2009

Critical infrastructure protection status and action items of Turkey

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

Sevgi Ozkan
Middle East Technical University

CRITICAL INFRASTRUCTURE PROTECTION STATUS AND ACTION ITEMS OF TURKEY

Bilge KARABACAK* - Sevgi OZKAN**

Abstract

Critical infrastructures are the physical and virtual systems essential to the minimum operations of the economy and the government. Critical Infrastructure Protection (CIP) is a critical agenda item for governments in the developed countries. In these countries, policies and procedures on CIP are already in place and required laws are in action as well. In Turkey, some official introductory studies have been performed in 2009. However, there are a number of steps that Turkey still has to take. In this study, key definitions are provided firstly. After the definitions, the efforts of USA, EU, OECD and NATO are summarized. The last two sections of the paper are dedicated to the steps taken by Turkey and the challenges still ahead Turkey.

Keywords: Critical infrastructures, critical infrastructure protection, cyber defense, cyber threat

1. INTRODUCTION

Governments, organizations, societies and individuals have increasingly dependent on information and communications technologies (ICT). ICT has brought both advantages and a new threat type called cyber threat into our lives. There are a number of countermeasures from individual level to governmental level in order to cope with cyber threats. Critical infrastructure protection is one of the crucial areas in which governments have to take action in order to cope with cyber threats. Critical infrastructures are those physical and cyber-based systems essential to the minimum operation of the economy and the government. Some examples of critical infrastructures are telecommunication infrastructures, energy production and distribution systems, banking and finance systems, transportation, water systems and emergency services. These services can be operated by a public organization or a private organization. The term of "critical infrastructure" is proposed after the widespread use of ICT [1]. Critical infrastructures and ICT have strong relationships in many different ways and levels [2]. Some critical infrastructures such as telecommunication infrastructures are composed of ICT entirely. Because of the strong relationship between these two concepts, a new term named "critical information infrastructure" was proposed and has been used by some organizations. OECD is one of these organizations. The expression "critical information infrastructures" is less commonly used in national policies, strategies and structures [3]. Critical information infrastructures are the information

* TÜBİTAK-UEKAE, ANKARA, bilge@uekae.tubitak.gov.tr

** METU-II, ANKARA, sozkan@ii.metu.edu.tr

networks and systems, the failure of which would have a serious impact on the health, safety, security, economic well-being of citizens, or the effective functioning of government or the economy [3]. Critical information infrastructures are also critical infrastructures in fact. In recent years, there are some academic studies that categorize Internet as a critical infrastructure as well [4, 5]. As a last remark, there are a number of relationships and dependencies among critical infrastructures [6]. ICT has started some of the relations and dependencies and has increased some others significantly.

The organization of this paper is as follow. The efforts of USA, EU, OECD and NATO are shared in the second section. The third section is about the efforts of Turkey that has taken place in 2009. The fourth section contains the possible future work that Turkey has to perform. The last section of the paper is the conclusion.

2. THE EFFORTS OF USA, EU, OECD AND NATO

The term "critical infrastructure" was first used in the document titled "Critical Foundations: Protecting America's Infrastructures" by the United States of America in October 1997 [7]. The subtitle of the document was "The Report of the President's Commission on Critical Infrastructure Protection". As stated at the beginning of this report, the president of the USA had asked to prepare such a report. The 192 pages report was composed of 12 sections and it was prepared by a number of public servants, academicians and private sector workers. The report contains mainly key definitions, as-is analysis and to-be analysis about critical infrastructure protection. After seven months, Presidential Decision Directive, code named NSC-63, was released in 22th May, 1998 [1, 8]. The report was signed by the president of USA. This directive was sent to all of the departments that either manage a critical infrastructure or are related with the national security. In this directive, the intent of the president, national goals, the list of critical infrastructures, the steps that should be taken by the departments and the issues related to coordination were covered.

The Homeland Security Act of 2002 made the Department of Homeland Security responsible for coordinating national efforts to protect critical infrastructure across all sectors, including information technology and telecommunications systems [9].

As another document; "The National Strategy to Secure Cyberspace" was prepared by the White House and dated February 2003. This document strongly relates the ICT with the critical infrastructures. The strategy document states that cyberspace is the nervous system of the critical infrastructures [10]. This document is an implementation component of the document titled "National Strategy for Homeland Security" and is complemented by another document titled "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" [10, 11, 12]. "National Strategy for Homeland Security" was prepared by the White

House, signed by president and released in July 2002. This formal document contains a number of policy statements about critical infrastructure protection, such as the roles of private sector, ensuring the resilience of infrastructures, preventing and disrupting terrorist attacks to critical infrastructures, recovering from the incidents and taking protective measures.

As a recent development, the president of the USA directed the national security and homeland security advisors to conduct immediate 60-day cyber security review in February 9th, 2009. The report of the review is released in the website of the White House [9]. This report also contains important future actions about critical infrastructures. It is stated that regulatory measures might be taken in order to increase information sharing capabilities for robust and resilient critical infrastructures, the Federal government should work with the private sector to define public-private partnership roles and responsibilities for the defense of privately owned critical infrastructures, the Federal government also should consider extending the availability of federal identity management systems to operators of critical infrastructure and to private-sector emergency response and repair service providers for use during national emergencies.

The studies within European Union dates back to 2004. The European Council asked the European Commission for the preparation of an overall strategy to protect critical infrastructures of Europe in June 2004. The European Commission adopted a document titled "Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight against Terrorism" which put forward suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving Critical Infrastructures [13]. The date of the document was 20th October, 2004. In this eleven page document, the threat is defined, the possible critical infrastructures of Europe are listed, security management initiatives are specified and most importantly European Programme for Critical Infrastructure Protection (EPCIP) is introduced.

On 17th November, 2005 the European Commission adopted a paper on EPCIP which provided policy options on the establishment of the EPCIP [14]. In April 2007, the European Council adopted conclusions on the EPCIP. It is said that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders. After this date, European Commission continued to develop a European procedure for the identification and designation of European critical infrastructures (ECI) and the assessment of the need to improve their protection.

After the completion of the procedure, the European Council Directive 2008/114/EC constituted a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection [15]. The title of this directive is "on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection". The

Directive concentrated on the energy and transport sectors without neglecting ICT. Thus the key element of EPCIP is this Directive which identifies the ICT sector as a future priority sector.

The latest document prepared by the European Commission is dated 30th March, 2009, entitled "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". The document was a communication from the European Commission to the European Parliament, the Council of Europe, the European Economic and Social Committee and the Committee of the Regions. The report contains the challenges of Europe and an action plan amongst other things [16].

OECD (Organization of Economic Cooperation and Development) has collaborative studies and documents about critical information infrastructure protection (CIIP). "Working Party on Information Security and Privacy-WPISP" of the OECD prepared a report titled "Recommendation of the Council on Protection of Critical Information Infrastructures" in January 2008 [3]. The European Commission has also benefited from this document [16]. The OECD document provides guidance on the protection of critical information infrastructures for member countries and all other countries in the world. The suggestions are divided into two parts. The first part is the protection of critical information infrastructures (CII) at the domestic level; the second part is protecting critical information infrastructures across borders. Thus, the document provides guidance on both national policies and international cooperation for the protection of CII. The recommendation document derived from the best practices identified in an OECD comparative study of CII policies in seven countries (Australia, Canada, Korea, Japan, The Netherlands, the United Kingdom and the United States) [17]. OECD WPISP urges applicant countries to comply with some crucial information security practices [18]. One of these practices is related with the critical infrastructure protection. As founding member, Turkey does not comply with these security practices. The questions about CII that are expected to be answered by applicant countries are listed below:

- Has your government created a policy and strategy related to the protection of CII?
- Does your government provide leadership and commitment to protect critical information infrastructures in government, private businesses and individual users?
- Has your government assigned specific roles and responsibilities for the protection of CIIs.
- Has your government created management structures for the different aspects of protecting CIIs?
- Has your government implemented programs and initiatives to promote awareness, educate and train government, private business and individual users in CIIP?

Almost all of the OECD and EU member countries have governmental studies on critical infrastructure protection. In these countries, new regulations are enacted, some present regulations are changed, new institutions are established and the coordinators are designated. These activities are started by the directive of president/prime minister and continued in the sponsorship of top level. It is acknowledged at these countries that the protection of national critical information infrastructures is one of the main drivers for developing a culture of security at the national level [19].

Regarding NATO activities in critical infrastructure protection; after the coordinated cyber attacks targeting the Internet infrastructure of Estonia in April and May 2007 by Russian hackers, some important steps had been taken by NATO and member countries. First of all NATO Cyber Defense Management Authority (CDMA) had been established in Brussels and started operations. The ratification of NATO Cyber Defense Concept had been completed as well. Within the scope of the Cyber Defense Concept of NATO, member countries had notified the CDMA about the National Contact Point (NCP) for cyber security. Also, according to the Cyber Defense Concept, member countries started to prepare national cyber defense policies.

3. THE EFFORTS OF TURKEY

In this section, two introductory studies about critical infrastructure protection are shared with the reader.

As a commitment to the Cyber Defense Concept of NATO mentioned in the previous section, Turkey has prepared the National Cyber Defense Policy in 2009. National Research Institute of Electronics and Cryptology (NRIEC) had been designated by Prime Ministry as the coordinator body for the preparation of the National Cyber Defense Policy of Turkey in May 2008. After this date, the policy had been prepared by 19 public organizations and delivered to the Prime Ministry in February 2009. The draft policy document has been waiting the approval of the Prime Ministry of Turkey. The draft policy document is the first formal study about critical infrastructure protection in Turkey. The following sentences are excerpts from the policy document: "the security of the critical ICT infrastructures has to be implemented. The critical ICT infrastructures of Turkey, the dependencies and criticality levels of them and the responsibilities have to be determined. The critical ICT infrastructures have to be protected against cyber threats."

More progress about CIP was made in the autumn of 2009. During inauguration of the eGovernment portal in 18th December, 2008, the Turkish Prime Ministry announced the formation of a new commission. The responsibility of the commission was described as to determine if public service infrastructures were compatible with the requirements of the information society and to determine and propose the changes to enacted regulations and to propose new regulations. The commission is established within the General Directorate of Laws and

Regulations of the Prime Ministry of Turkey by the participation of designated public organizations. The commission is called "eGovernment regulations working group". The working group become active on the 3rd of March, 2009. The working group prepared the "The draft of law of eGovernment and information society" in 7th August, 2009. The institutional and individual comments had been welcomed until 15th September, 2009. It is expected that the draft will be sent to the council of ministers shortly and to be enacted at the end of 2009 or at the beginning of 2010. The draft law does not contain the expressions "critical infrastructures" or "critical information infrastructure". On the other hand, the term "critical information system" is described as "those information systems that the partial or complete loss of functionality would affect the public safety and order adversely". This definition is in complete accordance with the definitions of critical information infrastructures. According to the draft law, a new institution called "Information Society Agency" is proposed to be established. One of the tasks of the "department of information society" which is placed under the "Information Society Agency" is to determine critical information systems and to decide the minimum security standards to be applied to those systems.

As a result, Turkey is at the beginning of the studies about critical infrastructure protection and critical information infrastructure protection. Turkey has a lot of work to do in this challenging area. The studies that have to be performed by Turkey and the challenges of Turkey are listed at the next section.

4. THE "TO DO" LIST AND CHALLENGES OF TURKEY

This section is composed of two bulleted lists. One of the lists is about the challenges of Turkey. The second bulleted list contains the more technical items that Turkey has to perform after overcoming the challenges. The second list is prepared by the help of guidance documents of developed countries and multi-national organizations [1, 3, 16].

The challenges of Turkey:

- Commitment at the highest levels (such as Prime Ministry)
- Formalization of the draft "National Cyber Security Policy"
- Preparation of the "National Cyber Security Strategy" and the "National Cyber Security Action Plan" (After the formalization of the "National Cyber Security Policy")
- Enactment of "The Draft of Law of eGovernment and Information Society"
- Harmonization with the OECD principles
- Preparation of the policy document about critical infrastructure protection
- Allocation of sufficient budget to support the studies

The list of items that Turkey has to perform:

The prerequisite of the items under this heading is the challenges of Turkey listed above. Thus, without overcoming the challenges, the bulleted items are definitely condemned to fail.

- Collaboration and coordination with private sector
- Establishment of a center that coordinates the studies related with the critical infrastructures
- Determination and designation of roles and responsibilities
- Performing a country wide risk analysis in order to determine the critical infrastructures and their dependencies
- Establishment of a partnership between government and the operators critical infrastructures (public or private) in order to share information
- Performing periodical security tests and exercises in order to determine vulnerabilities and to take countermeasures
- Performing training, education and awareness activities in order to build capacity for secure digital nation
- Establishment of international cooperation with other countries and multinational organizations
- Support for research and development activities
- Establishment of strong and country wide CERTs (Computer Emergency Response Team)

5. CONCLUSION

To conclude, Turkey has been adopting technology and as a result digitalizing rapidly. It is crucial to develop and advance a critical infrastructure protection program of Turkey as done by developed countries. There are some international organizations that Turkey is already a member of and those organizations have strong know-how and a number of guidance documents for CIP. Turkey should not lose time in this important area, because the levels of cyber threats have been increasing each passing day depending on the developments and proliferation of technology. As a first step, Turkey has to take some fundamental steps that are listed under the challenges heading of section four. After overcoming these challenges, Turkey has to perform the items listed under the fourth section to bring its critical infrastructure protection preparedness level to accepted worldwide norms

6. REFERENCES

[1] USA Presidential Decision Directive/NCS-63, "http://www.fas.org/irp/offdocs/pdd/-pdd-63.htm", 1998 (accesses on 30th October, 2009)

[2] Jayawickrama, W., "Managing Critical Information Infrastructure Security Compliance: A Standard Based Approach Using ISO/IEC 17799 and 27001", Book Chapter: On the Move

to Meaningful Internet Systems 2006: OTM 2006 Workshops, Vol. 4277/2006, p. 565-574, 2006.

[3] OECD Recommendations of the Council on the Protection of Critical Information Infrastructures, 2008.

[4] Beltran F., Fontenay A., Alameida M. W., "Internet as a critical infrastructure: lessons from the backbone experience in South America", Communications & Strategies, No. 58, 2005

[5] Fischer W., Lepperhoff N., "Can Critical Infrastructure rely on the Internet", Computers & Security, Cilt. 24, s. 485-491, 2005.

[6] Lewis T. G., "Critical Infrastructure Protection in Homeland Security - Defending A Networked Nation", A John Wiley & Sons, Inc., Publication, 2006.

[7] The Report of the President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, 1997

[8] Jones A., "Critical Infrastructure Protection", Computer Fraud & Security, p. 11-15, April 2007.

[9] Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure, PDF doküman Internet adresi: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accesses on 30th October, 2009)

[10] The White House, Washington, The National Strategy to Secure Cyberspace, 2003 http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (accesses on 30th October, 2009).

[11] The White House, Washington, The National Strategy for Homeland Security, 2002 http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (accesses on 30th October, 2009).

[12] The White House, Washington, National Strategy for Physical Protection of Critical Infrastructure and Key Assets, 2003, http://www.dhs.gov/xlibrary/assets-/Physical_Strategy.pdf (accesses on 30th October, 2009).

[13] Commission of the European Communities, "Communication from the Commission to the Council and the European Parliament, Critical Infrastructure Protection in the Fight Against Terrorism- COM(2004) 702 final", 2004.

[14] Commission of the European Communities, "Green Paper on a European Programme for Critical Infrastructure Protection - COM(2005) 576 final", 2005.

[15] European Council Directive 2008/114/EC, "on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection", Official Journal of the European Union, 2008.

[16] Commission of the European Communities, "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience- COM(2009) 149 final", 2009.

[17] OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Development of Policies for Protection of Critical Information Infrastructures, 2007.

[18] OECD, Committee for Information, Computer and Communications Policy, "Fact Finding Questionnaire for Candidate Countries to Accession", 2008.

[19] OECD, "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries", OECD Digital Economy Papers, No. 102, OECD publishing, doi:10.1787/232017148827, 2005.