Research Article

Creating and Implementing an Effective and Deterrent National Cyber Security Strategy

Mustafa Senol and Ertugrul Karacuha

Informatics Institute, Istanbul Technical University (ITU), Ayazaga Campus, Maslak, 34469 Istanbul, Turkey

Correspondence should be addressed to Mustafa Senol; senolm15@itu.edu.tr

Received 29 March 2020; Accepted 4 May 2020; Published 1 June 2020

Academic Editor: Kevser Dincer

Copyright © 2020 Mustafa Senol and Ertugrul Karacuha. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper presents a new national cyber security strategy (NCSS) covering the deterrence perspective from creation to implementation. With the aim of responding to and ensuring cyber security effectively, studies on which pathways should be followed and what methods should be used to develop, create, and implement a NCSS are being conducted in Turkey, as in all countries. In this context, by explaining the importance of cyber power, the need for cyber power to be considered as one of the elements of national power and the importance of providing security against cyber attacks with deterrence by cyber power are discussed, while a new and integrated approach for the creation and implementation of a NCSS and an authoritarian organizational structure responsible for this strategy is proposed. It can be concluded that the proposed effective and deterrent NCSS model and approaches might help to efficiently and effectively handle these issues for better management, control, and auditing for cyber security issues; provide new concepts for cyber security issues supported by cyber power and deterrence on this issue in the world; introduce integrated approach to cyber security strategies and policies on the stages of developing and implementing a NCSS; bring a number of issues to support cyber security and defence in different perspectives; and achieve a high degree of success, especially in terms of effectiveness and existing deterrence strategies and action plans of basic structure, with the proposed approach. Finally, it is expected that the proposed strategy, steps, and suggestions might help to improve cyber security issues and national strategies in near future to secure national assessment more than ever with a powerful concept of deterrence. In addition, this approach, which has been put forward for effective implementation of cyber security by ensuring better management, control, and supervision, can be easily used by all other countries.

1. Introduction

The developments in ICT and the improvements of state's power particularly in the economic, political, and military fields have made cyber space (cyber domain) critical in combination with physically and virtually valuable assets as given in Figure 1. The cyber space is being referred to as the 5th operational domain after the operation (warfighting) domains of land, sea, air, and space.

As the importance of cyber space increases, malicious movements and attacks that have come with the development of information and informatics systems continue to increase rapidly today. The following statement of Alvin Toffler, a US writer and futurist known for his works discussing technology and for his predictions for the future,

depicts a clear picture of the current situation, in addition to drawing attention to the issue at hand and emphasizing its importance: "our technological power is increasing, but the side effects and possible dangers are growing much faster than this" [1].

While the facilities and conveniences provided by the cyber space with the developments in information and communication technologies make life more dependent on such facilities and conveniences every day, significant damages that individuals, societies, and countries have suffered as a result of using cyber space for threats, attacks, harm to life and property, and similar malicious purposes have caused great changes in the understanding of the notion of security. In cyber space, the intentions and needs to harm or negatively affect the counterparty's information

and informatics systems have created the concept of “cyber attack–cyber assault,” and the need to protect information and informatics systems against malicious acts and attacks has created the concept of “cyber security–cyber defence.” Countries have started to develop and implement strategies and policies on cyber defence and cyber attack, and the concept of “cyber war” has been discussed more and more every day. In this context, it becomes a common thought that cyber security is a national security issue and it is an integral part thereof.

Strategies, policies, and measures are being developed to prevent cyber attacks due to dominant effect or deterrence of “cyber power” on attackers, crackers, or hackers, i.e., informatics systems and infrastructures that are required for the initiation and maintenance of cyber war and are attained in cyber space, the ability to use them effectively, and wars caused by cyber attacks, and to dissuade those who think about cyber attacks or war from pursuing such thoughts and actions. Renowned Chinese philosopher and war strategist Sun Tzu, who lived in the 500s BC, stated that “forcing someone to submit without war is the best” [2]; the famous quote emphasizes that deterring the attackers from their wishes, attacks, or wars, in particular cyber wars and “cyber deterrence,” may be the best. In addition, the possibilities and capabilities of cyber power attained in cyber space can be used to ensure “deterrence” in many areas, especially in diplomacy and military fields.

Governments are trying to carry out enormous work in the fields of cyber security, cyber warfare, and cyber deterrence, to evaluate the situation within the framework of technological developments, take measures by identifying risks and threats, make targets in line with their needs by making predictions for the future, develop strategies and policies, and implement them effectively. With the increase in the use of computers and the widespread of the Internet, which is a constantly growing communication and information communication network around the world, significant progress has been attained compared to past with the work initiated to prevent and eliminate the risks, threats, dangers, etc. that occur in parallel with the developments in the world. In this context, besides increasing the efficiency by eliminating the deficiencies and inadequacies related to cyber security strategies and policies against cyber attacks and incidents, it is thought that it would be appropriate to address the issue of cyber deterrence, which is recently a hot topic of conversation and study, with a holistic approach along with cyber security strategies and policies.

Based on the thoughts put forward, in this study, we aimed to answer the question as to what ways should be followed to create a needed strategy and how this strategy should be developed in order to ensure effectiveness of the cyber security of assets, information and communication systems, and infrastructures owned by a country in a cyber space to become an effective power for cyber war and deterrence and to create a summary resource for the studies to be carried out.

This paper consists of 5 main sections. In Section 2, the methodology followed is explained and supported by explanations and examples from the literature. In Section 3, the

terms for cyber security, cyber power and deterrence, approaches, and studies are expressed. An integrated approach has been introduced to cyber security strategies and policies on the stages of developing and implementing a national cyber security strategy (NCSS). In the approach as a proposal, creating a NCSS, implementation and development method for Turkey with the organizational model that will accomplish this strategy has been proposed. The proposed models can be easily adapted and used by all countries. In Section 4, the significance of findings is briefly interpreted and described. Opinions, suggestions, and the outcomes achieved in this study are given in Section 5.

2. Methodology

The methodology of this study was based on the corresponding author’s ongoing Ph.D. thesis entitled “Turkey’s National Cyber Security Strategy and Policy Framework Creation of Deterrence.” In this context, publications of relevant institutions and organizations, especially academic publications, documents, books, magazines, library, and Internet environments were reviewed on the concepts of cyber space, cyber attack, cyber assault, cyber crime, cyber terrorism, cyber security, cyber defence, cyber warfare, cyber intelligence, cyber power, cyber security strategies/policies, and cyber deterrence, in addition to the activities (seminars, symposiums, and conferences); all are summarised in Table 1.

Based on literature, malicious actions and attacks in cyber space continue to increase day by day along with the technological developments in ICTs in the fields of processing, producing, storing, transmitting, and using data in all areas in parallel with the increase in efficiency and effectivity. In this context, it is inevitable to create and implement national cyber security strategies (NCSSs) and policies to ensure cyber security issues for countries due to the drastic increase in attacks and vulnerabilities. The literature survey is explained in two groups. The first group studies are as follows:

International Telecommunications Union (ITU) NCSS Guide prepared by Wamala [3] recommends governments to use all national power tools to reduce cyber risks, to prevent attacks, to handle the risks, and to remind national leaders of their responsibilities for preparing NCSS and policies for collaborating and managing cyber security issues properly.

NCSSs Good Practice Guide published by the European Network and Information Security Agency (ENISA) [4] states that European Union Member States should prepare NCSSs and recommendations about how to develop, apply, and maintain NCSS and keep improving the strategies and action plans for cyber security threats and attacks.

NATO Joint Cyber Defence Centre of Excellence (CCDCOE) established in Tallinn on May 14, 2008, pays attention to increasing NATO’s cyber defence capacity. Its main task is to strengthen the ability, cooperation, and information sharing among NATO

FIGURE 1: Components of cyber space.

TABLE 1: Inventory of books, documents, publications, and studies reviewed.

R. no.	Subject	Type	Quantity
1	Strategy and security	Books, documents, and studies	23
2	Cyber security and strategy	Books, documents, and studies	32
3	Countries' cyber security strategies	Documents and plans (US, China, Russia, France, Britain, Israel, India, North Korea, Germany, Canada, Netherlands, Finland, Japan, Australia, Iran, etc.)	18
4	Turkey's cyber security strategy	Documents and plans	17
5	Deterrence and cyber deterrence	Books, documents, and studies	30
6	Events on developments on the subject	Seminars, symposiums, and conferences	35

countries and their partners in the field of cyber defence, through education, research and development, lessons learned, and consultations. In the official website of the centre [5, 6], preparation and implementation of national cyber security strategies and policies, suggestions, training, exercises, expertise and consultancy aids, and studies on international legal regulations for cyber environment are located, besides the cyber security strategy documents of the member countries.

The first group studies from past to present cover many studies conducted by several state agencies and institutions in Turkey; the official documents prepared for the work were put into practice after their approval and publication. The relevant findings with some academic studies and documents related to the subject are as follows:

The most important dimension of cyber security at the national level is strategic management including strategic planning, and the first thing to do against cyber threats is a national cyber strategy document that should be prepared covering the strategic goals and the measures to be reached, as reported by Senturk [7].

Akyazi [8] has stated that cyber space, unlike other conflict areas, provides effectiveness for each of the national power elements; NATO's cyber security policy, US doctrines, and strategies of some countries are briefly summarised, in addition to putting forward measures to be taken in this context.

Küçükşille [9] has introduced the concept of information security with the widespread use of the Internet in the world; legal arrangements are made by the states in this context and cyber security strategies have started to be created, emphasizing principles that should be taken into consideration while developing a cyber security strategy.

Gungor [10] has reported that realization of the strategies produced to protect the critical infrastructure and information systems both in the public and private sectors is going through a corporate structure where they will work in coordination, but some kind of desired result could not be achieved because of the lack of legal infrastructure in this area, and the concept of information security is not fully understood due to a wrong conceptual framework in Turkey.

Within the scope of national cyber security strategies and policies, some of the important work and activities that started in Turkey in 2003, with the Prime Ministry Circular No. 2003/10 [11], are presented in Table 2. Documents related to these studies were examined separately during the thesis, deficiencies were detected in their preparation and implementation, and inadequacies have been revealed. We have also benefited from the current and past studies on how ideal NCSS and policies needed for Turkey should be prepared and implemented effectively. It can be clearly stated in the strategy that cyber security (defence) is discussed in detail related to cyber security strategies and policies; the documents are prepared and put into practice so far in

TABLE 2: Turkey's important cyber security strategy documents and plans.

R. no.	Subject	Responsible authority	Date
1	Information Society Strategy and Action Plan	Ministry of Development	2006–10
2	National Virtual Environment Security Policy	Ministry of Industry and Technology	2009
3	Turkey Cyber Security Organization and Roadmap	Ministry of Industry and Technology	2012
4	Cyber Security Board Formation	Ministry of Transport and Infrastructure	2012
5	National Cyber Security Strategy and Action Plan	Ministry of Transport and Infrastructure	2013–14
6	Information Society Strategy and Action Plan	Ministry of Development	2015–18
7	Personal Data Protection Law	Ministry of Justice	2016
8	National e-Government Strategy and Action Plan	Ministry of Transport and Infrastructure	2016–19
9	National Cyber Security Strategy and Action Plan	Ministry of Transport and Infrastructure	2016–19
10	Giving the task or taking all kinds of measures to provide cyber deterrence to the Information and Communication Technologies Authority	Ministry of Transport and Infrastructure	2016
11	Turkey Software Sector Strategy and Action Plan	Ministry of Development	2017–19
12	Presidential Circular on Information and Communication Security Measures	Presidency Digital Transformation Office	2019

Turkey. In the strategy, the other main dimension of cyber warfare was not addressed in the size of cyber attack, and the subject of “cyber deterrence” clearly did not find place, except for the issue of providing deterrence by legally fighting cyber crime [6]. Besides, the “cyber power” issue, which should be included among other national power factors and is necessary for cyber warfare, was not addressed; the issues of creating, developing, and using cyber power were not explained.

In the work entitled *Cyber Power* in [12], Nye states that countries also have the capacity to use hard and soft power in cyber space. Although a number of countries are very strong in land, sea, and air operations, Nye emphasizes that they may not show the same power and impact in the cyber space, and nonstate actors may also be effective in cyber space due to their asymmetric usage effects.

In *Cyberpower and National Security* by Kramer [13], it is stated that the cyber space has undergone extraordinary changes that offer both outstanding opportunities and major challenges for cyber space users; difficulties arise from malicious actors using cyber space and many vulnerabilities affecting this space; balanced knowledge is required in the cyber space in order to take advantage of opportunities and overcome difficulties. For the purpose of developing international partnerships to address cyber challenges in “cyber power and national security,” attention is drawn to the issues of building and using human capacity.

Haley, in *A Theory of Cyber Deterrence* [14], states that cyber deterrence differs from nuclear deterrence in many basic ways, and it is not possible for the application to eliminate the possibility of all attacks, no matter how effective it is, but it can play a critical role in reducing it to a manageable level at low cost.

US cyber security expert Libicki emphasizes the importance of military cyber power in [15]; the network-centred execution of the operation in the operational areas as the use of cyber power is referred to. Libicki claims that if the military cyber power is used in conjunction with other classical military power elements, it further increases the effectiveness of those forces. Libicki, in his book *Cyberdeterrence and Cyberwar* [16], states that providing deterrence in cyber space is different and much more difficult than classical or nuclear operation; it is possible and it can work, but it is bound by some terms and rules.

In the work of *Solution Architecture for Cyber Deterrence* by Mowbray [17], it is stated that the tools for distributed decommissioning, parallel scanning, exploration, surveillance, and other capabilities in addition to the network penetration tools of that country for a country's cyber deterrence strategy are effective. Mowbray emphasizes that the most important issue in cyber deterrence is that the country or the target of the cyber attack can be evaluated quickly and precisely.

Lupovici in his study, *Cyber Warfare and Deterrence* [18], questions whether deterrence can be achieved by states in cyber space. According to Lupovici, in order for deterrence to be successful through punishment, the abilities (capacity) of the deterrent, the reliability of the retaliation threat, and the retaliation threat must be announced to the attacker successfully.

In [20], Jensen states that deterrence in cyber space, in addition to traditional retaliation, does more legal action than traditional deterrence methods in the nuclear age of the cold war, and offers options such as making networks invisible, flexible, and

interconnected, while struggling to defend the networks and infrastructures of nations.

Thomassen's book, *Cyber Deterrence—A 21st Century Maginot Line* [21], emphasizes that ensuring cyber security is among the top threats faced by modern states. Thomassen states that the issue of securing cyber systems is considered to be the heart of national security; developing attack capabilities in cyber space should be sought while maintaining international cooperation in cyber space; cyber deterrence is one of these approaches.

Bendiek and Metzger, in their study *Cyberdeterrence Theory in the Cyber-Century* [22], state that the deterrence theory to protect against cyber attacks has long been considered as a valuable concept and that it is applicable in cyber space. They explained how the principles of classical deterrence can be applied in cyber deterrence, whether cyber abilities can be effective in deterring aggressive enemies, the idea that classical retaliation should be considered for deterrence, and implementation challenges of cyber deterrence.

Davis in [23] emphasizes that cyber attacks and cyber warfare are national security threats, deterrent efforts have failed in the past but can sometimes play a useful role, and academics and policy makers should avoid early conclusions about what actions in the international and legal fields can be beneficial.

Lindsay in [24] states that cyber attackers use their vulnerabilities to hide and deceive their identity, which leads to pessimism for success in cyber deterrence. Lindsay reports that the retaliation penalty is ineffective and that trusting the deception gives the attacker some advantages.

According to Singer and Friedman [25], deterrence is the ability to change an enemy's actions by changing cost and benefit analyses. The most important difference of cyber deterrence from deterrence in other environments is the problem of "against whom to deter or retaliate."

"NATO's Cyber Deterrence" [26] reports that NATO's mission in cyber space is solely for defence purposes, which includes protecting their networks and helping their allies in the context of cyber attacks; there is no chance to use cyber attack abilities with no ability to maintain reliable deterrence. In addition, it recommends that plans and preparations are made because it is possible to provide better protection of NATO missions and operations by treating the cyber space as operational field.

It is very difficult and sometimes impossible to test cyber security and deterrence strategies before implementing them. If they have not been tested in practice or are not experimental, the striking common feature of the theoretical studies on issues of cyber security, cyber warfare, cyber deterrence, etc. addressing strategies and policies is that they

lead to indecision and controversy over whether they can be effective in cyber space. The field of testing, trial, or implementation of the countries' cyber security strategies and policies is the cyber space that the countries have located and their people live in today. The most important ways and methods and the conclusions drawn from them with events and practices in the past and present will be put into practice with determinations and predictions regarding the future and needs.

3. National Cyber Security Strategy and Policy

National strategies are developed based on concepts, objectives, and resources and built up to manage those imbalanced issues and risks. The concept of strategy, whose meaning has expanded from the past to the present, has been used in many fields, including politics, economy, and culture, as a martial art term and is defined in dictionaries as "the main way to reach a goal." Today, it is accepted as a branch of science beyond the definition of martial art; various classes have started to be taught to all elements that make up business and social life, especially organizations and societies, at universities on different subjects, including strategic awareness and approach skills, determining the structure and activities of state administrations.

The definition of strategy is described in Turkey as "the science and art of a nation or a community of nations to use political, economic, psychological and military forces together to support policies adopted in peace and war" in [27]. Based on this, the definition of national strategy can be as follows: "it is the science and art of using the elements that make up the national power together in order to support national policies." Politics is also defined as "a whole set of decisions and actions to reach the determined goals or objectives" [28]. The nations identify national security politics and policies sometimes in secret and sometimes explicitly in order to implement them to ensure their countries' security.

This term is also clearly defined in the NATO Cyber Security Framework Guide as follows: "based on the common meanings of different terms and concepts related to the subject, cyber security is the fundamental basis for the protection of state secrets and the provision of national defence" [29]. International Telecommunication Union (ITU) defines cyber security as "the sum of tools, policies, security concepts, security measures, rules, risk management approaches, actions, training, best practices, and technologies used to protect the assets of institutions, organizations, and users in cyber space" [30].

The definitions clearly demonstrate that countries are aware of dangers of cyber space, pay more attention to cyber security issues due to cyber threats as one of the most important threats to national security, and consider it imperative to produce solutions to protect and secure the assets of individuals, institutions, and organizations against cyber risks, vulnerabilities, threats, and attacks. Understanding security, they have also changed the form, techniques, and methods of wars as a result of using cyber space for threats,

assaults, damage to life and property, etc. In this context, cyber warfare has emerged as a result of cyber assaults and attacks, leading to recognition of cyber security as an integral part of national security and as national security issue. Cyber war is stated as “including activities aimed at attaining information supremacy to harm political, military or economic information and information systems or to protect their own information and information systems” [31]. Cyber warfare by another definition is to attack the other party’s informatics systems or to slow down, disrupt, stop, disrupt, or seize information technology services to protect valuable assets in cyber space [32].

As in the classical definition of war in the military sense, one of the purposes of cyber war is to win the war by forcing another nation or a community of states to accept the request/s and to give up the action that they will carry out, as stated in the following quotes:

Sun Tzu, who lived in the 500s BC, states that “forcing someone to submit without war is the best” [2]

Belisarius, Eastern Roman Commander, said in the 500s AD that “forcing the enemy to give up its purpose without harming yourself” [33] may be better than winning a combat

Similarly, in cyber warfare, deterring the attacker from willingness, attack, or war, i.e., cyber deterrence, may be the best thing to do and the most excellent target to achieve. The term “deterrence” is described in dictionaries as “taking precautions to prevent and deter an aggression” [34], that is,

Avoiding committing a crime for fear of punishment or imprisonment in law terms [35]

Behaving to direct the other state to certain political behavior or dissuade its political desires in terms of international relations [36]

Persuading the enemy that the negative consequences of the oppression or armed conflict will be more severe than the earnings for him in the military field [37]

The common use of deterrence when an attack or war is concerned is that an enemy is guided over its estimate of the cost/benefit calculation to perform a specific action [38]. Libicki explains the deterrence in general terms as “intimidating the opponent not to take hostile actions” and defines cyber deterrence as “discouraging the attack by frustrating or punishing the action of the attacker in cyber space (threat of retaliation)” [16].

Based on various thoughts, approaches, and practices on cyber deterrence [1, 14–22], it is seen that the strategy on this issue generally consists of two basic classifications as indicated in Figure 2. Prevention/frustration aims to prevent attacks and actions and frustrate the attackers’ cyber security and defence capacity, further increased with its intelligence, detection and attribution, prevention, assurance, etc. In punishment, engagement, threats, and competencies are announced to the attackers, with the capability, ability, and policy support to show and retaliate to cyber attacks/assaults and give punishment by various sanctions.

Before going further, it needs to be emphasized that attacks are made or achieved in cyber space using cyber attacks and incidents carried out by small attack groups such as institution, organization, society, group/s, or person/s, located in open sources, printed and visual media, etc. from past to present, and targeted at loss of reputation, violating privacy, public or national interest, national and international security breaches, or other targets not explained here.

Besides deterring cyber criminals, terrorists, spies, hackers, or attackers preparing for cyber attack/war with cyber security/defence or counter-cyber attacks/war, stopping or directing noncyber environment activities of government, like civil or military formations along with other national power elements and sanctions, or only using cyber power, can be evaluated within the scope of cyber deterrence (Figure 3).

In the light of the above explanations, there have been a number of issues to be considered, defined, and achieved to support cyber deterrence:

Discouraging and pursuing attackers or hackers not to attack or hack the systems

Stopping any attack before it is done in cyber space

Finding a method of ensuring cyber security

Giving trust to users and fear to enemies

Executing cyber attacks or cyber defence at the right time, target, technique, and method

Developing and applying cyber security strategies and policies in order to minimize uncertainties

Determining exact time and target of cyber attacks/war

Performing right techniques and methods to defend the assets

Having advanced protection and using them

Being ready for any attack to defend the systems

As can be clearly seen from the explanation, deterrence requires advanced thinking, planning, preparation, protection, capability, and capacity.

The entire goal to protect national assets depends on the effective use of national power:

To achieve national objectives, interests, and targets

To ensure the survival and welfare of the country

To win wars in all areas or provide deterrence

National power might be a strategic approach and is defined as “total potential power of a nation with its material and spiritual values.” It consists of 7 different power elements [39], namely, man power, geographical power, economical power, political and administrative power, psychosocial power, scientific and technological power, and military power, to achieve its national interests and goals. “Cyber power,” whose importance has increased day by day after the development of technology and the fact that cyber space has become an indispensable part of life and become the 5th area of movement, is defined in [16] as “informatics systems and infrastructures that one has in cyber space and

FIGURE 2: Cyber deterrence strategy methods and techniques.

FIGURE 3: Deterrence targets and objective.

ability to use them effectively.” It may be more appropriate to describe cyber power, which means “domination of the cyber space,” as the 8th power element, instead of considering it under the scientific and technological power element, which is one of the national power elements as indicated in Figure 4.

When one examines the detail of cyber power, it can be seen that cyber power affects all other national power elements, can further increase their effects, and can be used effectively on its own. In terms of the size and methods of use of power, cyber power is also included in the soft power, which is manifested by the widespread use of technology and informatics systems, as well as hard power, which is based on military and economic power. It is evident that the cyber power of countries can be both an instrument of attack and a target of attack and that the parties can use their mutual cyber powers in order to harm each other, weaken their cyber powers, or disable some of their elements or capabilities.

In order to support the deterrence, national cyber security strategies should be created, developed, and implemented on the premise that cyber security is one of the most important components of national security in order to subdue one’s opponent first without combating in any war

or, if war is inevitable, to effectively use cyber power to win the war with a view to achieving national goals, protecting national interests, and ensuring the security of the country.

3.1. Developing and Implementing National Cyber Security Strategies and Policies. In general terms, national security strategies and policies of the countries are defined as “processes and elements which will enable the determination of the policy and the implementation of the most appropriate policies by monitoring the regional and global environment and identifying threats and opportunities to take measures against threats to the national presence, survival, and security of the state” [40].

Countries create and implement cyber security strategies and policies, as well as forming national security strategies and policies. The main and common goal of developing strategies and policies is to ensure security and defence of countries’ valuable assets, informatics systems, and infrastructures against cyber threats and attacks. As meant and defined in the cyber security strategy documents, it is necessary to determine the responsibilities including the deficiencies, negatives, and inadequacies against the harms and attacks in cyber space, to arrange the principles of

FIGURE 4: National power elements.

coordination and cooperation, and to manage comprehensive safety and defence issues.

It would be appropriate to establish comprehensive strategies and policies in the definition of national strategies based on the development, protection, and effective use of the cyber power of a country within a holistic approach similar to acting on the use of all power elements together for national policies. In this context, a new approach will be introduced to consider national cyber security and policies, and the guidelines and principles determined by examining the cyber security strategies and policies of some countries that are prominent in cyber space.

3.2. Overview of National Cyber Security Strategies and Policies in the World. Countries around the world continue to develop and strengthen their national strategies and policies incorporating cyber power, which comprises accumulation of their cyber defence and attack forces, into their national power that they can use to achieve their national interests and achieve their national goals. It is obvious that cyber power can be used to create an asymmetrical effect on national cyber security that affects this power negatively at various levels of dependence of informatics systems. Although there are no clear and concrete ways and methods to measure the cyber power of countries, it is seen that various studies have been carried out to determine the level of cyber power. In a study covering the USA, Russia, China, Iran, and North Korea in this respect, it was considered that North Korea is the country with the highest cyber power and ability due to its defence and dependency values, even though its cyber attack power is low as indicated in Table 3 [19].

As reported by Dennesen in iDefense 2011 Trends Report in [41], countries were classified into 4 groups according to their cyber power, cyber power capabilities, specific characteristics interpreted, and cyber security strategy and policy as indicated in Figure 5.

3.2.1. Countries in Group 1 (USA, China, and Russia). These countries have the following characteristics:

- (i) Have the ability to develop an international policy in addition to their cyber security and defence development efforts

TABLE 3: Evaluation of countries' cyber power and capabilities [19].

Countries	Cyber attack	Cyber defence	Cyber addition	Total
USA	8	1	2	11
Russia	7	4	5	16
China	5	6	4	15
Iran	4	3	5	12
North Korea	2	7	9	18

- (ii) Provide the most resources and human support to cyber security policies and cyber defence activities
- (iii) Have many well-defined and specialized military and intelligence agencies
- (iv) Are capable of carrying out comprehensive, continuous, and complex offensive and defensive actions against other countries

3.2.2. Countries in Group 2 (France, UK, and Israel). These countries have the following characteristics:

- (i) Closely follow the countries in Group 1 and have fewer personnel and more limited infrastructure
- (ii) Have numerous, well-defined, and specialized military and intelligence agencies but fewer resources
- (iii) Have the ability to carry out continuous and complex attacks and defence actions in a limited scope against a limited number of countries

3.2.3. Countries in Group 3 (India, South Korea, North Korea, Germany, Turkey, Taiwan, and Estonia). These countries have the following characteristics:

- (i) Allocate substantial resources to develop cyber security policies and defence capabilities
- (ii) Imitate the countries in Group 1 and Group 2 for many cases
- (iii) Have several well-defined institutions but have limited institutionalization
- (iv) Have comprehensive and continuous cyber defence capabilities but weak cyber attack capabilities

FIGURE 5: Situations of countries according to cyber power and capability [41].

3.2.4. *Countries in Group 4 (Brazil, Canada, Italy, Sweden, Netherlands, Finland, Japan, Australia, Pakistan, Iran, and South Africa).* These countries have the following characteristics:

- (i) Allocate limited resources to develop cyber security policies and defence capabilities
- (ii) Have fewer institutions that need improvement
- (iii) Have a cyber defence, which is strong but inadequate, and limited cyber attack activities
- (iv) Focus on protecting their own internal resources

3.3. *International Cyber Security Cooperation Principles.* In addition to domestic coordination and cooperation in ensuring the cyber security of a country, international cooperation, i.e., cooperation and coordination of countries, is of great importance. In this context, ITU, aiming to establish a synergy between current and future initiatives for countries within the framework of international multistakeholder cooperation in the preparation and implementation of national cyber security strategies and policies, attaches importance to the following main principles [3]:

- (1) Legal: measures based on the existence of legal institutions and frameworks related to cyber security and cyber crime
- (2) Technique: framework-based measures based on the existence of technical institutions and cyber security
- (3) Structural: measures based on the presence of coordination agencies and national cyber security development strategies and policies
- (4) Capacity Building: measures based on the existence of research and development, education and training programs, certified experts, and public sector organizations supporting capacity building
- (5) Cooperation: measured based on partnerships, collaborative entities, and the presence of information sharing networks

As a result of research carried out by ITU, countries have been evaluated and ranked according to these principles as reported in [42]. The top ten countries including England,

USA, France, Lithuania, Estonia, Singapore, Spain, Malaysia, Canada, Norway, and Australia are given in Table 4. Although the time period between the two studies is close to 10 years, the evaluation scales of countries and the evaluation results of some countries are similar.

3.4. *Steps for Creating and Implementing National Cyber Security Strategy.* Comprehensive national cyber security strategies have become important to avoid or manage dangers, vulnerabilities, targets, hackings, attackers, etc. that adversely affect individuals, institutions, and hence countries. Institutions work in this context and they prepare and publish guidelines, which include targets, actions, and suggestions in the preparation of a NCSS, while states develop national cyber security strategies in different ways and methods to make cyber space safer and more secure in achieving their national goals.

In the published guidelines, it is seen that the common approach of **PDCA (plan, do, check, and act)** cycle model [43], developed by Deming, has been followed for continuous improvement activities as given in Figure 6:

P (plan): plan development and improvement

D (do): plan implementation

C (check): check implementation and result

A (act): correct plan according to the deficiencies and improvements in the implementation

Security studies in all kinds of institutions and organizations are modelled with a lifecycle similar to the PDCA approach. After their creation, the strategies and policies applied are considered as specific laws, i.e., specifically monitored and developed for the organization, and the process continues as a lifecycle.

PDCA approach is also used to create, control, and continuously improve cyber security strategies and policies, and processes. Security work in all kinds of institutions and organizations is modelled with a lifecycle similar to PDCA approach. While the strategies and policies that are formed are considered to be laws specific to the organization, generally, similar processes are followed for each organization.

TABLE 4: ITU global ranking of countries in the field of cyber security [42].

Global Rank	Countries	Score
1	United Kingdom	0.931
2	USA	0.926
3	France	0.918
4	Lithuania	0.908
5	Estonia	0.905
6	Singapore	0.898
7	Spain	0.896
8	Malaysia	0.893
9	Canada, Norway	0.892
10	Australia	0.890
11	Luxembourg	0.886
12	Netherlands	0.885
13	Saudi Arabia	0.881
14	Japan, Mauritius	0.880
15	South Korea	0.873
16	Oman	0.868
17	Qatar	0.860
18	Georgia	0.857
19	Finland	0.856
20	Turkey	0.853
21	Denmark	0.852
22	Germany	0.849
23	Egypt	0.842
24	Croatia	0.840
25	Italy	0.837
26	Russia	0.836
27	China	0.828
28	Austria	0.826
29	Hungary	0.815
30	Sweden	0.814

FIGURE 6: PDCA cycle model and corporate cyber security lifecycle [43, 44].

In the guidelines reported by the European Network and Information Security Agency (ENISA) [45], it is stated that there are two main steps of managing a NCSS based on this approach:

- (1) Developing and implementing the strategy
- (2) Evaluation and maintenance of the strategy

In addition, three approaches can be adopted to create a NCSS:

- (1) Linear Approach: the strategy will be developed, implemented, evaluated, and eventually terminated (or replaced)

- (2) Lifecycle Approach: the output of the evaluation phase will be used to maintain and adjust the strategy itself
- (3) Hybrid Approach: several continuous improvement cycles on different levels may exist

It is seen that the most widely accepted approach in the preparation of national cyber security strategies is lifecycle approach. In this context, Figure 7 shows the lifecycle approach [4] proposed by ENISA with the aim of controlling and continuously improving the strategy and related policies as well as implementation through measures, actions, and processes. As shown in Figure 7, NCSS lifecycle consists of 4

FIGURE 7: ENISA NCSS lifecycle [4].

phases: the strategy is developed and implemented in Phases 1 and 2, and it is ensured that it is evaluated and maintained in Phases 3 and 4. The activities include both one-time and ongoing/periodic evaluations.

In recent years, there has been a guide including the approaches and suggestions by ITU in publications and studies on the implementation of cyber security strategies. Strategy lifecycle approach [46] in the NCSS Development Guide of ITU describing the steps to be taken by a country for the NCSS, possible structures and inclusive principles for its implementation according to its specific needs, and the essentials for its good implementation, is shown in Figure 8. As can be seen in the figure, the strategy lifecycle, which is aimed at guiding and focusing on strategic thinking about cyber security at the national level, consists of the following 5 stages: initiation, collection and analysis, production, implementation, and monitoring and evaluation. In the 5th stage, unless a decision is made to prepare a new strategy after the monitoring and evaluation process, the existing strategy is continued with adjustments.

Based on the information obtained from the **national cyber security strategy (NCSS)** documents of those countries that have prominence in the field of national cyber security and the information obtained from the work of some international institutions, it is clear that the NCSS should be structured in a harmonious and logical order according to the national policy/strategy principles and rolled out by working with scientific methods. Considering the existing strategies and action plans, **the NCSS**, whose **basic structure** can be seen in Figure 9, which is to be created as **a lifecycle in 8 stages**, is expected and proposed to achieve a high degree of success, especially in terms of effectiveness and deterrence.

3.4.1. Assessment of the Situation. This stage, the starting part of the cyber security strategy, involves a study that is similar to the estimation of situation, which is conducted to determine the most appropriate way of action by examining all factors related to the past, present, and future in order to best fulfill the task in military strategy. This study examines what has happened in cyber space from past to present and makes future predictions.

During the situation assessment, the current situation of the country in cyber security should be analysed by comparing it with the legislation of different countries and regional and international studies, and to this end examples of

countries that have developed successful national plans, programs, and legislation on cyber security should be used. In this context, some of the important studies that need to be examined and conducted are listed below in order of priority:

- (i) Issues affecting the NCSS, in particular issues related to the cyber security dimension of national politics and strategy
- (ii) Structuring the national cyber power
- (iii) Links of national power elements with cyber power and cyber security
- (iv) Important past and current cyber security events occurring in cyber space and their consequences
- (v) Future prospects for cyber security including technological developments in cyber space
- (vi) Strengths, weaknesses, and vulnerable sides of national cyber power
- (vii) Evaluation of cyber security opportunities, threats, and risks
- (viii) Current national and international laws and policies related to cyber security
- (ix) Analysis of the duties (duties and motivations for tasks) given to and/or removed from the use of cyber power

The success of the evaluation depends on the determination of all relevant factors and the fact that these factors are examined in a logical order in a realistic and detailed manner. Constitutions, issues of laws and international agreements, human rights and freedoms, etc. should be considered. As the factors affecting the studies change and new facts appear, the situation should be reviewed and new assessments and corrections should be made.

3.4.2. Setting the Target. The target, which means a place to be reached or a goal to be attained [47], must be achieved in order to release the task or the specified purpose in the sense of strategy. In the national strategy, a state's survival and the well-being of a nation [48] can be defined as tasks and goals; there are many goals for many areas and there may be many different ways and methods to achieve each goal.

Similarly, as a result of the assessment of the situation in the NCSS, many tasks and objectives can be put forward after the task is set in relation to the goal in stage 6, before

FIGURE 8: ITU NCSS lifecycle [46].

FIGURE 9: Proposal for creating a NCSS and implementation steps.

proceeding to stage 2, and there may be different goals for each of them which need to be realized. Instead of being used in a disintegrated manner to achieve different objectives for effective use, it should be directed to the goal that will perform the task or ensure the maximum gain in order for the task to take place. The main basis for this is the analysis of the duty, which is the expression of the purpose deduced from the task or duties resulting from the assessment of the situation. The target to be determined should directly or indirectly ensure or support the realization of all or majority of open or closed tasks and goals thereof after the analysis of the duty.

Based on these thoughts, the target in a NCSS can be determined as “maintaining and improving cyber power, being effective and successful with other power elements, or providing deterrence in all aspects of the cyber environment alone when necessary.” Even if it appears that such a target may not be achievable, attainable, or immeasurable, whether or not it has been attained, it should be noted that the important thing is the gains to be achieved by the agency to

be created and the elements included in the mandate thereof, in stages and at various times. However, the point to be considered here is that such a goal will change shape and position continuously over time, so the strategy will need to be improved continuously. Such hurdles as uncertainties, limitations, etc. related to the subject can be eliminated at the planning stage.

3.4.3. Organization, Duties, Powers, and Responsibilities. When NCSS entities are analysed, it is seen that countries are working for coordination systems and implementing the structures they have determined to ensure cyber security. As with the management systems and structures of the countries, there are differences in cyber security strategies and policies, especially in coordination of ensuring cyber security, due to the differences in informatics systems and infrastructures and their needs and expectations. The biggest similarity among them is that the paths and methods followed aim to ensure a strong coordination.

The protection of information, informatics systems, and infrastructures, which are the most valuable assets of the country, is a vital issue; in addition, its cost is high. Within the scope of cyber security, difficulties and costs will increase even more considering the dimensions of using cyber power more actively and effectively by ensuring the cyber space to be more reliable. In addition, coordination and cooperation are required not only in the country but also in the international arena.

However, it should be considered not only to coordinate national cyber security studies, but also to establish an institutional organization to manage this work and to ensure that cyber power is used and managed effectively from a single source. In the report prepared by the International Telecommunication Union (ITU) in 2008, it is stated that this task can be fulfilled by a high level government authority, which will be established under the name of “National Cybersecurity Council” in Figure 10, which can provide coordination and guidance for relevant institutions [49].

Although the responsibilities of cyber security strategies and policies are widely distributed in the USA, the highest level of coordination responsibility is fulfilled by the Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC), affiliated to the Presidency National Security Council, National Security Council, and Cyber Security Coordinator. It is managed by CSC [50]. In the Russian Federation (RF) the structure, power, duties in relation to the creation and implementation of the cyber security strategy, which is considered an important part of the national security system in the Russian Federation, are handled within the framework of the power and responsibilities of the State Duma, government, security council, executive bodies, Central Bank, and Military-Industrial Commission [51]. In China, coordination and implementation of cyber security are fulfilled by the Ministries of Public Security, State Security, and National Defence [52].

In this context, Cyber Security Council was established in 2012 under the direction of the Ministry of Transport, Maritime Affairs and Communications (UDHB) with the participation of 11 member senior executives listed below representing ministries and other relevant public institutions and organizations in order to determine the measures to be taken in relation to cyber security in Turkey, to approve the prepared plans, programs, reports, procedures, principles, and standards, and to ensure the implementation and coordination of them [53].

Turkey's National Cyber Security Council:

Chairman: The Minister of Transport, Maritime Affairs and Communications:

- (1) Undersecretary of the Ministry of Foreign Affairs
- (2) Undersecretary of the Ministry of Interior
- (3) Undersecretary of the Ministry of National Defence
- (4) UDHB Undersecretary
- (5) Chief of General Staff Communications, Electronics and Information Systems

- (6) Undersecretary of the National Intelligence Agency (MIT)
- (7) Undersecretary of Public Order and Security
- (8) President of the Scientific and Technical Research Council of Turkey
- (9) President of Information and Communication Technologies Authority
- (10) President of the Financial Crimes Investigation Board
- (11) President of Telecommunications Communication (was closed on 15 August 2016)

The fourth meeting of the said committee, whose effectiveness is being discussed, was held in 2016 and the need to “establish a strong central public authority to ensure coordination in the field of cyber security” [6] was emphasized in the 2016–19 NCSS and Action Plan published after the meeting.

In order to comply with the amendments made in the constitution, the duties of the Cyber Security Council have been transferred to the presidency with the Decree Law No. 703 of 09 July 2018 [54]. Although some cyber security-related duties and responsibilities are carried out by the Office of Digital Transformation of the Presidency, there is still a multiheaded organization in terms of the competent, responsible, and coordinating unit.

Although the primary duties, power, and responsibilities of institutions and organizations at all levels are determined by laws and regulations, there are areas that are left incomplete and ineffective in terms of national security; also, there are repetitions and confusions in terms of cyber security. “Integration of cyber security into national security” [6], which is one of five important actions in the 2016–2019 NCSS and Action Plan and is vital to national security, is also one of them.

For managing national cyber security and in order to meet the need for a strong public authority to ensure coordination in cyber security and to eliminate uncertainties related to the issue, an effective organization, which will be responsible for all aspects of the country's cyber security and serve as the “Cyber Army Command Headquarters” in the country's 5th Operational Domain, cyber space, should be established. As a suitable way of solution for this, **National Cyber Security Presidency (NCSP)** can be established by taking the example of an organization similar to the National Intelligence Agency Presidency (NIAP) affiliated with the presidency. The main organizational structure of the NCS Presidency as an exemplary state style is presented in Figure 11, not only for Turkey but also for the other countries and other governments.

The organization structure given in Figure 11 is suggested for other countries and governments having the NCS Presidency: 7 departments, an operation centre, and an office of the undersecretary. With this organization structure, the presidency shall be responsible for the development of national policies and strategies related to cyber security, carrying out planning and coordination studies (Department of Planning and Coordination), defence, assault and

FIGURE 10: ITU National Cyber Security Coordination Council [49].

FIGURE 11: Proposal for structuring of national cyber security presidency.

deterrence, and the execution of all such operations, including cyber intelligence (Department of Intelligence and Operations), responding to cyber incidents including cyber security crisis management (Operations Centre), cyber security of critical infrastructures (Department of Critical Infrastructure Security), ensuring international cooperation and coordination (Department of International Cooperation), meeting training and exercise needs and coordinating and directing the training of cyber security experts (Department of Training and Exercise), guiding cyber security technology research and development studies (Department of Technology), carrying out any kind of support, control, and audit activities related to cyber security and similar activities (Department of Control and Supervision), and the performance of duties of the president and judicial duties (Legal Counsellor) related to cyber security.

The President of NCS (under the presidency) will also preside over the proceedings of the **Cyber Security**

Coordination Council (C3), which will be created with the participation of authorized representatives of relevant public institutions and organizations as in the case of Cyber Security Council, which was established in 2012 and later its duties were transferred to the Office of President in 2018. NCSP will act as an approval and coordination committee rather than a decision-making body, but will also work to set strategic goals and policies in the field of cyber security when required and requested by the NCSP.

It will be ensured that the cyber security strategies and policies to be prepared under the responsibility and coordination of the NCS are examined and discussed by C3 and put into practice after its approval, and that they will be developed according to current conditions in case of need. The Cyber Security Operations Centre will also serve as the National Cyber Incidents Response Centre. In full coordination with the Department of Cyber Intelligence and Operations and the Turkish Armed Forces (Cyber Defence

Command), NIAP, Gendarmerie General Command, and General Directorate of Police, Presidency of NCS shall together with other institutions or alone prepare and implement cyber security and all kinds of cyber attacks and deterrence operations when necessary, in addition to cyber security and defence related task.

3.4.4. Scope, Duties, and Responsibilities. Starting from a single individual in a country to all private (real) and legal entities and public or private institutions and organizations, the NCSS covers all entities and components that use cyber media. In the cyber space, absolute security is not possible, nor is it possible to ensure the same level of cyber security of all assets and components. In order to use the cyber security force and capacity effectively, the importance and priorities should be determined.

In this part of the cyber security strategy, all state levels, including all persons and public/private institutions and organizations that fall within the scope, should be identified by specifying their duties and responsibilities in general. For an individual using cyber space, personal cyber security is primarily their own responsibility. However, the state also has a duty and responsibility to provide training and awareness on this issue. When it comes to the country's cyber defence, even a single individual may have actions and things to contribute.

Protection of the informatics systems of the country's critical infrastructures should be at the top of the state's cyber security priorities. However, the public/private sectors that own these infrastructures will also have duties and responsibilities to fulfill. In this regard, duties and responsibilities should be determined, control and audit principles and sanctions should be identified, and plans and regulations should be made for this purpose.

In the cyber space, it is known very well that absolute security ensuring the same level of cyber security of all assets and components is not possible. In order to use the cyber security force and capacity effectively, the importance and priorities should be determined.

In this part of the cyber security strategy, all state levels, including all persons and public/private institutions and organizations that fall within the scope, should be identified by specifying their duties and responsibilities in general. For an individual using cyber space, personal cyber security is primarily their own responsibility. However, the state also has a duty and responsibility to provide training and awareness on this issue. When it comes to the country's cyber defence, even a single individual may have actions and things to contribute.

First of all, to dissuade the attack, i.e., to provide a strong cyber security and defence based on the idea of cyber deterrence and especially the protection of informatics systems of the country's critical infrastructures, should be ranked at the top of cyber security priorities. However, the public/private sectors that own these infrastructures will also have duties and responsibilities to fulfill. Planning must be made including measures and manners of actions, where the attackers will fail in the event of any attack, the cost will be

high, and also punishment is necessary for retaliation. For achieving this, the following are considered:

Infrastructures should be established in relation to this matter

Capacity and capability should be built up and capabilities available should also be improved

Duties and responsibilities should be determined

Control principles, auditing procedures, and sanctions should be specified

Plans and legal arrangements should be made for this purpose

3.4.5. Planning. In this part of the created NCSS, the modes of action towards the goals are considered to be achieved during assessment of the situations and goals supposed to be acquired during determination of the targets, and the objectives of tasks are examined. In order to implement the decisions made after the examinations, necessary plans are made and accomplished with the cyber security agency or the relevant state departments and public/private institutions and organizations under its responsibility and coordination.

In the implementation step, it is better to answer the simplest questions (5W1H) for better management:

Who?

Why? For what purpose?

When? How long?

Where?

How?

What will be done?

These should be answered during the transformation of realistic decisions into plans based on real data.

The motto of "**Safety First, Movement Next!**" which is frequently used in military activities and especially in hazardous work areas might also be an important principle in cyber security. Based on this principle, planning is a priority in defence. Planning to establish and operate national cyber incident response systems (cyber incidents response centre/teams, etc.) to counter cyber attacks and incidents is made primarily. In this context, detailed plans must be made first to ensure their cyber security by extracting inventory of the informatics systems of critical infrastructures that make up the largest and most important part of the country's cyber power.

Plans for all kinds of cyber operations should be prepared for protection against cyber attacks, crisis management, retaliation when necessary, cyber intelligence and counterintelligence, cyber defence, assault, deterrence, etc. In addition to the stand-alone use of cyber power, the plans should have the option to coordinate or to support the plans of government agencies and public or private institutions/organizations responsible for managing other power elements. The control and audit activities to be carried out in the process must be done effectively, and the goals set out in

the strategic plans must be associated with objective and measurable indicators before proceeding to the implementation phase. It should be noted that the plans are not contrary to the constitution and laws, international treaties, and obligations.

3.4.6. Implementation. As with all strategies, one of the most important parts and stages of cyber security strategy is the implementation phase. Because, even though the plans are the most perfect work that includes the perfect and best action style, their success depends on their implementation. In history, since most plans that promised success and victory on paper or thought were either not implemented or implemented correctly, the expected objectives could not have been attained and the goals could not have been achieved.

The plans may be centrally made and implemented by several entities, ranked based on the duties and responsibilities in the matter and implemented by the same entities. Among the other important issues in the implementation of the plans are complying with the confidentiality rules and timing, making necessary adjustments and changes in time to eliminate the problems arising from the application, not delaying the updates of the plans to be implemented, etc.

Success in cyber security is a holistic approach and decisive practice. At the level where the plan is implemented, all elements of the institution or organization, especially the management level, should own the plan, and each employee of the agency should completely fulfill their duties and responsibilities. As in all informatics systems, since all cyber security plans are run by staff, the principle that the weakest link in the security chain is the human element should not be forgotten.

If necessary, detailed follow-up and control activities should be carried out on the basis of person, system, and even device in order to fulfill the duties and responsibilities in the implementation of the plans. Whether activities are carried out by designated person/persons in methods and times should be closely monitored, the results must be followed, necessary measures should be taken according to instant and periodic assessments, deficiencies should be corrected without delay, all training needs, if any, should be met, successes should be recognized through awards, and failures, incompetence, and negligence, etc. should be subject to sanctions based on penalties.

3.4.7. Control and Supervision. Whether the plans are implemented as scheduled or the targets to be reached in the sixth stages have been achieved, how much has been achieved, how much gains have been made, or how much efficiency is received is determined by control and check activities. This section is briefly the stage involving systematic monitoring, control, auditing, and reporting of the strategic plan implementation.

Scientific control and inspection activities should be carried out based on advanced statistical data and criteria (standards), the implementation results of the plan should be measured by comparing them against the goals and

objectives, and the consistency and appropriateness of the said goals and objectives should be analysed. The importance of this issue is emphasized by the Austrian management science expert Peter Drucker in his following statement: "It is not possible to manage what you cannot control and you cannot control what you cannot measure!" [55].

Control and audit activities are carried out in the forms of internal and external action plans. Internal audit and control activities should be carried out by the senior management with the levels of implementing plans, and external audit activities should be carried out in accordance with the action plans to be prepared by the relevant boards of the NCSS management or the authorized units determined by them.

Control and audit action plans must include the following:

- Control forms and standards

- Tasks to be performed

- Objectives and targets to be achieved by responsible persons, groups, or units, and so on

Audit activities should be carried out impartially, and their results should be compared with the results of previous audit and control activities and presented in objective reports. Areas that have been progressed and cannot be achieved, goals that are reached, and goals that are unreachable must be specified, and necessary assessments should be made to be used in subsequent improvement and development activities.

3.4.8. Development. This phase is the most important one and the last part of creating a cyber security strategy. From the holistic point of view, it is generally a cyclical process, and plans are made in this context. In the process, plans and strategies are reviewed using the information in the reports prepared as a result of control and inspection activities, comparing the targeted and achieved results.

The reasons for the differences and deviations between the planned activities and the application are investigated. Errors, mistakes, deficiencies, and inadequacies identified in practice and all the issues considered positive are examined together with the evaluations of the audit experts. Investigations are initiated to eliminate problems, and work is initiated to incorporate positive aspects into the planning.

These efforts consist of the activities of reviewing, reorganizing, and updating the studies in the situation, organization, scope, and planning departments, which take place in the first four stages of forming the strategy. The NCSS is improved by maintaining the cycle in this way. Conducting the development work by all relevant management levels and boards without interruption with due care and diligence would also contribute greatly to the training and the formation of a corporate culture.

4. Discussion

It is observed that in parallel with developments in computer and communication technologies nowadays, the variety,

severity, numbers, and technical complexity of cyber attacks that can be made by persons, groups, and states capable of conducting attacks within or outside the organization or the country, criminal organizations, terrorists, hackers, spies, and so on increase, while the expertise and skill of the attack, i.e., the attackers' knowledge levels and expertise [49], have been gradually lessened. Parallel to this threats, risks and damages which may be caused as a result of attacks increase, while attacks have become difficult to detect and prevent.

Also in this study when cyber attacks and incidents in many countries were analysed, it was observed that the common fundamental reasons for the higher impacts and damages are the following:

- (1) Laws and policies related to cyber security being not sufficient or not implemented effectively
- (2) Technology and infrastructure inadequacies and lack of knowledge and preparedness against attacks
- (3) Lack of training and awareness of users and lack of coordination and cooperation between institutions and organizations, etc. [56]

Cyber security is a national security issue now and should be integrated into national security. For all the reasons stated above, it is evident first of all that the elimination of the issues and problems faced can be achieved through the creation and implementation of the NCSS without any delay. Drafting a NCSS first requires a solid understanding of basic concepts on cyber space and a consensus on related terminology. The NCSS should be established on the basis of national policy/strategy and developed through efforts based on scientific methods.

As an approach style (proposal), "**8 stages of organization**," scope, planning, and implementation must be monitored, from assessing the situation to achieving the goal, control and inspection activities, and development activities in the process, scientific tactics and techniques can be carried out as a lifecycle (**proposal for creating a NCSS and implementation steps**).

The situation should be evaluated in detail; tasks should be analysed according to national laws, policies, and strategy; and strategic goal(s) should be determined objectively. As the importance of cyber security is understood, the importance of cyber power should also be understood, and it should be ensured that it is properly configured and developed. Because in cyber security strategy, the target can be achieved with cyber power, cyber power should be included in the national power elements, the necessary attention should be given, and its development should be ensured. In this context, the link between, and harmonization of, the national security strategy and cyber security strategy must be ensured.

Cyber security is not the task and responsibility of a single person, government/civilian institution, or organization. Everyone and all institutions and organizations at all levels have cyber security duties and responsibilities. However, a strong central public (government) authority is essential to ensure management and coordination in the cybersecurity field. A strong and authoritarian organization

that can provide effective coordination and one-stop management among the relevant institutions in the country should be established as one of the most important issues that will ensure the cyclical success of the strategy to be developed (**proposal for structuring of National Cyber Security Presidency, NCSP**). This agency should have the authority and power to execute and handle all types of cyber operations to be carried out in cyber space, including those related to defence, assault, and deterrence, as well as all kinds of cooperation, support, control, and inspection activities related to cyber security and to ensure national security in coordination with other national power elements.

The NCSS should cover all private and legal entities and public or private institutions, organizations, and components, starting from a single individual in a country. Duties and responsibilities should be determined in this regard; planning and administrative and legal arrangements should be made for this purpose.

Plans may be made centrally and applied individually, or they may be made by staff and organization levels, which have duties and responsibilities in this regard, and be implemented by the same entities. Although plans are the most perfect work that includes the perfect and best action style, it should not be forgotten that its success depends on correct implementation thereof.

During the process, the work should be checked and inspected frequently, necessary evaluations should be made by comparing the targeted and achieved results, plans should be renewed, and the strategy implemented should be improved. For success, NCSP, which is supported by law and is strong in terms of staff, organization, and materials, should be established and should work in harmony and intensively with C3.

As previously emphasized, it is very difficult and sometimes impossible to test cyber security and deterrence strategies before implementing them. In this study, we have benefited from the past and present events and applications as well as the lessons and methods learned from them. Successful results of the study will be seen with the application of NCSS; NCSS will be developed, and the study can be updated according to the results of the application. In addition, according to these results and developments, users or related researchers/academics will be able to benefit from the study.

In today's world we see comments like the following: the attackers have so far not used their most advanced cyber weapons not to reveal their true capabilities, the consequences of a full-scale cyber war cannot be predicted, and what could happen could destroy a modern country [19]. It is of vital importance to have a secure cyber space and a cyber power that will also provide deterrence. It should not be forgotten that what is fundamental and important in cyber deterrence is the execution of cyber attacks/war at the right time, on the right target, and with the right techniques and methods [56]. If victory is desired in the event of cyber warfare, a holistic approach, addressing cyber security in all its dimensions, should be adopted and a more effective and deterrent NCSS should be developed, created, and implemented with determination.

5. Conclusions

In this paper, a new national cyber security strategy covering the deterrence perspective from creation to implementation was introduced for the first time. The outcomes can be concluded as follows:

A flowchart covering 8 steps to create and implement a NCSS, which may be used by all countries, has been introduced

The proposed steps introduced in this article might bring a number of issues to support cyber security and defence in a different perspective

The proposed organization (National Cyber Security Presidency) might help to efficiently and effectively handle the issues for better management, control, and auditing for cyber security issues

The information obtained from NCSS documents of those countries has prominence in the field of national cyber security

The existing strategies and action plans of basic structure (given in Figure 9) are expected to achieve a high degree of success, especially in terms of effectiveness and deterrence

We explained the importance of cyber power, which needs to be considered as one of the national power elements, and the importance of providing security against cyber attacks with deterrence by cyber power

An integrated approach for creating and implementing a NCSS and an authoritarian organizational structure responsible for the strategy might help to reveal the contribution of the proposed strategy

It can be finally concluded that the proposed strategy, steps, and suggestions might help to improve cyber security issues and national strategies in near future to secure national assets more than ever with a powerful concept of deterrence. Also, it is expected that this approach, which has been put forward for the effective implementation of cyber security by ensuring better management, control, and supervision, can be used as a NCSS or be integrated into available strategies and policies of countries.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors thank Prof. Dr. Seref Sagiroglu, Head of the Department of Computer Engineering at Gazi University, for his support and contributions to the preparation of this article.

References

- [1] M. Goodman, *The Crimes of the Future the Dark Side of the Digital World*, TIMAS Press, Istanbul, Turkey, 2016.
- [2] S. Tzu, *The Art of War*, T. Is Bankasi Kultur Press, Istanbul, Turkey, 2016.
- [3] F. Wamala, *The ITU National Cybersecurity Strategy Guide-2011*, ITU, Geneva, Switzerland, 2012.
- [4] ENISA, *NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies*, ENISA Publications, Heraklion, Greece, 2016.
- [5] NATO CCDCOE, "Cyber security strategy documents," <https://ccdcoe.org/library/publications/tracing-opinio-juris-in-national-cyber-security-strategy-documents/>.
- [6] T. R. UDHB, *2016–2019 National Cyber Security Strategy and Action Plan*, UDHB Publication, Ankara, Turkey, 2016.
- [7] H. Senturk, "Cyber security analysis of Turkey," *International Journal of Information Security Science*, vol. 1, no. 4, 2012.
- [8] U. Akyazi, "Measures that can be taken within the scope of international cyber security strategies and doctrines," in *Proceedings of the 6th International Cyber Security and Cryptology Conference*, Ankara, Turkey, 2016.
- [9] U. Küçüksille, "Cyber security strategies in the world and formation of a cyber security strategy," in *Proceedings of the 1st International Symposium on Digital Forensics and Security*, Elazığ, Turkey, 2013.
- [10] M. Gungor, "National information security: strategy and institutional structuring," Specialization thesis, Information Society Administration Publication, Ankara, Turkey, 2015.
- [11] T. R. Prime Ministry, "Security culture for information systems and networks," Prime Ministry Generation No. 2003/10, Ankara, Turkey, 2003.
- [12] J. S. Nye, *Cyber Power*, Belfer Center for Science and International Affairs, Cambridge, MA, USA, 2010.
- [13] F. D. Kramer, *Cyberpower and National Security*, NDU Press, Washington, DC, USA, 2011.
- [14] C. Haley, "A theory of cyber deterrence," <https://www.georgetownjournalofinternationalaffairs.org/online-edition/a-theory-of-cyber-deterrence-christopher-haley>.
- [15] M. C. Libicki, "Military cyberpower," <https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-11.pdf?ver=2017-06-16-115053-350>.
- [16] M. C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Corporation, Santa Monica, CA, USA, 2009.
- [17] T. J. Mowbray, "Solution architecture for cyber deterrence," <https://www.sans.org/reading-room/whitepapers/legal/solution-architecture-cyber-deterrence-33348>.
- [18] A. Lupovici, *Cyber Warfare and Deterrence*, Military and Strategic Affairs, Tel Aviv, Israel, 2011.
- [19] R. A. Clarke and R. K. Knake, *Cyber War*, Istanbul Kultur University Press, Istanbul, Turkey, 2010.
- [20] E. Jensen, Talbot cyber deterrence, Emory International Law Review 773, 2012, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2070438.
- [21] T. Thomasen, "Cyber deterrence—A 21st Century Maginot Linen," <http://www.fak.dk/publikationer/Documents/Cyber%20Deterrence.pdf>.
- [22] A. Bendiek and T. Metzger, "Cyberdeterrence theory in the cyber-century," https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf.
- [23] P. K. Davis, *Deterrence, Influence, Cyber Attack, and Cyberwar*, NYU International Law And Politics Journal, New York, NY, USA, 2015.

- [24] J. R. Lindsay, "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack," *Journal of Cybersecurity*, vol. 1, no. 1.
- [25] P. W. Singer and A. Friedman, *Cyber Security and Cyber Warfare*, Buzdagi Press, Ankara, Turkey, 2015.
- [26] P. Pernik, "NATO's Cyber Deterrence," <https://www.icds.ee/publications/article/natos-cyber-deterrence/>.
- [27] TDK Dictionaries, "Strategy," <https://sozluk.gov.tr/?kelime=strateji>.
- [28] TDK Dictionaries, "Policy," <https://sozluk.gov.tr/?kelime=politika>.
- [29] A. Klimburg, *National Cyber Security Framework Manual*, NATO Press, Tallinn, Estonia, 2012.
- [30] ITU-T, *Overview of Cybersecurity*, Recommendation ITU-T X.1205, Geneva, Switzerland, 2009.
- [31] UNTERM, "Cyber warfare," <https://unterm.un.org/UNTERM/display/Record/UNHQ/NA/c263537>.
- [32] S. Sagioglu, "Cyber security and defence: importance, definitions and precautions," in *Cyber Security and Defence—Awareness and Deterrence*, vol. 1, pp. 21–45, Grafik Press, Ankara, Turkey, 2018.
- [33] B. H. L. Hart, *Strategy Indirect Approach*, TGS ATASE Press, Ankara, Turkey, 1973.
- [34] TDK Dictionaries, "Deterrence," <https://sozluk.gov.tr/?kelime=caydiricilik>.
- [35] Z. Kizmaz, "Deterrent effect of criminal or criminal sanction on crime rates," *Afyon Kocatepe University Journal of Social Sciences*, vol. 7, p. 215, Afyonkarahisar, Turkey, 2005.
- [36] H. Ozdemir, "A power-multidimensional assessment in international relations," *Ankara University Journal of Political Sciences*, vol. 63, no. 3, pp. 128–139, Ankara, Turkey, 2008.
- [37] MS 76-3 TAF Joint Military Terms Dictionary, *Deterrence*, TGS Press, Ankara, Turkey, 2010.
- [38] A. Long, *Deterrence from Cold War to Long War*, RAND Corporation, Santa Monica, CA, USA, 2008.
- [39] E. Mutercimler, *Strategic Thinking to Manage and Think the Future*, Alfa Press, Istanbul, Turkey, 2006.
- [40] NSC Secretary General, *General Information on the National Security Council and the Secretariat General of the National Security Council*, <https://www.mgk.gov.tr/index.php/kurumsal/hakkimizda>.
- [41] K. Dennesen, "Latin American cyber threat landscape and 2011 trends," iDefense 2011 Trends Report, <http://www.cu.ipv6tf.org/lacnic15/LACNICV3.pdf>.
- [42] ITU, *Global Cybersecurity Index 2018*, ITU Publications, Geneva, Switzerland, 2019.
- [43] R. Moen, *Foundation and History of the PDSA Cycle*, https://deming.org/uploads/paper/PDSA_History_Ron_Moen.pdf.
- [44] M. Tekerek, "Information security management," *KSU Journal of Science and Engineering*, vol. 11, no. 1, pp. 132–137, 2008.
- [45] ENISA, *National Cyber Security Strategies Practical Guide on Development and Execution*, ENISA Publications, Heraklion, Greece, 2012.
- [46] ITU, *Guide to Developing a National Cybersecurity Strategy*, ITU Publications, Geneva, Switzerland, 2018.
- [47] TDK Dictionaries, "Target," <https://sozluk.gov.tr/?kelime=hedef>.
- [48] M. Erendil, *National Strategy and National Power*, *Armed Forces Magazine Supplement*, TGS ATASE Press, Ankara, Turkey, 1980.
- [49] ITU, "ITU global cybersecurity agenda high-level experts group global strategic report," ITU, Geneva, Switzerland, 2008.
- [50] A. J. Peritz and M. Sechrist, *Protecting Cyberspace and the US National Interest*, Belfer Center for Science and International Affairs, Cambridge, MA, USA, 2010.
- [51] Security Council of the Russian Federation, *Doctrine of Information Security of the Russian Federation*, http://www.scrf.gov.ru/security/information/DIB_engl/.
- [52] The People's Republic of China Information Office of the State Council, *The Diversified Employment of China's Armed Forces—China Defence White Paper*, https://media.nti.org/pdfs/China_Defense_White_Paper_2013.pdf.
- [53] Official Gazette, "Decision regarding execution, management and coordination of national cyber security studies," http://www.resmigazete.gov.tr/eskiler/2012/10/2012_1020-8.htm.
- [54] Official Gazette, "Transfer of the duties of the removed boards with decree no. 703 to the presidency," 2018, <https://www.resmigazete.gov.tr/eskiler/2018/08/20180802-2.pdf>.
- [55] A. Weber and R. Thomas, "Key performance indicator," <http://www.plant-maintenance.com/articles/KPIs.pdf>.
- [56] M. Senol, "Deterrence by cyber power but how," *International Journal of Information Security Engineering*, vol. 2, no. 2, pp. 10–17, 2016.