Cyber Security Analysis of Turkey

Hakan Şentürk*, C. Zaim Çil**, Şeref Sağıroğlu***

* Department of Management of Technology, Defense Sciences Institute, Turkish Military Academy, 06100, Ankara, Turkey

**Department of Electronic and Communications Engineering, Faculty of Engineering, Çankaya University, 06810, Ankara, Turkey

*** Department of Computer Engineering, Faculty of Engineering, Gazi University, 06500, Ankara, Turkey

‡ Corresponding Author; Address: Tel: +90 312 414 2631, Fax: +90 312 414 2537, e-mail: hsenturk@hvkk.tsk.tr

Abstract- Considering the criticality of the cyber security threat in the 21st century, it is presumed that the nations are busy with series of activities in order to protect their security in the cyber space domain. In this paper, in light of the recent developments in the cyber security field, Turkey's cyber security analysis is performed using a macro analysis model. We researched for the measures taken in Turkey with respect to those in the other countries, reviewed the posture, the activities and actions taken in the last ten years and provided recommendations deemed necessary to enhance national cyber security. The paper aims to contribute to the cyber security literature on governance issues as well as to national security preparations. It needs to be emphasized that the views contained in this paper belong to the authors and do not reflect any official view of the respective institutions.

Keywords- cyber security; national cyber security analysis; cyber warfare; cyber security strategy

1. Introduction

Cyber security is defined by ITU as, "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." [1].

Since the first State-level Cyber War in Estonia in 2007, a number of cyber war incidents have taken place in countries such as Russia-Georgia (South Ossetia dispute), North Korea-US, China-India, Stuxnet attack on Iran's nuclear facilities, more advanced Duqu worm, latest Flame virus and Gauss with a mystery payload, aimed at Middle Eastern government systems as well as Shamoon virus that damaged 30,000 Saudi Aramco workstations. These attacks prove that cyber warfare will increase its severity over time, revealing the critical importance of ensuring the security of cyber-space in the 21st century. In fact, the report "Cyber Security Strategy of the United Kingdom" prepared by the UK Cabinet Office in June 2009, points out the importance of the cyber space with the statement "Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our advantage in cyber space" [2].

Nations are struggling to adapt themselves to the new century's warfare which is transformed into wars with cyber battle space [3] and cyber warriors. Every new day brings about a number of news stories such as various countries establishing cyber units with defensive and offensive capabilities, implementing training and exercise activities, performing symposiums, workshops, etc. in order to raise security awareness of the public. The attack type on the rise last year is the advanced persistent threats (APTs). They use highly customized stealthy intrusion techniques and aim to gather high value, national information such as military, political or economic intelligence

[4]. The Trendmicro 3Q/12 report states that 76% of the APTs target corporate/government systems [5]. Official sources state that US, China, UK, Iran and at least other 140 countries are developing cyber weapons [6,7]. Considering these recent developments in the field of cyber security, it is possible to claim that nations are in a fierce competition in the cyber space domain in terms of both defensive and offensive measures.

Percentage of households with internet access in Turkey has increased to 42.9% in recent years [8]. According to a survey conducted in 2011, 14% of Turkey's population owns a smart phone of which 66% connect to the internet with their mobile phones [9]. Turkey is in the eight order in the list of countries that host botnets [10], it is ranked third in the production and distribution of spam e-mail [5] and ranked ninth (fifteenth previous year) in the source of malicious activities with a 3% of the total worldwide malicious activity [10]. In the botnet rental advertisements on the Internet, Turkey is in the cheap botnet league with 40 U.S. dollars per 1000 computers. Thus, it is likely to assert that Turkey's current computer park (virtual soldiers), becomes a powerful weapon that can be used against her [11] and her risk high at a possible cyber war.

This paper focus on analyzing cyber security posture of Turkey using a cyber security macro analysis model [12] and is organized as follow. The second chapter provides the aim, scope and methodology of the study. The third chapter provides a brief introduction to the seven main indicators used in the model and then presents the findings regarding the current state of activities in Turkey. The chapter also places special focus on the national strategies. The fourth and fifth chapters provide recommendations and the conclusion, respectively.

2. The Aim, Scope and Methodology

The aim of this study is to analyze the cyber security posture of Turkey in accordance with the model's seven main indicators as indicated in Fig.1: National Cyber Security Strategy, Action Plans and Official Reports, Legal Framework, Responsible Authority and Organizations, Cyber Security Programs, Cyber Security Activities of the Armed Forces, National/International Cooperation. The model encompasses the cyber security strategy of the nation and the action plans and programs which are in close interaction with each other, as well as the institutions/organizations responsible for implementing them. It also covers the activities of the armed forces. All these factors are complemented by the legislative framework and the national/international co-operation.

The cyber security analysis of Turkey is carried out in accordance with the proposed indicators, accompanied by the identification of the weaknesses as well as the measures to be taken. In the analysis, only publicly available open source official reports, strategic plan documents and other activities between 2002 and 2012 are taken into consideration and evaluations are made with the assumption that there exists no other plan, report or activity.

Figure 1. Cyber Security Macro Analysis Model [12].

3. Analysis and Findings

The analysis is performed in seven sub-chapters. In each sub-chapter, a brief introduction of the used model's indicator is provided and then findings regarding the respective indicators are presented.

3.1. National Cyber Security Strategy

The most important aspect of cyber security at the national level is strategic management which also covers strategic planning. For a comprehensive analysis, the first line of measure should be the nation's cyber security strategy.

In the 21st century, cyber wars and ensuring security at the cyber space is evidently a top strategic priority. Therefore, it is vital to develop a national strategy. Marsan compares the cyber war with conventional wars and determines the differences as the importance of winning the first

fight, the speed, the targeted nature of the attacks, the secrecy, the techniques, goals and the objectives [13]. He concludes that cyber-wars can not be tackled with conventional warfare strategies.

With recent developments in technology, cyber-attacks are increasing their sophistication; hence it is almost next to impossible to trace the attacks to its source [14]. It is suggested that cyber warfare is the transformation of the known nature of the conventional warfare [15]. Against such warfare, the application of the conventional strategies will not work. As in the case of nuclear deterrence between the United States and the Soviet Union, Libicki replies negatively to the question "... Is the strengthening of cyber-attack capabilities likely to prevent the cyber wars?"; due to the fact that in the case of cyber wars, most of the times it is not possible to determine who attacked, it is not effective if the same type of attack is used repetitively and when the attackers are small countries with closed systems, retaliation with cyber tactics and resources will not pose a similar threat [16].

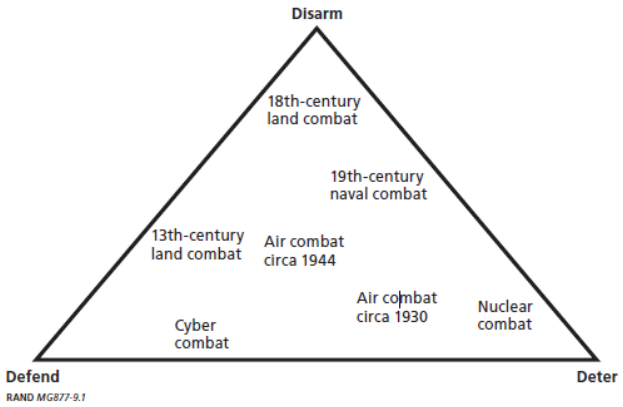

Figure 2. Deter-Disarm-Defend Triangle [16].

In the face of a cyber threat, there are three basic strategies that the target country may apply: Deterrence, Disarmament and Defense. Libicki explains the various forms of combat and where they fit in the Deter-Disarm-Defend Triangle shown in Fig. 2. He concludes that rather than the disarmament and deterrence, the best strategy is a good defense [16]. To achieve a good defense, it is imperative that a nation develop a national strategy document which includes the strategic goals as well as the measures to achieve them [17]. All military and political disputes in the future will have a cyber security aspect. That's why countries that have no cyber security strategy and a central defense and response capability will be weak [18].

Specific aspects to analyze a strategy document could be: the distribution of responsibilities between the institutions, the prioritization of strategic objectives, the identification of necessary action plans and roadmaps for achieving the strategic goals, the determination of the R&D subjects in the field of cyber security technologies and respective financial/executive government initiatives to encourage related work, the protection of national critical infrastructures, the preparation of action plans to achieve this purpose and the provision of public and private sector cooperation.

Before going any further, it is a good start to review National Cyber Security Strategy Documents in the world. The following paragraphs focus on these documents.

U.S. National Cyber Strategy document ("National Strategy for Securing Cyber Space") was published in February 2003 [19]. The document, that has been developed by thousands of people across the nation and many public and private organizations, states that securing the cyber space is only possible with the contribution of all the American people and especially the private sector as well as public and private sector cooperation. The document assigns the main responsibility of ensuring cyber security to the U.S. Department of Homeland Security (DHS) and dictates that the strategy document that comprises three strategic goals is a complement to the "National Strategy" prepared for the protection of the U.S. homeland. Another strategy document ("Comprehensive National Cybersecurity Initiative-CNCI") was prepared in 2008 as a "CONFIDENTIAL" document but in 2010 made available to the public by downgrading the security classification of one part of the document. The document comprises twelve directives that address the government's comprehensive strategy regarding the protection of military, civilian and government computer networks and systems and the critical infrastructures as well as the strategies to implement against cyber war [20]. U.S. international strategy for cyberspace document was published in May 2011 focusing on protecting U.S. networks, law enforcement, preparation of

military, internet governance and freedom as policy priorities [21].

The UK cyber security strategy document, published first in June 2009, addresses the main themes as the security, flexibility, and resiliency in cyberspace; identifies the greatest threat in the current century as the cyber security risks; points out the need for international co-ordination and the establishment of a central Office of Cyber Security; and the requirement to determine the current doctrinal, political, and legal shortcomings [22]. The updated strategy document, published in 2011, aims to make the UK one of the most secure places in the world to do business. With the strategy document, the UK Government commits funding of 650 million pounds over a four year period for a transformative National Cyber Security Programme to strengthen UK's cyber capabilities; the document also outlines UK's plans for a new cybercrime unit and a center for national critical infrastructure protection [23].

Germany's cyber security strategy document states the requirement to establish a National Cyber Security Council and the National Cyber Response Centre, with emphasis on critical information infrastructure protection and national public systems security [24].

Australian cyber security strategy document, published in 2009, addresses the threat awareness and intervention, cultural change and the resiliency of all of the electronic systems that might pose a threat to national security [25].

French cyber security strategy document addresses the strategic goals to be the superpower of cyber defense, to protect the information regarding the national independence, to protect the national critical infrastructure and to ensure cyber security in the cyber space [26].

The cyber security strategy document of the Netherlands attaches special importance to the public-private partnership and international cooperation [27].

In the Indian cyber security strategy document, legal framework, establishment of security incidents early warning and response system, Digital forensics and Research & Development centers and international cooperation issues are emphasized [28].

When we generally reviewed other countries' official reports and publications, the concepts of security perspectives are similar and they consider people, organizations, institutions, developments, action types and precautions as well as future plans and strategies.

The process of developing National Cyber Security Strategy Document of Turkey is summarized as follows. There had been many meetings, workshops, seminars and conferences, held in Turkey to discuss the issues initially but the most compact event was a workshop in Ankara, Turkey. A Cyber Security Strategy Workshop was held in Ankara on June 16, 2012, through the initiative of the Turkish Information Security Association. The members of this society initially prepared a draft document which further on, was shared with private and public institutions. This document was then discussed in a workshop with the participation of more than 80 IT security professionals and experts from public and private institutions, a draft strategy document was revised in this workshop and presented to the Ministry of Transport, Maritime Affairs and Communications [29]. This Turkish Strategy Document states that in order to protect the nation's land, citizens, all assets, today and future, it is imperative that the security of the cyber space is ensured [30]. The document also addresses following key points:

- The establishment of National Cyber Security Council,
- The performance of national cyber security risk analysis annually,
- The establishment of National Cyber Threat and Vulnerability Analysis Center Laboratory,
- The establishment of Cyber Security Center of Excellence,
- The requirement for government/private agencies that manage critical infrastructures to be compatible with TS ISO/IEC 27001 Information Security Management System (ISMS),
- The need to increase the cyber security awareness, in this respect, a suggestion of an awareness month, May,

- The proposal of a core "Cyber Security and Defense" course in the universities programs.

Another official policy document is the "National Cyberspace Security Policy", prepared in 2008 by the collaboration of 19 government agencies and submitted to the Office of Prime Minister in 2009 [31]. The aim of the document is to identify the steps for Turkey to prepare the nation against the attacks in the cyber space and to recover in a resilient manner. The identified steps are as follows:

- The preparation of National Cyber Security Strategy,
- Legal regulations
- The development of national cyber capabilities
- The establishment of National Cyber Incident Response Organization
- The training and awareness Activities
- The protection of Critical Infrastructures
- International Cooperation
- Cyber Security of the Public Institutions

3.2. Action Plans and Official Reports

In order to achieve the strategic goals identified in the national strategy, there must be strategic plans that address specific programs and roadmaps. With this indicator, these strategic plans as well as the official reports generated to address strategic issues for the nation are evaluated in order to determine the nation's potential to achieve a secure cyber space.

Following policy documents have been released by the State Planning Organization in the last 10 years: "e-Turkey Initiative Action Plan-2002", "e-Transformation Turkey Project Short-Term Action Plan (2003-2004)", "e-Transformation Turkey Project 2005 Action Plan", "Information Society Strategy (2006-2010)", "Information Society Strategy Action Plan (2006-2010)". "Information Society Strategy and its Annex, Action Plan" dated July 11, 2006 was approved by the Supreme Planning Council and was published in the Official Gazette of Republic of Turkey dated July 28, 2006, numbered 26242. This document has five action plans that are related to the national cyber security, which are:

1- "Security and Privacy of Personal Information" category, action plan 88 determines a 24-month period from 2007 to establish a National Information Systems Security Program (UBGP in Turkish) by the responsible organization TUBITAK-UEKAE.

2- "Information Security Related Legal Regulations" action plan 87 dictates that legal regulations be made for below issues by the responsible organization of the Ministry of Justice:

- Protection of all information in electronic form which is related to the national security as well as the protection of government information security systems.

- Protection of Personal Data [32].

3- "Citizen-Focused Approach" category, action plan 27 requires web sites of all public institutions to ensure standardization of the content, security, identity management, and usability. For this, a guide named "Standards and Recommendations for Websites of Public Institutions" was prepared and introduced to the public at a meeting held on January 27, 2009. In addition, the web site http://www.kakis.gov.tr has been activated in order to promote the standards.

4 - "The Adoption of Information and Communication Technologies by Businesses" category, action plan 26 dictates e-commerce security infrastructure requirements by the Turkish Standards Institute.

5 - "Social Transformation" category, action plan 10 named as "Internet Security", requires the monitoring the results of the "Law No. 5651, entitled Regulation of Publications on the Internet and Combating Crimes Committed by means of Such Publication" by the Ministry of Justice. Until the analysis is completed, no further action is foreseen on this action plan and thus it is treated as closed [33].

With respect to the official reports; we could only find one cyber security reference in the 2010-2014 Strategic Plan of the Ministry of Health. Other Ministries' and even the Information and Communications Technologies Authority (BTK in Turkish)'s strategic plans that are published on

respective web sites do not address cyber security within the scope of their strategic goals and objectives. State Planning Organization's 2009-2013, Undersecretariat for Defense Industries (SSM)'s Sectorial Strategy Document 2009-2016 and SSM's 2012-2016 Strategic Plan documents do not include any goals or action plans regarding cyber security.

One last report that can be mentioned, although it does not reflect the views of the institution, is the 2009 report "Securing Cyberspace: Turkey's Current Situation and Measures to be Taken" prepared by the staff of the Department of Information Technology & Coordination. It presents recommendations for the provision of the national cyber security [34].

3.3. Legal Framework

One of the cornerstones of the used model is legislation, which emerges as the most important problem area if not regulated. After the distributed denial of service attacks against the US and South Korean government systems in July 2009, the central control computer of the attacks was traced back to an IP address in Miami/Florida [35], not in China or North Korea. In such cases it is hard to determine who is guilty and where he or she is. These examples prove the importance of legal necessities. In this aspect, we'll first evaluate if the current national laws ensure the security of the classified information and the public/government systems and networks on which the information is processed. Next, the regulations regarding the private sector, end-users and the critical infrastructures of the nation will be examined.

Findings

This document was finally shared and discussed with the all state institutions and accepted in a meeting of national board of Turkey.

The Cabinet Decision Nr. 2012/3842 [36] which has been published on the Official Gazette on 20 October 2012 determines a number of responsibilities on the implementation, management and coordination of Turkish national cyber security activities to be implemented by the responsible authority - The Ministry of Transport, Maritime Affairs and Communications. The decision also establishes the National Cyber Security Board which is explained in the next sub-section.

Law No. 5809, entitled "Electronic Communications Act" regulates information security and confidentiality of communications to ensure the security of the networks against unauthorized access, including compliance with security and quality of service standards and specifications for electronic communications sector. The task to perform the required measures envisaged by the legislation is to be carried out by National Information and Communication Technologies Authority [37].

Electronic Communications Security Regulations was published in the Official Gazette No. 26 942, dated July 20, 2008. With this, Communications Operators are required to be certified with TS ISO/IEC 27001 Information Security Management System.

Law No. 5070, entitled "Electronic Signature Act" regulates the technical criteria regarding secure electronic signature as well as the authorization and supervision of Electronic Certificate Service Providers,

Law No. 5651, entitled "Regulation of Publications on the Internet and Combating Crimes Committed by means of Such Publication" in 2007 regulates Internet actors in terms of content, location, access and access providers and content control,

Draft Law on Electronic Commerce provides the authority to make secondary legislation on unsolicited electronic mail,

"Regulation of Processing of Personal Information and Protection of Privacy in the Telecommunications Sector" regulates the confidentiality of correspondence, processing of traffic data, and detection of location,

Draft regulation regarding Unsolicited Electronic Messages determines the procedures to block spam SMSs,

Draft Principles and Procedures for the Secure Use of the Internet, 2011, regulates operators to deliver secure internet service,

The State Planning Organization Strategy Document Action Plan 87, entitled "Regulations

Regarding Information Security", dictates the legislations for protection of privacy, the classified information and government information security systems and networks. In this context, the Draft Law on Personal Data Protection was submitted to the Parliament on April 22, 2008, but has not been approved yet [38].

Draft Law on National Information Security Organization and Its Duties has been prepared and this work of Ministry of Justice to establish a commission is ongoing.

The IT crime is dealt with the Turkish Penal Code 10; specifically below three crimes are defined:

- Item 243 regulates the breach to the IT system,

- Item 244 regulates denial of service, system disruption, data modification and destruction,

- Item 245 regulates the offense of misuse of debit and credit cards.

3.4. Responsible Authority and Official Reports

This is the main indicator to analyze if a country has established necessary organizational structures for national cyber security. One of the most important issues is the designation of one single central authority that will be responsible for overall national cyber security. This authority should harmonize all the efforts and activities of other organizations that have cyber security tasks such as, accreditation, auditing, standards, specification and protection of both public and private systems as well as critical infrastructures. To enhance the nation's cyber security capabilities, the existence of specialized institutes, laboratories and centers that engage in research and development of cyber security technologies is also important.

Findings

Until October 2012, the responsible authority for cyber security was TUBITAK agency. As of 20 October 2012, after the Cabinet Decision Nr. 2012/3842 publication on the Official Gazette; the responsible authority became The Ministry of Transport, Maritime Affairs and Communications. The decision also establishes the National Cyber Security Board with membership of Ministries of Foreign and Internal Affairs and Defense and several undersecretaries and chief executives of National Intelligence Agency, Public Order and Security, Turkish General Staff, TÜBİTAK, BTK, Financial Crimes Investigation Board (MASAK in Turkish), Telecommunications and Communications Commission (TİB in Turkish) and others that will be deemed necessary by the Ministry [36].

There are currently two accredited Computer Emergency Response Teams (CERTs). One is government-run (TR-BOME) and the other belongs to TUBITAK (ULAK-CSIRT) operated for the purpose of research and education. TR-BOME is also active in the international arena. It has signed a memorandum of agreement with NATO Computer Incident Response Capability-NCIRC in 2007 on the issues of staff exchange, participation to NATO cyber defense exercise, joint incident response, access to NCIRC network, vulnerability database and alarm/warnings and support on malicious code analysis [39]. TR-BOME has represented Turkey at the "International Cyber Defense Workshop, Fall 09 - ICDW09" exercise and participated actively to the NATO Exercise Cyber Coalition 2009.

Established under the National Information Systems Security Program, The CERT Coordination Centre is tasked with the responsibility of helping the public/private institutions across the country to gain the ability to respond to computer security incidents. There is also a CERT in its organization as explained above [40].

Cyber Space Defense Centre (SOSAM in Turkish) is a research center established in Ankara under the National Information Systems Security Program. It has real and honeypot systems that gather statistics on traffic data and cyber-attacks. Its activities focus on threat detection against public institutions, profiling and reporting of cyber-attacks, issuing warnings and precautionary measures and botnet detection and destruction [41].

There is no authority or center for the protection of critical infrastructures.

3.5. Cyber Security Programs

This is the main indicator to analyze the realization of strategic plans into specific programs

and the projects on a national scale. Especially, awareness-raising academic activities, training programs, exercises, research and development projects, defense programs specific for the protection of critical infrastructure, risk management, vulnerability analysis such as databases or web portals as well as participation to international initiatives are all issues that can be evaluated in this context.

Findings

State Planning Organization's "Information Society Strategy and its Annex, Action Plan 88 dictates the National Information Systems Security Program. The program is a follow-on project to the e-Transformation of Turkey Project, 2005 by TÜBİTAK-UEKAE. Within the scope of the project;

- In item "Co-ordination", the establishment of National Computer Incidents Response Team Coordination Center,

- In item "Training", the training of data processing personnel working in public institutions,

- In item "Documentation", the preparation of information systems security-related guidance documents for public institutions and sharing via the Information Security Portal (Gate),

- In item "Management", the establishment of Information Security Management System (ISMS) to the selected public institutions,

- In item "Monitoring", the establishment of Cyber Space Defense System [41].

The implementation of the above mentioned programs are underway. The Fifth Assessment Report of the Information Society Strategy Action Plan states that university staff is provided with cyber security training; TR-BOME has been working to provide free online courses such as user awareness training, CERT installation and management training, incident response and system analysis training. For the Information Security Management System (ISMS) Project, risk analysis of several government offices and ministries such as the Office of Prime Minister and the Ministry of Justice has been completed.

Within the scope of National Information Security Gate project, the web site at http://www.bilgiguvenligi.gov.tr/ publishes technical articles, standards and guidance documents and information security papers on cyber security issues.

In addition, there are a large number of cyber security training programs provided by private educational institutions. For example, for the first time a cyber security summer camp is held in July 2011 by the Academy of Information Security. A group of 20 university students are given intensive training for five weeks [42]. There are also free programs such as http://www.CEHTurkiye.com which is an online library managed by ethical hackers in order to share their information security knowledge and experience [43].

In order to increase public awareness, a security awareness day was put into place for the first time on February 23, 2010. In addition a booklet has been published by the government that provides useful information on secure use of information systems by the students and their parents [44].

Regarding the conferences and symposium, a sufficient number of such activities are held in Turkey. The International Conference on Information Security and Cryptology (ISC) held its fifth organization in May 2012 with the main theme of Cyber Security and Defense. All of the presentations and articles are published online on the ISC website (http://www.iscturkey.org). Other examples are; Information Technology Security Conference for Public Institutions held its sixth panel in 2011, National Cyber Security Workshop conducted second time in September 2011, Cyber Security Law Workshop conducted in January 2012, Cyber Security Conference held in December 2011.

Within the scope of Cyber Security Exercises, the first CERT exercise was held on November 20-21, 2008 with the participation of eight public institutions. The second one entitled Information Systems Security Exercise was held between January 25-28 2011 with the participation of 41 public and private institutions and ministries from a variety of sectors such as finance, electronic communications, education, internal security and defense. During the 3-day exercise, over 450

scenarios were tested including distributed denial of service and website security audits [45]. An important CERT exercise was also achieved for only internet service providers and GSM operators in the second period of 2012.

However, as of today, there is no official program for the protection of critical infrastructures.

3.6. Activities of Armed Forces

This is the main indicator to analyze a country's approach to cyber security as warfare. McAfee Virtual Criminology Report 2009 states that the countries not only collect information on their adversaries' activities in cyber space but also developing sophisticated cyber-attack techniques. The countries, known to have offensive cyber capabilities are China, Russia, the U.S., Israel and France [46]. North Korea, Iran, Taiwan, Brazil [47] and India [48] are also known to have offensive programs. In an analysis, the U.S. is alleged to have the offensive power score of 8, cyber defense power score of 1, whereas North Korea has 2 and 7, respectively [49].

When we consider the need for both civilian and military measures [50] in order to protect the information and the processing systems that operate in the cyber space, it is a common sense that a country's armed forces activities should also be analyzed. The existence of a military cyber security strategy document, doctrine, concept and action, defensive and offensive cyber security command, CERT, specialized cyber security staff, training institute, level of participation to National/international programs, etc. can be evaluated in this context.

Findings

In July 2012, Undersecretariat for Defense Industries (SSM) has signed a feasibility contract with STM AS., a government-owned company, for information assurance and cyber defense capability development. The Project entitled "Integrated Cyber Security System" aims to produce a prototype on a test bed and a network enabled capability feasibility report on cyber defense systems, software and processes for the purposes of concept validation [51]. This also implies that a concept is available. In a press release in August 2012, the Minister of Transport, Maritime Affairs and Communications, Binali Yıldırım talked about cooperation between the Turkish Armed Forces (TAF) and NATO; he also mentioned that several projects are underway for the Turkish General Staff and other forces [52]. Participation of the TAF personnel to several symposium and conferences are also observed.

3.7. National and International Cooperation

All the activities, programs and projects explained above serve a common, shared goal to ensure national cyber security. To achieve this, a great deal of harmonization as well as cooperation is required. There is also a need for international cooperation particularly for the protection of critical infrastructures against cyber-attacks. Thus, the U.S. "Cyber Space Policy Review Report" draws the attention to national and international dialog between all actors [53].

Findings

As an example of national cooperation, a project about working against spam e-mail is performed in 2009 by BTK with the participation of many public and private institutions. At the end of the project, which is a good example of best practices, the IP address count that transmits spam mails has declined 99 percent and overall spam mail count per day has declined from 6,5 billion to 394 million [44]. One of the issues that come forward from the 13th e-government round table meeting is the necessity of public awareness as well as public and private sector's trust based cooperation. The meeting was held on February 23, 2012 in Ankara with the participation of many institutions with a theme of Turkey's Cyber Security Roadmap [54].

An index search of cyber security in the Official Gazette of Turkish Republic revealed a finding with regards to international cooperation which is a memorandum of understanding between Malaysia and Turkey that includes possible cooperation on the field of cyber security technologies [55].

One negative example is the Cyber Space Conference held in London in November 2011 [56]. Turkey was not among the 60 countries that participated to the conference which emphasized globally coordinated intervention against cyber-attacks [57].

4. Recommendations

In this chapter, considering the findings in previous chapter, some recommendations are provided for each main indicator used to perform the analysis.

In the context of the national strategy; the draft strategy document needs to be reviewed and published officially. Although most of the strategies are defensive in nature, the fact that cyber warfare poses risks not only at cyber space but also in terms of physical damage as experienced in the Stuxnet incident should not be underestimated and offensive strategies should also be developed. Recent analysis publicized by Kaspersky Lab states that traces of collaboration have been found in the development of Stuxnet, DuQu, Flame, Gauss and miniFlame that are believed to be produced allegedly by the same state-sponsored cyber weapon factory [58,59]. These sophisticated malware tools indicate that such capabilities are being developed by state-sponsored parties. Besides, the US National Defense Authorization Act, signed in December 2011 and the annual defense budget grants the authority for offensive operations [60].

In the context of action plans and official reports; each ministry and government authority should develop their own cyber security strategic plans. For the protection of critical infrastructures mostly owned and controlled by the private sector, the role and responsibility of the government should be clearly identified; a public-private partnership model should be developed and joint CERTs should be established for the protection of critical infrastructures. Government and military systems that process classified information should be isolated with secure air gapped systems. In the case of an attack, well-developed response and recovery plans should be made readily available. The analysis in this context observes many deficiencies. In addition, public/private institutions such as Information Communication Institute and TÜBİTAK should be encouraged to publish national reports containing a variety of analysis and recommendations especially for the attention of government.

In the context of legal framework; after enactment of National Cyber Security Board that is established by the Cabinet decision 2012/3842 [36], most legislative changes and other deep-rooted activities are believed to take place more rapidly. The scope of current three IT crimes in the Turkish Penal Code should be enlarged to address crimes that involve advanced technology. The domestic laws should be adapted in parallel to the European Convention on Cybercrime. As a country with young and well-educated population, capable especially in software engineering, developing more secure software and hardware systems should be made mandatory by enforcing necessary security standards and related criteria in production processes [17]. The Draft Law on Personal Data Protection should be approved as soon as possible. In addition, another issue to consider could be to give the internet service providers to the authority and the obligation to prevent violations of information security [61]. In agreement with the final report for 3rd International Conference on Information Security and Cryptology, a forensic institute and a new governance model can be established for the analysis of cybercrimes [62]. In summary, as the final declaration of Workshop on Cyber Security Law 2012 suggests, the current regulations explained and analyzed in this paper are sufficient to support the cyber security legal infrastructure but they are not enough to meet all the current needs in the area [63].

In the context of responsible authority and organizations; the recently established National Cyber Security Board should convene for the first time as soon as possible and should kick off the long-standing strategic actions regarding cyber security. Joint incident response centers for critical infrastructures should be established. All ongoing and future cyber security programs should be assigned to specific bodies and program audits should be performed by a central higher authority.

In the context of cyber security programs; there is a good progress on the action plan 88, however, much effort is required. With the Cabinet Decision 2012/3842 [36], the Ministry of Transport, Maritime Affairs and Communications has been given a number of responsibilities that require starting necessary programs and projects in the near future. The government incentives for research and development should be enlarged to include nationally critical cyber security

technologies. In 2012, the United States Defense Advanced Research Projects Agency (DARPA) research budget for cyber security has been increased by 50 percent to 208 million dollars [64]. Training in the field of cyber security should be provided at all levels from primary school to graduate; the curricula should be updated accordingly. Importance should be given to specialized cyber security manpower. As the final report of ICT Conference held on February 7 2012 states, a Cyber Security Centre of Excellence could be established [65]. Especially the security audits and pen tests performed on the government information systems should be performed by a national authority with respect to the current national security policies [66]. The number of conferences and symposiums appear promising, whereas for cyber exercises, the results of the cyber exercise display a negative image for public institutions and organizations. The results prove that a focused approach is necessary to enhance the cyber security of public institutions.

In the context of cyber security operations of the armed forces; the awarded feasibility project is a good indication of progress. The military should prepare itself for cyber security threat. However, it should be noted that rather than just defensive, both defensive and offensive capabilities should be developed if a nation would like to have its advantage in the cyberspace domain. The USCYBERCOM and South Korean Cyber Command is known to have offensive programs [67,68]. The military should participate in the national cyber security exercises and red-blue cyber warfare exercises such as Shriever in the US, should be regularly performed.

In the context of national / international cooperation; particularly in the area of critical infrastructures protection, cooperation between government and private sector critical infrastructure operators is required. All the activities such as detection and prevention of cyber-attacks, monitoring, analysis and intervention should be guided and controlled by a central facility of high authority.

5. Conclusion

In the world where systems are increasingly online and where information technology has become an inevitable part of life, cyber-attack techniques are undoubtedly the most effective and least expensive method to cause harm to an individual, group, company, institution or a country. For this reason, there's no doubt that the cyber threat is going to increase its severity.

This paper used the proposed cyber security macro analysis model and performed a cyber security analysis of Turkey. The findings and respective recommendations are provided in the chapters three and four. The summary of analysis is shown in Table 1.

Table 1. Summary of Analysis

Model Indicators	Summary of Actions
National Cyber Security Strategy	- Strategy document drafted in Oct 2012 - Policy document (2008) in effect
Action Plans and Official Reports	- Five action plans in progress - Only one cyber security reference in Ministries' Strategic Plans - No official reports except one individually authored
Legal Framework	- Cabinet Decision 2012/3842 - Several Laws approved or drafted
Responsible Authority and Organizations	- Ministry of Transport, Maritime Affairs and Communications determined to be Responsible Authority (Oct 2012) - Cyber Security Board establishment approved (Oct 2012) - No specific authority/center for Critical Infrastructures Protection
Cyber Security Programs	- Several ongoing projects - Satisfying number of symposiums and conferences - More need for cyber exercises - No programs for Critical Infrastructures Protection
Activities of Armed Forces	- Feasibility Project awarded - No other publicly available activity.
National/International Cooperation	- Good example - spam prevention project - Lack of participation to activities in international arena. - No specific public-private cooperation for Critical Infrastructures Protection.

With respect to the cyber security analysis of Turkey, it is concluded that without a national strategy and a responsible senior level authority, the impact of all cyber security activities, programs and projects are to be limited in nature. There are also observed deficiencies in the areas of legislation and cooperation especially for protection of critical infrastructures.

It should be kept in mind that the cyber security technologies are not in the hands of a few

countries like nuclear technology. Both targeted and untargeted cyber-attacks can be performed using cyber security technologies. It is a common misconception to think that production of cyber weapons is too early [69]. When it is known that countries are increasing their cyber security capabilities and developing cyber weapons just as they do so for other warfare domains i.e. land, sea, air and space; it would be a crucial mistake to stay behind that inevitable race. For this reason, in parallel to the intensive preparations for cyber wars as in the other countries such as US, Turkey should immediately adapt itself against the new century's critical threat. The incorporation of cyber threat into the National Security Policy Document aka the "Red Book" is a very positive step taken at the highest level, however there is more to be done in many areas as explained in chapter four.

For a nation that would like to strengthen its place in the 21st century's battlefield of cyber space, it is believed that the recommendations be considered and put into practice in a timely fashion.

Acknowledgements

This article is an extended version of the paper presented at the 5th International Conference on Information Security and Cryptology, 15-17 May 2012, Ankara, Turkey.

References

[1] ITU web site, accessed 23 December 2012, <http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx />
[2] UK Cabinet Office, "Cyber Security Strategy of the United Kingdom", June 2009, accessed 02 November 2012, <http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf/>
[3] Ayers, R., "The New Threat: Information Warfare, RUSI Journal", 144:5 (1999:Oct.) p.23
[4] Symantec "Internet Security Threat Report, 2011 Trends. Vol. 17", April, 2012
[5] TrendMicro 3rd Quarter 2012 Security Roundup Report, accessed 31 October 2012, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-3q-2012-security-roundup-android-under-siege-popularity-comes-at-a-price.pdf/>
[6] Paganini, P., "The Rise of Cyber Weapons and Relative Impact on Cyberspace", 05 October 2012, accessed 31 October 2012, <http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/>
[7] Paganini, P., "Israil vs Iran. The strategic importance of 5th domain, the cyberspace", 30 October 2012, accessed 31 October 2012 <http://securityaffairs.co/wordpress/9856/cyber-warfare-2/israel-vs-iran-the-strategic-importance-of-5-domainthe-cyberspace.html/>
[8] Star Gazete web site, accessed 08 October 2012, <http://www.stargazete.com/politika/tsk-ve-natonun-siber-guvenlikte-isbirligi-var/haber-631491/>
[9] US White House, "Cyberspace Policy Review", May 2009
[10] Interpromedya News Center, "No Cyber Security without Awareness", accessed 02 November 2012, <http://www.bthaber.com.tr/?p=10979/>
[11] Tettersall, A., Düven, A., "Russia and China: Against Cyber Space Conference", accessed 02 November 2012, <http://www.dha.com.tr/haberdetay.asp?Newsid=230255/>
[12] Şentürk, H., Çil, C. Z., Sağıroğlu, Ş., "A Proposal for a Cyber Security Macro Analysis Model and Analysis of Turkey", 5th International Conference on Information Security and Cryptology, 15-17 May 2012, Ankara, Turkey.
[13] Marsan, C. D. "10 Things You Didn't Know About Cyber Warfare", Network World, June 08 2009, accessed 01 November 2012, <http://www.networkworld.com/news/2009/060809-cyberwarfare.html/>
[14] Gökpınar, E. S. "Networks and War", Cyber Warfare Symposium, Ankara, Turkey, 10 December 2009
[15] Arquilla, J., Ronfeldt, D., "In Athena's Camp, Preparing for Conflict in the Information Age Ch.2 : Cyberwar is Coming", RAND Corporation, 1997
[16] Libicki, M. C. "Cyberdeterrence and Cyberwar", RAND Corporation, 2009
[17] Mulligan, D. K., Schneider, F. B., "Doctrine for Cybersecurity", 15 May 2011
[18] 3rd International Conference on Information Security and Cryptology, 25-27 December 2008, Ankara, Turkey, <http://www.iscturkey.org/2010/2008/index.php?id=sonuc>
[19] US White House, "The National Strategy to Secure Cyber Space", February 2003
[20] US White House, "The Comprehensive National Cybersecurity Initiative", accessed 03 November 2012, <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative/>
[21] US White House, "International Strategy for Cyberspace", May 2011.
[22] UK Office of Cyber Security, "Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space", June 2009, accessed 03 November 2012, <http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf/>
[23] UK Office of Cyber Security, Written Ministerial Statement regarding UK Cyber Security Strategy, 2011, accessed 03 November 2012,

<http://www.cabinetoffice.gov.uk/sites/default/files/resources/WMS_The_UK_Cyber_Security_Strategy.pdf/>

[24] Cyber Security Strategy for Germany, February 2011,accessed 03 November 2012, <http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile/>

[25] Australian Government Cyber Security Strategy, ISBN: 978-1-921241-99-4, 2009, accessed 03 November 2012, <http://www.ag.gov.au/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf/>

[26] French Network and Information Security Agency (FNISA), "France's Strategy : Information Systems Defense and Security", February 2011, accessed 03 November 2012, <http://www.enisa.europa.eu/media/news-items/Information_system_security_France_strategy.pdf/>

[27] Netherlands National Cyber Security Strategy : Success Through Cooperation, 2011, accessed 03 November 2012, <http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011/>

[28] Sağıroğlu, Ş., "Cyber Security and Turkey", Cyber Security Workshop, 29 September 2011, Ankara, Turkey.

[29] Information Security Association web site, accessed 23 December 2012, <http://www.bilgiguvenligi.org.tr/duyurular.html/>

[30] Draft Turkish Cyber Security Strategy Document, accessed 23 December 2012, <http://www.bilgiguvenligi.org.tr/index_files/pdf/Ulusal_Siber_Guvenlik_Stratejisi.pdf/>

[31] Karabacak, B., "Cyber Threats against Critical Infrastructures and Recommendations for Turkey", Cyber Security Workshop, 29 September 2011, Ankara

[32] SPO Information Strategy Annex and Information Society Action Plan, 2006

[33] SPO Information Society Strategy Action Plan (2006-2010) Assessment Report, Nr.:5, Ankara, March 2010.

[34] Ünver, M., Canbay, C., Mirzaoğlu, A. G., "Ensuring Cyber Security", BTK Report, Turkey, May 2009 (in Turkish).

[35] Carr, J., "Inside Cyber Warfare : Mapping the Cyber Underworld", ISBN : 978-0-596-80215-8, 2010

[36] Turkish Cabinet Decision Nr. 2012/3842, published in Official Gazette of Republic of Turkey, 20 October 2012.

[37] Law No 5809, Electronic Communications Law, 10 November 2008

[38] Office of Prime Minister, KKGM, B.02.0.KKG.0.10/101-902/1812, 22 April 2008.

[39] Eriş, M., "Turkey Computer Incident Response Center Coordination Center" 3. TÜBİTAK-UEKAE Information Technologies Security Conference, 06 June 2008

[40] Tatar, Ü., "TR-BOME Studies against Cyber Threats", İstanbul Information Security Conference, 10 June 2009

[41] Bircan, B., "Cyber Space Defense Center (SOSAM)", 3. TÜBİTAK-UEKAE Information Technologies Security Conference, 06 June 2008

[42] Information Security Academy web site, accessed 09 March 2012, <http://blog.bga.com.tr/duyurular/bga-siber-guvenlik-kampi-ilk-mezunlarini-verdi/>

[43] CEH Turkey web site, accessed 09 March 2012, <http://www.cehturkiye.com/index.php/ceh-turkiye-hakkinda/>

[44] Ulaşanoğlu, M. E., Yılmaz, R., Tekin, M. A., "Information Security: Risks and Recommendations", August 2010

[45] TÜBİTAK Web Site, accessed 03 November 2012, <http://www.tubitak.gov.tr/sid/0/cid/21886/index.htm;jsessionid=122D580937878F69C4C9D54A5A49B706/>

[46] McAfee, "Virtual Criminology Report, 2009", accessed 03 November 2012, <http://resources.mcafee.com/content/NACriminologyReport2009NF/>

[47] Jancewzski, L. J., Colarik, A. M., "Cyber Warfare and Cyber Terrorism", ISBN : 978-1-59140-992-2, 2008

[48] Gürkaynak, M., İren, A. A., "Virtual Dilemma in Real World: International Relations in Cyber Area", Süleyman Demirel University, Journal of Economics and Administrative Sciences, 2011-16, I.2, p.263-279.

[49] Clarke, R. A., "Cyberwar: The Next Threat to National Security and What to Do About It", ISBN-13: 978-0061962233, 20 April 2010

[50] Keggier, J., Mahon, T., "Preparing for Cybergeddon", Armada International, s: 34-36, 01 Nisan 2009.

[51] Undersecretariat for Defense Industries web site, accessed on 08 October 2012, accessed 01 November 2012, <http://www.ssm.gov.tr/anasayfa/hizli/duyurular/etkinlikler/torenler/Sayfalar/20122507ButSbrGuvSist.aspx/>

[52] Conference on Cyberspace, 01-02 November 2011, London, <http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/>

[53] Bensghir, T. K., "E-Transformation and E-Signature Applications", TODAİE e-Government E-İmza Seminar, 16-17 November 2011, Ankara

[54] Starcom MediaVest Group (SMG) Connected web site, accessed 09 April 2012, "Smart Phone Use of Turkish Consumer", accessed 03 November 2012, <http://smgconnected.com/turk-tuketicisinin-akilli-telefon-kullanimi/>

[55] Turkish Cabinet Decision Nr. 2008/13685, published in Official Gazette of Republic of Turkey, 16 June 2008.

[56] Symantec "Global Internet Security Threat Report, Trends for 2008. Vol. XIV", April, 2009

[57] Üneri, M., "Computer Security and Internet", July 2009, accessed 03 November 2012, <http://www.bilgitoplumu.gov.tr/Documents/1/Icra_Kurulu/090715_IK27.ToplantisiInternetVeBilgisayarGuvenligi.pdf/>

[58] Zetter, K., "State-Sponsored Malware 'Flame' Has Smaller, More Devious Cousin", 15 October 2012, accessed 18 October 2012, <http://www.wired.com/threatlevel/2012/10/miniflame-espionage-tool/>

[59] Kaspersky Lab web site, "Kaspersky Lab Discovers "miniFlame," a New Malicious Program Designed for Highly Targeted Cyber Espionage Operations", 15 October 2012, accessed 18 October 2012, <http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_Discovers_miniFlame_a_New_Malicious_Program_Designed_for_Highly_Targeted_Cyber_Espionage_Operations/>

[60] Hoover, N. J., "Defense Bill Approves Offensive Cyber Warfare", Information Week, 05 January 2012

[61] Özenç, K., Alkan, M., Acarer, T., "Legal and Technical Approach to International Security of a Nation", 3rd International Conference on Information Security and Cryptology, 25-27 December 2008, Ankara

[62] Cyber Security Law Workshop, 26-27 January 2012, Ankara, accessed 03 November 2012, <http://www.iscturkey.org/calistay/2/>

[63] Hoover, N. J., "DARPA Boosts Cybersecurity Research Spending 50%", Information Week, 07 November 2011

[64] IT in Defense Conference, 07 February 2012, accessed 03 November 2012, <http://www.interpromedya.com.tr/savunmadabilisim/?p=777/>

[65] Vural, Y., Sağıroğlu, Ş., "National Information Security", 3rd International Conference on Information Security and Cryptology, 25-27 December 2008, Ankara

[66] Anıl, S., "Cyber Security in NATO and Nations", Turkish Symposium on War on Digital Media, Ankara, Turkey. 10 December 2009.

[67] Keith B. A., "Letter to Senator McCain", accessed 20 October 2012, <http://info.publicintelligence.net/CYBERCOM-McCainLetter.pdf/>

[68] Sung, K., J., "Cyber Warfare Command to Be Launched in January". Koreatimes.co.kr., accessed 22 October 2012,<http://www.koreatimes.co.kr/www/news/nation/2009/12/205_56502.html/>

[69] Gündoğan, M., "Cyber Weapon Industry and Turkey", Cyber Security Conference, 22 December 2011, Ankara.