2017

From the National Cyber Maturity to the Cyber Resilience: The Lessons Learnt from the Efforts of Turkey

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Unal Tatar

From the National Cyber Maturity to the Cyber Resilience: The Lessons Learnt from the Efforts of Turkey

Bilge KARABACAK[a,1] and Unal TATAR[b]
[a] *Graduate School of Informatics, Middle East Technical University, Ankara, Turkey*
[b] *Business Administration Department, Yildirim Beyazit University, Ankara, Turkey*

Abstract. In this paper, the details of critical infrastructure protection program of United States of America are shared by taking the cyber resilience into account. The academic and institutional studies on the concepts of cyber maturity, critical infrastructure protection program and cyber resilience are explained in detail. By the help of these studies and national efforts, the relations among these concepts are proposed. The key components of a cyber security strategy and action plan for a cyber resilient society is proposed by taking these three concepts into account. As the final step, the recent cyber security efforts of Turkey is shared with the reader and assesses according to the determined key components.

Keywords. Critical Infrastructures, Critical Infrastructure Protection, Cyber Resilience, Cyber Maturity, Cybersecurity Strategy

1. Introduction

Critical infrastructures are vital assets for public safety, economic welfare and/or national security of countries. In recent years, both government officials and academia work through the damage potential of cyber war to critical infrastructures. Most of the developed countries have governmental/national critical infrastructure protection programs. All of the critical infrastructure protection programs take the consequences of cyber threats and/or a possible cyber war into consideration. Turkey has such a critical infrastructure protection program as well. By looking at the results of the two-year cyber efforts in Turkey, it can be seen that the success of critical infrastructure protection program is directly related to the level of the national cyber maturity. The second finding is the relation between critical infrastructure protection program and cyber resilience. A successful critical infrastructure protection program will result in a resilient society against cyber threats and cyber war. In this regard, critical infrastructure protection program stands between national cyber security and cyber resilience in the context of cyber war.
Firstly, national cyber maturity is a must-have baseline for the success of critical cyber efforts of Turkey; especially the ones that require the cooperation between different types of organizations. The critical infrastructure protection program will be left

[1] Corresponding author, Graduate School of Informatics, Middle East Technical University, Ankara, Turkey; E-mail: e171018@metu.edu.tr

unfinished and be condemned to fail without sufficient level of the national cyber maturity. The most important subjects of national cyber maturity are individuals and organizations. There are vital technical and organizational efforts that will create or increase the cyber maturity of individuals and organizations within a country and will result in cyber maturity of a country. There are good practices in Turkey for this goal. These efforts will definitely take some time in order to be internalized by individuals and organizations, also these efforts need to be measured and assessed in order to take consecutive actions.

Secondly, cyber resilient society is a result of a successful critical infrastructure protection program. Once a countrywide and strategically embraced critical infrastructure protection program is succeeded, the effects of this program will penetrate into the organizations, individuals and society by taking some technical or organizational actions like awareness activities, exercises and new coordinator bodies. So that cyber resilient society will emerge. Therefore, national cyber maturity is a prerequisite to a successful critical infrastructure protection program. In the same way; critical infrastructure protection program is a prerequisite to cyber resilient society. Although it seems like the efforts pertaining to these three concepts are sequential, they should be iteratively completed. As an example, the output of critical infrastructure protection program may provide useful inputs to national cyber security efforts.

This article will focus on both technical (IT) and organizational/policy (public and private sector) aspects of cyber security. In order to build a cyber-resilient society to cyber warfare, best practices will be shared with the government officials and researchers.

2. Background

At this section, firstly, the term critical infrastructure is defined and the brief history of the term is shared. Secondly, the use of cyber systems in critical infrastructures and the rise of cyber threats are depicted with examples. Thirdly, the terms critical infrastructure protection and cyber resilience are explained by giving example from United States of America. Fourthly, the studies that explore the cyber maturity and cyber readiness are summarized.

2.1. Cyber Systems and Cyber Threats as Enablers

Any physical or cyber infrastructure is called critical infrastructure, if damage to that infrastructure will have a harmful effect on economy of the country, social order and/or national security [1]. The term critical Infrastructure is first used within the Executive Order of President of United States in 1996 [2]. The purpose of the order was to introduce the term “Critical Infrastructure Protection”, to define the problem and to establish interim commissions in order to recommend comprehensive strategies and amendments to the existing laws in order to protect critical infrastructures. Executive order mentioned two types of threats against critical infrastructures; physical threats and cyber threats. Although, critical infrastructures exist long before the widespread use of cyber technologies and Internet prevalence; the Critical Infrastructure Protection is defined as an important governmental term because of dominant use of cyber systems in infrastructures that serve society. There are two reasons for this. Firstly, cyber systems welcomes a novel type of threats; called cyber threats. Cyber threats are

asymmetric in nature; an attacker can hide himself easily, the cyber weapons are extremely cheap and prevalent compared to the conventional weapons. Therefore, cyber threats pay the way for harmful attacks against critical infrastructures easily and effortlessly. Secondly, cyber systems caused or increased interdependencies among critical infrastructures. These interdependencies are considered the main cause of cascading failures [3], [4]. Meaning that, a problem in one infrastructure may result in a subsequent failure in another. As an example, a problem in telecommunication infrastructure may have weakening effect on finance infrastructure, as witnessed in Russian hackers' attacks to Estonian networks in 2007 [5]. Therefore, countries started to think about critical infrastructure protection more seriously.

2.2. Cyber Threat Landscape

Today, cyber systems are used vastly in monitoring and controlling of critical infrastructures. SCADA systems that are used in controlling energy, water management systems are example of such cyber systems. Smart grids, smart transportation systems, remotely controllable local gas distribution systems have been emerging as vital parts of modern society. Apart from SCADA systems, some critical infrastructures are completely dependent on conventional cyber systems. For instance, the banking and finance infrastructure depends on conventional information technologies to a great extent. The daily operations of banking and finance companies are totally depended on their huge server parks and network infrastructures. Telecommunication infrastructure is completely composed of cyber systems. In other words, cyber systems created a new critical infrastructure called telecommunication. Without telecommunication infrastructures, modern society cannot be maintained. Because of new service models like cloud computing, Internet can be regarded as critical infrastructure. The attacks to the Estonia networks in 2007 showed how a well-being of a country is depended on Internet infrastructure.

Although Internet is physically distributed, it is logically single. Therefore, Internet connects physically detached things (people, organizations and states) in the same medium. This means that, we share the same medium with cyber attackers having different motivations; from cyber criminals to state sponsored hackers. Today, some of the critical infrastructures are connected to the Internet [6]. The infrastructures that do not have direct connection to Internet are usually connected to internal production networks of organizations. Hence, critical infrastructures are connected to the Internet after passing one hop [7].

Once a simple search is performed by using popular search engines, one can come across with a number of news speaking of cyber attacks against critical infrastructures like nuclear plant, electrical grid, sewing infrastructure, flight control systems and harbor [8], [9].

2.3. Critical Infrastructure Protection Program and Cyber Resilience

The use of cyber systems at critical infrastructures is a necessity without doubt. For some infrastructures, Internet connection is a rigid requirement to serve citizens and/or customers suitably. The focus for critical infrastructure operators is the contribution of cyber systems to efficient and cost effective management of critical infrastructures. However for states, cyber systems must be used according to some specific policies because of attack potential of cyber threats. At this point, critical infrastructure

protection program comes to scene. The importance of critical infrastructures necessitates the state level coordination of security efforts according to the some rigid policies, strategies and procedures. These hierarchical set of rules are called critical infrastructure protection program. Critical infrastructure protection program is the national and coordinated efforts in order to keep the critical infrastructures protected from both cyber and physical threats. A number of countries, including developing ones, have critical infrastructure protection programs. Some developed countries, like Unites States of America, have been working on this subject for decades. Most of the developed countries started to prepare programs within last five to ten years. Today, critical infrastructure protection programs of all countries give an important place to cyber threats.

In developed countries, critical infrastructure protection program is an important part of the national security efforts. In other words, national security officials take cyber security into account because of widespread use of cyber systems and their vulnerable nature. This consideration is materialized with the critical infrastructure protection programs. Because critical infrastructure protection programs fall under national security programs of developed countries, critical infrastructure protection programs not only deal with cyber threats but also with physical threats.

Critical infrastructure protection program is not a single strategy document or it is not associated with a single governmental effort. It does not have to be a unified effort or document with predefined start and due dates so that after some sufficient time period critical infrastructures will be protected. Rather, it is an ongoing and always evolving set of activities, which can be revised according to the new type of threats or recently added national critical infrastructures. That is, critical infrastructure protection is an everlasting process. It is the total effort of a country in order to protect critical infrastructures from cyber and physical threats. A critical infrastructure program is composed of policies, strategies, standards, legislations. As environment and requirements change, new policies and strategies may be released, new responsibilities may be emerged. Since an effective critical infrastructure protection program requires the participation of a number of public and private entities, the coordinator body should be at the highest possible government level.

2.3.1. Cyber Resilience Efforts of Unites States of America

National Infrastructure Protection Plan is the central document of the current critical infrastructure protection program of United States of America [10]. The subtitle of the plan is “Partnering for Critical Infrastructure Security and Resilience”. As this subtitle implies, the National Infrastructure Protection Plan emphasizes the partnership of public and private entities. The aim of the plan is to establish the collaboration and cooperation routines in order to achieve secure and resilient infrastructures. National Infrastructure Protection Plan is released pursuant to the Presidential Policy Directive-21 [11]. The name of Presidential Policy Directive -21 is Critical Infrastructure Security and Resilience. This directive can be regarded as the initiator of the critical infrastructure protection efforts of United States in recent years. Presidential Policy Directive -21 equally emphasize the physical and cyber threats. Directive says that “It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats.”

The term “resilience” is used both in National Infrastructure Protection Plan and Presidential Policy Directive – 21. It implies that the protection of critical

infrastructures is an exhaustive process; it should be considered as not a simple result. Presidential Policy Directive – 21 defines resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents".
Cyber resilience can be defined as the robustness of a country against cyber attacks. It is the preparedness efforts of a country for a cyber war. Therefore, cyber resilience is something parallel with defensive actions of a state [12]. The offensive strategies and efforts cannot be regarded within the cyber resilience effort of a state. Hence, there is strong relationship between critical infrastructure protection programs and cyber resilience. Critical infrastructure protection program is the prominent effort in order to have a cyber resilient country and society.

2.3.2. National Infrastructure Protection Plan

Some introductory information about National Infrastructure Protection Plan is given in the previous section. The national plan is a document that sets forth the details of a risk management framework and a detailed call to action. Risk management is the core process for critical infrastructure security and resilience; and it is fully integrated with the National Infrastructure Protection Plan. Because achieving resilience is directly related with the successful risk management process [10]. The proposed risk management framework has five steps. These steps are:

1) Set goals and objectives
2) Identify infrastructures
3) Assess and analyze risks
4) Implement risk management activities
5) Measure effectiveness

According to the framework, physical, cyber, and human elements of critical infrastructures should be considered through all steps of the framework. Entire risk management framework is accompanied by information sharing mechanisms. Information sharing is used as feedback mechanism to convey the results of measurement of effectiveness. All of the steps of risk management framework is set forth in this section. The linkage between these steps and call to action items are shown with call-out boxes. National Infrastructure Protection Plan does not urge critical infrastructure operators to use this framework. Rather, risk management framework is an "organizing construct" for different type of infrastructures.
The call to action section of the National Infrastructure Protection Plan is a detailed action plan in order to enhance national critical infrastructure security and resilience. This section refer to all of the critical infrastructure partners and stakeholders, whether public and private entity. The basic themes of the call to action section are sector or cross-sector collaboration, cooperation, partnership and information sharing among different types of partners and stakeholders. The details of collaboration, cooperation, partnership and information sharing activities and routines are given under this section. Call to action has twelve actions to advance national efforts. All of these actions are linked to national goals by using call-out boxes which were given in second section of National Infrastructure Protection Plan.
National Infrastructure Protection Plan contain the list of the partners and stakeholders of the critical infrastructure protection community, form federal government agencies to private sector entities. The document also list the roles, responsibilities and

capabilities of these stakeholder. These appendices are extremely useful for the experts who try to understand the organizational structure of United States.

2.3.3. Presidential Policy Directive – 21

Presidential Policy Directive -21 is the stimulus of the National Infrastructure Protection Plan. It determined the organizational structure, roles and responsibilities for critical infrastructure protection. Presidential Policy Directive -21 organized critical infrastructure into 16 sectors and identified Sector-Specific Agencies for these sectors.
It is important to share some remarkable points of the Presidential Policy Directive - 21. The "interconnectedness and interdependency" of critical infrastructures are emphasized in the directive. Directive draws attention to interconnectedness and interdependency in order to emphasize the importance of coordination, collaboration and partnership. Directive mentions the "effective partnerships with critical infrastructure owners and operators". It is said that "this partnership is imperative to strengthen the security and resilience of the Nation's critical infrastructure". Three strategic imperatives for critical infrastructure security and resilience are:

1) "Refining and clarifying functional relationships across the Federal Government"
2) "Enable effective information exchange"
3) "Implement an integration and analysis function" [11].

From these excerpts, it can be easily seen that, isolated, infrastructure-specific efforts do not performed. Because of connected nature of cyber space, the national efforts have to be unified, collaborative. These efforts have to take interdependencies, relationships and partnership into account. These are prerequisites of a successful Critical Infrastructure Protection Plan. These prerequisites are not technical countermeasures. These can be thought as soft skills of a state. Soft skills means they are related with security culture and years and even decades can be required in order to be internalized. Once internalized, cyber maturity is succeeded.
Finally, Presidential Policy Directive – 21 emphasize the importance of international cooperation and promoting research and development activities.

2.3.4. Executive Order - 13636

Executive Order – 13636 is released at the same time with Presidential Policy Directive – 21 [13]. The title of the Executive Order 13636 is Improving Critical Infrastructure Cybersecurity. As the name implies, it is dedicated to cyber security Executive Order – 13636 is released after the delay of US Cybersecurity Act in Senate in summer of 2012. Executive Order – 13636 assigns duty to Federal Government to coordinate with critical infrastructure owners and operators to improve information sharing and collaboratively develop and implement risk-based approaches to cybersecurity [10].
Some of tasks that are assigned by Executive Order to Federal Agencies are as follows:

1) Increasing the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities (Responsible bodies: Attorney General, the Secretary of Homeland Security, the Director of National Intelligence)
2) Expanding the Enhanced Cybersecurity Services program (voluntary information sharing program) to all critical infrastructure sectors in order to assist the owners and operators of critical infrastructure in protecting their systems (Responsible bodies: the Secretary of Homeland Security, the Secretary of Defense)

3) Developing a Cybersecurity Framework (Responsible body: National Institute of Standards and Technology Director) This framework is prepared by the participation of representative of public and private organizations and released [14].
4) Reviewing the preliminary release of Cybersecurity Framework (Responsible bodies: Sector-Specific Agencies, Department of Homeland Security, Office of Management and Budget)
5) Preparing a report for the President, on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. (Responsible body: Secretary of Defense)
6) Using a risk-based approach to identify critical infrastructure, reviewing and updating the list of identified critical infrastructure on an annual basis (Responsible bodies: the Secretary of Homeland Security)

2.4. Cyber Maturity and Cyber Readiness: The Definitions

There is limited number of academic studies that try to define the term cyber maturity on its own. However they express slight difference between these terms. Most of the studies use cyber maturity instead of cyber readiness. The term cyber maturity and readiness is used in order to represent the preparedness level of the states against cyber threats.

Cyber maturity is a set of underlying soft skills of a country in order to increase its cyber resilience persistently and continuously. These skills help a country in succeeding its cyber security efforts like critical infrastructure protection program. The critical infrastructure protection programs of cyber mature countries always evolves and improves. Cyber maturity is not a technical notion. It is the set of capabilities that are created and internalized in a long time. It is closely related with the security culture and awareness level of society. The countries that are mature in terms of cyber security, will probably have long lasting and ever evolving critical infrastructure protection programs. This kind of countries increase their cyber resilience constantly over years.

These good practices are underlying success factors for countries dealing with cyber threats and will definitely affect the quality of critical infrastructure protection programs. If a country implements these good practices, critical infrastructure protection program will be successful. If a country is not mature, its cyber security efforts will not be vigorous. Although the country may take successful steps for the cyber security of critical infrastructures occasionally, the efforts will not be long lasting, they will probably depend on some enthusiastic people or organizations. In other words, the efforts will not be the result of the real state policy.

In this section of paper, the parameters and metrics that constitutes the cyber maturity are extracted from the efforts of United States, OECD (Organization of Economic Cooperation and Development), ITU (International Telecommunication Union) and related academic studies. While examining these studies, the technical countermeasures and policy items are not on focus, but the underlying long-term countermeasure, which are mostly related with the security culture.

2.4.1. The Paper of Hurley, Kern, & Everetts

This academic work draws a difference between cyber maturity and cyber readiness. Cyber readiness implies completeness; however this is not possible [15]. Because

100% security is impossible. Therefore, authors propose the term cyber maturity instead of cyber readiness in order to have more practical outcomes. According to the paper, the concept of cyber readiness is usually used with the terms situational awareness and resilience. Some crucial components that imply a cyber-mature state are extracted from the paper. These components are:

1) Information sharing
2) Education and awareness activities
3) Support for cyber research and development
4) Risk assessment and management
5) Performance measurement
6) Executive support
7) Addressing international challenges
8) Determining detailed roles and responsibilities
9) Overarching cybersecurity strategy
10) Justification the need for investments by measuring costs.

2.4.2. The Paper of White

According to the White, a certain level cyber security maturity has to be accomplished in order to prevent and detect cyber events [16]. At this paper, cyber security maturity is stated along with the current cyber security posture. The paper devises the model called Community Cyber Security Maturity Model, having five levels form initial to vanguard level. According to the White, there are four key areas for cyber security maturity. These are awareness, information sharing, processes and procedures to handle cyber events and test and evaluation of the cyber security countermeasures. The author emphasis the importance of training in order to transition from one level to upper level.

2.4.3. Development of Policies for Protection of Critical Information Infrastructures

The OECD publication named Development of Policies for Protection of Critical Information Infrastructures compares the development of policies for the protection of critical infrastructures in seven developed countries [17].
The comparative study of OECD shares some of the good practices of cyber security. It is said that these good practices are critical for successful implementation of information security in public and private organizations. Some of these good practices are listed as follows:

1) Clear policy and objectives for cyber security have to be set at state level.
2) The adopted approach for cyber security have to be consistent with the culture of all the participants, whether public or private.
3) The state administration have to support and commit to the cyber security studies.
4) Risk assessment and management processes have to be internalized in order to identify the requirements of cyber security.
5) Information sharing has to be substantiated effectively among all of the participants.
6) All relevant policy and standards have to be distributed to all of the participants.
7) Required training and education facilities have to be performed.
8) In order to improve persistently and continually, measurements have to be conducted in order to review the studies and countermeasures and give

necessary feedbacks.

Based on the good practices, some components are examined by OECD in order to compare the critical infrastructure protection studies of seven developed countries. It is claimed that these components are taken by governments into account when implementing critical infrastructure programs. These components are:

1) A national strategy
2) Legal foundations
3) Incident response capability
4) Industry-government partnerships
5) A culture of security
6) Information sharing mechanisms
7) Risk management approach

Some of the good practices and components that are listed in OECD report can be regarded as the parameters of cyber maturity.

2.4.4. Global Cybersecurity Index

Another comparative study is performed by ITU, which is called Global Cybersecurity Index [18]. It is an ITU and ABI Research joint project in order to rank the cybersecurity capabilities of countries. Four goals of this study are listed in the webpage. These goals are as follows:

1) Promote government strategies at a national level
2) Drive implementation efforts across industries and sectors
3) Integrate security into the core of technological progress
4) Foster a global culture of cybersecurity

In order to reach these goals, ITU and ABI Research intent to identify the metrics of cyber security performances of the nation states. A global ranking mechanism is aimed based on these metrics. One of the important part of the project is its mechanism to collect data. There are primary and secondary data sources. Primary data source is the relevant national stakeholders. The secondary data source is publicly available sources. There is an online questionnaire in project webpage as well. Anybody can participate in this questionnaire. Another important part of the project is contact with relevant organizations of nations' in order to acquire data from primary sources. The final goal of the project is to publish a global cybersecurity index of nation states.

The study of Global Cybersecurity Index evaluates the cyber security developments of the states according to the five different areas. These areas are:

1) Legal Measures
2) Technical Measures
3) Organizational Measures
4) Capacity Building
5) Cooperation

Under legal measures area, both criminal legislation and general cyber security regulation / compliance are assessed. Technical measures look at the existence of national Computer Security Incident Response Teams (CSIRT), the government-approved standardization and personal certification studies. In organizational measures area, the existence of a policy, which is expected to cover the following areas, are examined:

1) Clear responsibility of cyber security at all levels of the government
2) Clearly defined, public and transparent roles and responsibilities;

3) Promotion of private sector involvement and public-private partnership

In this section, the existence of cyber security governance, responsible agency for implementation of cyber security policies and the national benchmarking in the light of nationally adopted standards are examined as well. Under the capacity building section, the studies of the standardization development, the professional manpower development, individual certification and agency certification are examined. Under the cooperation section, intra-state, intra-agency and international cooperation activities are examined. Apart from these activities, public-private partnership practices are examined as well.

ITU published the parameters of ranking at project's webpage in Global Cybersecurity Index Conceptual Framework document which can be downloaded from project's website.

2.4.5. Cyber Readiness Index

A similar study was performed by cyber security expert Melissa Hathaway in 2013 [19]. The name of this study was Cyber Readiness Index. Hathaway published five evaluation criteria in order to determine whether a country is cyber ready or not. These criteria are as follows:

1) The existence of national cyber security strategy
2) The existence of operational Computer Security Incident Response Team
3) The commitment (by country) to protect against cyber crime
4) The existence of information sharing mechanisms
5) The existence of investments and funding (by country) of research activities

Under the first criterion, not only the existence of national cyber security strategy is examined; but also the existence of budged that is assigned to strategy is examined. This criterion also considers the participation and engagement of private sector to national cyber security strategy.

Under the second criterion, the existence of tested emergency and recovery plans that taking the infrastructure dependencies into account is examined. The existence of different networks that are composed of governmental / regulatory bodies and critical infrastructure operators with national contact details are exchanged are examined. The existence of information sharing and alert system based on this network is also examined under this criterion.

Under the third criterion, some concrete steps are defined in order to struggle with cyber crime. First of all, it is asked whether monetary loss because of crimes is determined. The other precautions that are questions are threat assessment, establishment of criminal offenses, reviewing existing laws, capacity building mechanisms.

Fourth criterion questions some crucial activities that render the information sharing. These activities are cross sector incident-information sharing during and after incidents, the existence of rapid reaction mechanism, the usage of unclassified intelligence data, the existence of situational awareness mechanism, cross sector incident management and coordination mechanism that take the interdependencies into account.

Fifth criterion questions the budget assigned for cyber security research, national funding for universities, the ratio of operational products that emanates from research activities, the universities that offer degree in cyber security or information security, the government incentive for innovation, the commitment to the internationally accepted

interoperability and security standards and the commitment to protect intellectual property.

By using the results of these projects and documents, it is possible to say that if a country lacks the following parameters or it has some deficiencies at these parameters, it is not a mature country in terms of cyber security:

1) Overarching cyber security regulation that covers critical infrastructures
2) Public-private partnership for cyber security
3) Existence of information sharing and exchange mechanisms, existence of collaboration and cooperation mechanism based on the relationships at state level
4) Existence of cyber security budgeting at state level and the funding of cyber security research
5) Existence of cyber security awareness and culture at state level, which also flourishes the information security governance

3. Critical Infrastructure Protection Efforts of Turkey

Since 2013, Turkey implemented some important steps at policy and strategy level in order to become more resilient against cyber threats. These steps are:

1) The establishment of Cyber Security Council
2) The development and enactment of national cyber security strategy and 2013-2014 action plan
3) The cyber security amendments to the Telecommunications law

The cyber security council was established in October of 2012 with eleven permanent members under the chairmanship of Minister of Telecommunication. All of the members are representatives of public organizations. Any organization whether public or private can be invited to the meeting of council according to the agenda. According to the rules of action of council, it meets every six months regularly. The principal duties of the council are

1) to determine the countermeasures
2) to approve policies, strategies and plans regarding cyber security; and
3) to ensure the application and coordination of policies, strategies, plans.

National cyber security strategy and 2013-2014 action plan was enacted in June of 2013. There are twenty-nine action items in cyber security action plan. These items are distributed under six different themes. These themes are:

1) Regulatory measures (2)
2) Activities to help with judicial processes (1)
3) Establishing the National Cyber Incidents Response Organization (1)
4) Strengthening the National Cyber Security Infrastructure (14)
5) Human Resources Education and Awareness Raising Activities in the Field of Cyber Security (6)
6) Developing National Technologies in the field of Cyber Security (4)
7) Extending the Scope of National Cyber Security Mechanisms (1)

The numbers in parentheses are the number of action item in the theme.

Every action item is assigned to one responsible organization and at least one relevant organization. All of the organizations, responsible or relevant, in action plan are public organizations. There are thirty-one organizations in action plan. Fifteen of them have responsibilities for at least one action item.

The scope of the national cyber security strategy and 2013-2014 action plan is the public organizations and critical infrastructures whether public or private organizations. Therefore, the private organizations that have operations in a noncritical sectors are not covered by national cyber security strategy and action plan.
A quick analysis of the action items yields the following results:

1) Six of the actions items are related with only public organizations.
2) One of the action item is related with only critical infrastructures.
3) Eight of the actions items are related with both public organizations and critical infrastructures.
4) Four of the action items are related with the universities, national education of different levels.
5) Ten of the action items are related with the whole country; although the scope of the strategy is public organizations and critical infrastructures.

The English version of National cyber security strategy and 2013-2014 action plan of Turkey can be downloaded from Internet page of ENISA or CCD-COEi.
The cyber security amendments to the Telecommunications law are performed in February of 2014. These amendments can be summarized as follows:

1) Insertion of Cyber Security Council with its roles and responsibilities
2) Insertion of new roles and responsibilities of Ministry of Telecommunication regarding cyber security
3) Insertion of new roles and responsibilities of Information and Telecommunications Technologies Authority regarding cyber security

The following roles and responsibilities of Ministry of Telecommunications are stated in the amendments:

1) Determining the policies, strategies and goals in order to ensure the national cyber security ,
2) Determining the methods and standards in order to ensure the cyber security for public organizations, individuals, and organizations,
3) Preparing action plans,
4) Fulfilling the responsibilities regarding secretariat of cyber security council,
5) Coordination of cyber security tasks,
6) Determining critical infrastructures and related organizations,
7) Establishing and auditing the required response centers,
8) Supporting the studies on producing national software and hardware
9) Executing the cyber security awareness and training activities

3.1. Critical Infrastructure Protection Program of Turkey

According to the National Cyber Security Framework Manual, a reference book prepared by NATO Collaborative Cyber Defense Center of Excellence, cyber security function in national strategies can grouped in five different mandates [20]. These are:

1) Military Cyber Operations
2) Counter Cyber Crime
3) Intelligence/Counter-Intelligence
4) Cyber Security Crisis Management and Critical Infrastructure Protection
5) Internet Governance and Cyber Diplomacy

When one examine the action items of Turkey's cyber security strategy, the major and dominant mandate of Turkey's cyber security strategy is "Cyber Security Crisis Management and Critical Infrastructure Protection". There are some sections and a few

action items about the “Counter Cyber Crime”. However these items do not enough to change the emphasis to another mandate. There are no items about military operations, cyber intelligence and internet governance and cyber diplomacy mandates in Turkey’s cyber security strategy.

When we look at Turkish national cyber security strategy and action items as a whole, it can be easily seen that Turkey tries to establish basic but essential countermeasures in order to increase cyber resilience. The action items under first and second themes aim to create necessary legal infrastructures on which other countermeasure will be built. The only action item under third theme is action-item 4, which proposes the establishment National Cyber Incidents Response Team (TR-CSIRT). The same action item also proposes the establishment of Sectorial CSIRT for critical sectors and CSIRT for public organizations. This action item is extremely important for state, sector and organizational level cyber resilience. The establishment of sectorial CSIRTS is one the most crucial study of Critical Infrastructure Protection agenda of Turkey. There are fourteen action items under fourth theme. For context of this article, the most important action items of this theme is action-item 5, which is called “Information security management program in critical infrastructures”. This action item proposes the following sub-actions:

1) Determination of critical infrastructures
2) Sectorial risk analysis of one of the critical infrastructures (pilot risk analysis)
3) Determination and publication of the method of sectorial risk analysis
4) Conducting risk analysis (yearly)
5) Determination of the requirements of sectorial emergency action plan and business continuity plan
6) Determining and implementing the sectorial security precautions according to the risk analysis, emergency plan and business continuity plan

The responsible organization for the first two sub-actions is The Scientific and Technological Research Council of Turkey. The responsible organizations for the other sub-actions are the public organizations responsible for regulating and auditing the critical sectors.

The last action item that is directly related with the security of critical infrastructures is action-item 10, which is under fourth team as well. Action-item 10 proposes publishing the document of fundamental rules of secure software development for the software to be used in critical infrastructures, preparing a feasibility report and submission of this report to cyber security council.

The major mandate of Turkey’s cyber security strategy is “Cyber Security Crisis Management and Critical Infrastructure Protection” as stated earlier. In this regard, the whole cyber security strategy can be seen as a holistic critical infrastructure protection program. On the other hand, there are three action items that are explicitly relates security study to critical infrastructures. The directly related action items and their effects on critical infrastructures are summarized in

Table **1**.

Table 1. The action items that are directly related with the security of critical infrastructures

The number of action item	Action item	Action sub-item(s)
4	Establishing the National Cyber Incidents Response team and establishing the Teams for Responding to Cyber Incidents for Critical Sectors and Public Entities	• Establishing the sectorial CSIRTs which are specific to critical infrastructure sectors, and creating their teams as well as providing trainings for them.
5	Information security management program in critical infrastructures	• Determination of critical infrastructures • Sectorial risk analysis of one of the critical infrastructures (pilot risk analysis) • Determination and publication of the method of sectorial risk analysis • Conducting risk analysis (yearly) • Determination of the requirements of sectorial emergency action plan and business continuity plan • Determining and implementing the sectorial security precautions according to the risk analysis, emergency plan and business continuity plan
10	Implementation of the software security program	• Publishing the document on fundamental rules on secure software development independent from programming languages for the software to be used in critical infrastructures. • The preparation of feasibility report and submission of the report to the cyber security council.

There are some other action items within the action plan that may be considered as contributing to the critical infrastructure protection program. However these contributions can be regarded as indirect contributions. This action items are listed at

Table **2**. The first action item at

Table **2** propose to establish a distributed honeypot system to the national public network in order to detect and response to cyber incident in a timely manner. The second action item at

Table **2** propose the establishment of a crisis management structure. Once this crisis management structure established, it will definitely improve the security of infrastructure especially during a cyber attack.

Table 2. The other action items that contributes to the Critical Infrastructure Protection

The number of action item	Action item	Action sub-item(s)
11	Implementation of cyber threats prevention project	• Establishing a Honeypot system to detect cyber threats.
29	Integrating national cyber security concepts into the national security context	• Determining the responsibilities of public organizations in case of cyber security incidents in the cyber space and how to ensure coordination at national level • Determining high priority potential attack scenarios targeting the country, including the effects of these attacks. • Determining priority actions required to be carried out to analyze and improve the status of the mechanisms that would be used in case of potential cyber security incidents.

3.2. Assessment of Cyber Security Maturity Efforts of Turkey

When we look at the efforts of Turkey between 2013 and 2014, the following results can be obtained:

- The correct steps are taken at the beginning.
    - Cyber Security Council is established in order to take decision effectively.
    - Cyber security strategy and action plan is prepared in a short time.
    - The council and the ministry that is responsible for coordination gained jurisdiction by law
- Some progress is observed in last two years. These are:
    - Turkey determined its critical infrastructures. Because it is not published by government, the authors cannot share the list of them.
    - National CSIRT is established.
    - A number of technical trainings on cyber security are completed.
    - Cyber security master programs are opened within at least five universities.

Despite the existence of some improvements in last two years, a number of tasks have not been finished or even started. The most important indication for this situation is the action items in national cyber security strategy and action plan. The action plan will expire by end of 2014. The number of completed action items are quite low compared to the uncompleted action items.

When the authors analyzed the core reasons for this situation, it has been seen that the imperfections in cyber maturity resulted in this situation.

First of all, there is no overarching regulation that cover all critical infrastructures by assigning duties to critical infrastructure operators and regulatory bodies of critical sectors. The only effective regulation is the one that assigns duties to Ministry of

Communication. However assigning duties to coordinator body but not assigning any responsibility to others will be not be effective.
Cyber security is a horizontal area because of ubiquitous use of cyber systems. Therefore cyber security is the common problem of all organizations in all sectors such that health, energy, transportation, public services. This situation requires collaboration and cooperation in order to cope with cyber threats [21]. Because, a threat to a sector will probably be threat to another. Threat information exchange is crucial in order to deal with cyber threat. In Turkey, because of the privacy and confidentiality constraints, organizations usually keep away from information sharing. The culture of cooperation, collaboration and information exchange is quite tenuous because of lack of mechanism to flourish these opportunities.
Public-private partnership is an accelerative force in order to cyber resilient societies. It is important to combat cyber threats [22]. It is an important instrument at the efforts securing critical infrastructures [23]. Turkey has not discovered the potential power of the private sector in cyber security. First example is that, private organizations did not participated in the preparation process of national cyber security strategy and action plan. The second example is that, there is no private sector representative in cyber security council. There are some critical sectors in which both public and private operators have operations. However there is not or limited information and experience sharing practices. There are no incentives by regulatory agencies in order to encourage the information sharing between public and private infrastructure operators.
Although some concrete improvements has been done during last two years, Turkey do not assigned budget to cyber security studies. The president of cyber security council stated that, there will be no specific budget, organizations shall use the budget dedicated to information processing facilities. The existence of dedicated budget will definitely be one of the driving factors for continual cyber security.
The final constituent of cyber maturity is security awareness. Unfortunately, the low level security awareness is a problem for Turkey. Despite the developments in recent years, cyber security awareness is not prevalent at state level, only a few organizations are aware of the criticality of cyber threats. This problem diffuse to the organizations. The most notable reflection of this problem to organizations is the lack of information security governance. The managers of organizations do not value the problem of cyber threat correctly.

4. Conclusion

The success of critical infrastructure protection program is directly related to the level of the national cyber maturity. A successful critical infrastructure protection program will result in a resilient society against cyber threats and cyber war. In this regard, critical infrastructure protection program stands between national cyber security and cyber resilience in the context of cyber war.
Once a countrywide and strategically embraced critical infrastructure protection program is succeeded, the effects of this program will penetrate into the organizations, individuals and society by taking some technical or organizational actions like awareness activities, exercises and new coordinator bodies. So that cyber resilient society will emerge. Therefore, national cyber maturity is a prerequisite to a successful critical infrastructure protection program. In the same way; critical infrastructure protection program is a prerequisite to cyber resilient society. Although it seems like

the efforts pertaining to these three concepts are sequential, they should be iteratively completed. As an example, the output of critical infrastructure protection program may provide useful inputs to national cyber security efforts.

References

[1] *USA Patriot Act*. USA, 2001, pp. 1–132.

[2] US President, *Executive Order 13010 - Critical Infrastructure Protection*. USA: Federal Register, 1996, pp. 37345–37350.

[3] R. G. Little, "Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures," *Journal of Urban Technology*, vol. 9. pp. 109–123, 2002.

[4] I. Eusgeld, C. Nan, and S. Dietz, "'System-of-systems' approach for interdependent critical infrastructures," *Reliab. Eng. Syst. Saf.*, vol. 96, no. 6, pp. 679–686, Jun. 2011.

[5] R. Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," in *Proceedings of the 7th European Conference on Information Warfare*, 2008, p. 163.

[6] J. Lopez, C. Alcaraz, and R. Roman, "On the Protection and Technologies of Critical Information Infrastructures," pp. 160–182, 2007.

[7] V. M. Igure, S. a. Laughter, and R. D. Williams, "Security issues in SCADA networks," *Comput. Secur.*, vol. 25, no. 7, pp. 498–506, Oct. 2006.

[8] S. M. Condron, "Getting It Right: Protecting American Critical Infrastructure In Cyberspace," *Harv. J. Law Technol.*, vol. 20, pp. 403–422, 2007.

[9] J. P. Farwell and R. Rohozinski, "Stuxnet and the Future of Cyber War," *Survival*, vol. 53. pp. 23–40, 2011.

[10] DHS, "NIPP 2013, Partnering for Critical Infrastructure Security and Resilience," 2013.

[11] The White House, *PRESIDENTIAL POLICY DIRECTIVE/PPD-21, Critical Infrastructure Security and Resilience*. 2013, p. 12.

[12] W. Harrop and A. Matteson, "Cyber resilience : A review of critical national infrastructure and cyber security protection measures applied in the UK and USA," *J. Bus. Contin. Emer. Plan.*, vol. 7, no. 1, pp. 149–162, 2013.

[13] US President, *Executive Order 13636—Improving Critical Infrastructure Cybersecurity*, vol. 78, no. 33. 2013, pp. 1–8.

[14] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 2014. [Online]. Available: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. [Accessed: 22-Oct-2014].

[15] J. Hurley, S. Kern, and R. Everetts, "Cyber Readiness : Are we There yet ?," in *9th International Conference on Cyber Warfare and Security*, 2013, pp. 92–98.

[16] G. B. White, “The Community Cyber Security Maturity Model,” in *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, 2011, pp. 173–178.

[17] OECD, “Development of Policies for Protection of Critical Information Infrastructures,” 2007.

[18] ITU, “International Telecommunication Union: Global Cybersecurity Index Conceptual Framework,” 2014.

[19] M. E. Hathaway, “Cyber Readiness Index 1 . 0,” pp. 0–7, 2013.

[20] A. Klimburg, *National Cyber Security Framework Manual*. Tallinn, 2012, p. 253.

[21] B. Karabacak and U. Tatar, “Strategies to Counter Cyberattacks: Cyber threats and Critical Infrastructure Protection,” in *Critical Infrastructure Protection*, M. Edwards, Ed. Ankara: IOS Press, 2012, pp. 63–74.

[22] A. Rak, “Information Sharing in the Cyber Age : a Key to Critical Infrastructure Protection,” vol. 7, no. 2, pp. 50–56, 2002.

[23] T. Kelly and J. Hunker, *Cyber Policy : Institutional Struggle in a Transformed World*, vol. 266. 2011.