber security is generally provided by the private sector. Although some universities began education in the last years, it is not sufficient.	The study of basic cybersecurity skills can be included inside the curricula of all levels of education including primary and secondary schools.
11	Laying Out National Cybersecurity Contingency Plans	-	An early warning mechanism by which the whole public will be informed about the situation in case of a large-scale cyber threat can be established.
12	Fostering Cyber Insurance in Businesses	A few insurer companies have started to provide cyber insurance, but it is not widespread.	As an alternative risk mitigation method, a cyber insurance encouragement mechanism can be established and via this mechanism, cyber insurance can be fostered across small and mid-sized businesses.

CHAPTER 5

THE FUTURE OF CYBERSECURITY

None of us can know exactly what the future world is going to look like. But we can foresee by paying attention to the key trends today that might shape the world in the future. For example, renewable energy is the key trend that will shape the future. This fact is also applicable to cybersecurity. Knowing key trends in cyberspace will help us understand the strengths and weaknesses of the future of cybersecurity.

Of these key trends, "Internet of Things" is maybe one of the most important ones. As better and cheaper electronic devices increase throughout the world, so do their connections to the web-enabled devices, thereby enabling cyber attackers to penetrate far deeper into our lives than ever before. Another key trend is "Cloud Computing" which moves personal computing and data storing from hardware you purchase to a service you buy online. Cloud computing might solve some security issues that an individual cannot but what about the responsibilities from the user to the cloud provider or vice versa? Yet another trend is "Artificial Intelligence (AI)". With the growing data, businesses are being obligated to reshape their existing infrastructure based on AI. But AI is a two-edged sword, having its own advantages and disadvantages. Whereas it provides many benefits in terms of automating the entire process, from identifying the threats to taking countermeasures, it may open doors to many vulnerabilities, providing opportunities to hackers to exploit AI for creating destructive algorithms that support their intention. [41]

There is a fact that the nature of cyberspace is constantly changing because cyberspace reflects the characteristics and needs of its users. The more the users differ, the more the content and the use they make vary. Anyone can see Cyrillic or Arabic characters on websites rather than Latin ones thereby causing the Internet to become more and more divided. On the other hand, "Mobile Trend" has been growing. Anyone is accessible from every point of the globe. As phones and tablets are used more, the security risks are also going mobile making everyone all targets.

So overall, it can be said that these trends will bring about new systems that are smarter and more sophisticated than today, consisting of large amounts of data (big data). They will have the ability to update themselves rapidly, taking decisions in real time and interacting with each other. As a result, these new systems on the back of key trends will also bring more sophisticated cyber threats along. Today, almost everybody locks their doors at nights and fastens seatbelts while driving. In the future, it is certain that the same level of caution will be given to ensure digital security, in other words, there will be much more cyber challenges in the future waiting of human beings.

CHAPTER 6

CONCLUSION

In the military circle there is a very accurate definition, it reads as "*Defence starts from the furthest point*". It means that if we would like to keep our country safe, we should eliminate the threats beyond our soils before they reach our soils. It is also valid for the cybersecurity. Cyber threats are international. They can be conducted at any part of the world at any time. Nations should form their cybersecurity posture away from their soils. In order to achieve this, strategic cybersecurity controls should be adopted as "the first line of defence".

This study puts forward the first line of defence in a methodical way. It should be acknowledged that the security controls in Chapter 4, even when implemented perfectly, will not guarantee a risk-free cyber environment. However, it can be expected that deployment of these security controls will facilitate a relatively rapid establishment of the first line. Additionally, these controls also improve public service delivery; accelerate economic growth; increase defence and countermeasure capabilities; accumulate knowledge and develop skills and expertise.

Most of the studies in the literature about cybersecurity controls overlook the first line. They generally include the second line controls such as using antivirus, firewall, IDS, network intrusion prevention systems (NIPS) and robust passwords; updating and backing up operating system and server; monitoring user activity; whitelisting applications; restricting administrative privileges and so on. These controls might be pre-emptive measures against cyber attacks but they do not prevent cybercriminals acting in the first place. International pressure on cybercriminals is needed in order to make them think twice before committing their cyber attacks. The best way for building up an international pressure requires nation-level planning.

Nation-level planning brings about numerous benefits both for the citizens and for the nation itself. For instance, the states that have internationally renowned cybersecurity situation are a lucrative target for foreign investment. Yet, while ensuring this nation-

level planning, the states should also be careful during their every movement. Because, cybersecurity is an ecosystem in which cyber-related laws, organizations, skills, cooperation and technical implementation need to be in harmony to be most effective. If the states diminish or infringe on the fundamental rights of their citizens while ensuring cybersecurity, the negative results might shake their existence.

For the states that are about to adopt strategic cybersecurity controls for the first time or intent to improve their cybersecurity posture, controls in Chapter 4 are the main guides that they can benefit. Among them, authorizing a competent organization is the first step. After that, identifying policy, strategy and goals via this organization constitutes the second step, and adopting remaining controls constitute the subsequent steps.

The cyber situation in Turkey has been improving day by day. Yet, there are still shortcomings that needed to be addressed. One of the most important ones is the weakness of Golden Triangle (the cooperation among government, private industry and academia). Golden Triangle should be first established inside the policy and decision-making bodies which in turn reflects its influences on the whole society. That’s why, it is highly recommended that the cyber decentralization frame in Turkey should be reformed once again towards the centralization in which Golden Triangle is ensured by the unique policy and decision-making body.

All in all, cyberspace is changing quickly. The states should keep pace with this quick change by implementing some strategic security controls. And these controls should first start with the states themselves. Otherwise, non-lethal results of cyber attacks might be as catastrophic as the lethal results of nuclear fallout.

REFERENCES

[1] Waldrop M., DARPA and the Internet Revolution, 50 Years of Bridging the Gap, DARPA

[2] The Economist, War in the fifth domain, Retrieved October 10, 2018, from http://www.economist.com/node/16478792, July 1, 2010

[3] Dunleavy P., Authoring a PhD – How to plan, draft, write and finish a doctoral thesis or dissertation, Palgrave Macmillan, 2003

[4] European Commission Migration and Home Affairs, Cybercrime, Retrieved November 02, 2018, from https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

[5] United Nations Office on Drugs and Crime, Cybercrime, Retrieved November 5, 2018, from https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

[6] USLEGAL, Cyber Warfare Law and Legal Definition, Retrieved November 08, 2018, from https://definitions.uslegal.com/c/cyber-warfare/

[7] Appazov A., Legal Aspects of Cybersecurity, Faculty of Law University of Copenhagen, 2014

[8] Global Risk Advisors, The United Nations and Cyberwarfare, Retrieved November 15, 2018, from https://gra.com/united-nations-cyber-warfare/, September 28, 2016

[9] Wikipedia, Cyberterrorism, Retrieved November 18, 2018, from https://en.wikipedia.org/wiki/Cyberterrorism

[10] NBCNews, A look at Estonia's cyber attack in 2007, Retrieved November 20, 2018 from http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/, July 8 , 2009

[11] Kozlowski, A., MA, Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan, European Scientific Journal, February 2014

[12] CSS Cyber Defense Project, Hotspot Analysis: Stuxnet, Zürich, October 2017, Version 1, Risk and Resilience Team Center for Security Studies (CSS), ETH Zürich

[13] GOV.UK, Cyber and Government Security Directorate, Retrieved November 22, 2018, from https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance

[14] Sullivan&Cromwell LLP, The Cybersecurity Act of 2015, December 22, 2015

[15] The White House, National Cyber Strategy of the United States of America, September 2018

[16] Ciglic K., Microsoft, Cybersecurity Policy Framework, A Practical Guide to the Development of National Cybersecurity Policy

[17] Oxford University Press (2012):Oxford English Dictionary, 7th Edition

[18] RETEL S., Cybersecurity Strategy (2014-2017), Ministry of Economic Affairs and Communication, 2014

[19] ENISA, NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies, November 2016

[20] ITU, Global Cybersecurity Index (GCI) 2017, Geneva, 2017

[21] ITU, National Strategies, Retrieved November 27, 2018, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx

[22] Luiijf E., Graaf de P., Besseling K., Spoelstra M., Ten National Cybersecurity Strategies: A Comparison, Conference Paper, January 2013

[23] ITU, The World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity, 2018

[24] Republic of Estonia, Ministry of Foreign Affairs, Estonian police to set up cyber crime unit, Retrieved November 28, 2018, from https://vm.ee/en/newsletter/estonian-police-set-cyber-crime-unit, July 28, 2015

[25] BSI Act of 14 August 2009 (Federal Law Gazette I p. 2821) last amended by Article 1 of the Act of 23 June 2017 (Federal Law Gazette I p. 1885)

[26] Tytarenko O., Selection of the best security controls for rapid development of enterprise-level cyber security, Monterey, California: Naval Postgraduate School, 2017

[27] Digital Austria, Cybersecurity, Austrian Cyber Security Platform (CSP), Retrieved November 30, 2018, from https://www.digital.austria.gv.at/cyber-security

[28] Cavelty, M.D., Cybersecurity in Switzerland, Springer, ETH Zürich, Center for Security Studies, Zürich, Switzerland, 2014

[29] Scarfone K., Benigni D., Grance T., Cyber Security Standards, National Institute of Standards and Technology (NIST), Gaithersburg, Maryland

[30] IT Alliance for Public Sector, State Cybersecurity Principals & Best Practices

[31] European cyber Security Month, What's ECSM?, Retrieved December 02, 2018, from https://cybersecuritymonth.eu/about-ecsm/whats-ecsm

[32] ICAO, Member states, Retrieved September 25, 2018, from https://www.icao.int/about-icao/Pages/member-states.aspx

[33] Sofaer A., Managing the Cyber Security Threat, Hoover Institution-Stanford University, 2014

[34] Holfeldt R., Swedish Civil Contingencies Agency (MSB), National Cybersecurity Exercise (NISÖ 2012), 2012

[35] Homeland Security, Cyber Storm IV, Retrieved December 02, 2018, from https://www.dhs.gov/cyber-storm-iv, May 17, 2018

[36] Study Estonia, MSc Cyber Security, Retrieved December 03, 2018, from https://estonia.dreamapply.com/courses/course/31-msc-cyber-security

[37] National Research Foundation, Singapore Government, Retrieved December 05, 2018, from https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme, November 07, 2018

[38] GOVCERT.lu, National Contingency Plan, Retrieved December 04, 2018, from https://www.govcert.lu/en/national_contingency_plan.html

[39] Wikipedia, Cyber Insurance, Retrieved December 06, 2018, from https://en.wikipedia.org/wiki/Cyber_insurance

[40] Lynch J, Small Business and Cyber Insurance, Insurance Information Institute, November 2017

[41] Cioreview, The Future of Cybersecurity: Artificial Intelligence, Retrieved December 09, 2018, from https://www.cioreview.com/news/the-future-of-cybersecurity-artificial-intelligence-nid-26476-cid-145.html, May 28, 2018

CURRICULUM VITAE



PERSONAL INFORMATION

Name Surname : Burak AYDIN

Date of Birth : 08.04.1983

Phone : 0530 408 0312

E-mail : burak.aydin83@outlook.com.tr

EDUCATION

High School : Maltepe Military High School

Bachelor : Military Academy

PROFESSIONAL WORK EXPERIENCE

2017-Cont.	Procurement Officer in Ministry of National Defence
2016-2017	Project Officer in Ministry of National Defence
2015-2016	Liaison and Observation Team (LOT) Deputy Commander in EUFOR
2013-2015	Army Property Accountant
2007-2013	Army Platoon and Company Commander

TOPICS OF INTEREST

- Defence and Logistics