2016

Regulatory approaches for cyber security of critical infrastructures: The case of Turkey

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

Sevgi Ozkan Yildirim
Middle East Technical University

Nazife Baykal
Middle East Technical University

Recommended Citation

Karabacak, B., Ozkan Yildirim, S., & Baykal, N. (2016). Regulatory approaches for cyber security of critical infrastructures: The case of Turkey. *Computer Law & Security Review, 32* (3), 526-539. https://doi.org/10.1016/j.clsr.2016.02.005

COMPUTER LAW & SECURITY REVIEW ■■ (2016) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Regulatory approaches for cyber security of critical infrastructures: The case of Turkey

Bilge Karabacak *, Sevgi O. Yildirim, Nazife Baykal

Graduate School of Informatics, Middle East Technical University, Universiteler Mah., Ankara, Turkey

Keywords:
Cyber security
Critical infrastructures
Critical infrastructure protection
National security
Regulation
Regulatory agency
Delphi survey
Grounded theory method
Focus group interview

A B S T R A C T

Critical infrastructures are vital assets for public safety, economic welfare and/or national security of countries. Today, cyber systems are extensively used to control and monitor critical infrastructures. A considerable amount of the infrastructures are connected to the Internet over corporate networks. Therefore, cyber security is an important item for the national security agendas of several countries. The enforcement of security principles on the critical infrastructure operators through the regulations is a still-debated topic. There are several academic and governmental studies that analyze the possible regulatory approaches for the security of the critical infrastructures. Although most of them favor the market-oriented approaches, some argue the necessity of government interventions. This paper presents a three phased-research to identify the suitable regulatory approach for the critical infrastructures of Turkey. First of all, the data of the critical infrastructures of Turkey are qualitatively analyzed, by using grounded theory method, to extract the vulnerabilities associated with the critical infrastructures. Secondly, a Delphi survey is conducted with six experts to extract the required regulations to mitigate the vulnerabilities. Finally, a focus group interview is conducted with the employees of the critical infrastructures to specify the suitable regulatory approaches for the critical infrastructures of Turkey. The results of the research show that the critical infrastructure operators of Turkey, including privately held operators, are mainly in favor of regulations.

1. Introduction

Any physical or cyber infrastructure is called a critical infrastructure if damage to that infrastructure will have a harmful effect on the economy, social order and/or national security of a country (USA, 2001). The term "critical infrastructure" was first used by the Executive Order of President of United States in 1996 (The White House, 1996). The executive order underlined two types of threats against critical infrastructures: physical and cyber threats.

Cyber space has been growing wider with every passing day through the participation of organizations and individuals all over the world into it. Along with the growth of cyber space, the probability of abuses by malicious users, groups, and even states increases as well (Deibert and Rohozinski, 2010). Until now, a number of cyber attacks against critical infrastructures like nuclear plants, electrical grids, sewing infrastructures, flight control systems and harbors have been reported (Condron, 2007; Farwell and Rohozinski, 2011). Malicious actors have been increasing their capabilities to acquire asymmetrical results on their behalf (Friedman, 2013). Asymmetrical cyber threats

* Corresponding author. 37200 Paseo Padre Parkway, Apt 252, Fremont, CA 94536, USA. Tel.: +1 408 816 0621; fax: +1 561 423 6345.
E-mail address: bilgek@gmail.com (B. Karabacak).

http://dx.doi.org/10.1016/j.clsr.2016.02.005

Please cite this article in press as: Bilge Karabacak, Sevgi O. Yildirim, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005

may cause serious harm to a critical infrastructure of a country at really low costs. No critical infrastructure in cyber space is untouchable, regardless of the country it belongs to. As a matter of fact, critical infrastructures of developed countries are more prone to the impact of cyber threats, as technological infrastructure of those countries are more prevalent and sophisticated (Clarke and Knake, 2010).

Today, cyber threats are some sort of a national security problem (Svete, 2012). Struggling with cyber threats requires large-scale efforts, which are organized by states and sustained through the cooperation among national actors (Nissenbaum, 2005). The practical reflection of those large-scale efforts is the inclusion of the cyber threats in the national security strategies of the countries (Robinson et al., 2013). Thus, critical infrastructure protection is one of the most important chapters of the national infrastructure strategies.

Ensuring cyber resilience of critical infrastructures is a prominent and difficult part of the national security efforts of countries (Young, 2012). The difficulties stem not only from the peculiarities of the cyber threats, but also from the critical infrastructure ownerships. Critical infrastructures are mostly owned and operated by private entities in developed countries. For example, the percentage of the private sector ownership of the infrastructures in the US was 85% eight years ago (de Bruijne and van Eeten, 2007). Therefore, the security of the non-state actors such as the private sector is closely related to national security in the digital era, which was not the case before (Andress, 2003).

The enforcement of security rules on critical infrastructure operators is a part of cyber resiliency efforts of countries. There are a couple of models, from market provision to government ownership, for critical infrastructure protection (Assaf, 2008). Strong government supervision on critical infrastructures for cyber resilience may seem trivial at first sight; however, it is a challenging issue for the governments of developed countries due to power and lobbying of private sector. Therefore, critical infrastructure protection is one of the most controversial aspects of national security domain because of the superiority of private sector in the ownership of infrastructures.

The number of academic studies that are about regulatory approaches on critical infrastructures is limited. Current studies are generally done by academics in developed democratic countries and they put non-regulatory notions like cooperation and innovation above regulations. It is underlined that collaboration of public and private entities in cyber security is important for national security (Hansen and Nissenbaum, 2009). The participation of non-state actors like private sector and even individuals in national cyber security concepts is a new phenomenon for decision makers (Brechbühl et al., 2010; Kramer, 2013; Mitchell, 2013; Stavridis and Farkas, 2012). Although the idea of non-regulation has gained wider acceptance in developed countries, there are still clear objections to that idea by some security experts and government officials (Wikipedia Contributors, 2015).

Cyber systems are used significantly in the energy, telecommunications, finance, government services, transportation, and water management sectors in Turkey. In spite of the recent national efforts, critical infrastructures of Turkey have still significant vulnerabilities that make systems prone to cyber threats. The principal author of this article made a PhD research that covered cyber security of the critical infrastructures of Turkey. In the PhD research, through grounded theory method, the root causes of the susceptibility of the critical infrastructures to cyber threats are extracted by an analysis of the data of a state-sponsored project. Secondly, the set of cyber security principles are specified through the use of expert opinion in a five-phased Delphi survey. Seven of the principles are the regulations on the cyber security of the critical infrastructures. Thirdly, the regulatory approaches for those regulations are determined by conducting a focus group interview with nine employees of critical infrastructure operators from six different critical sectors. Thirdly, part of the research is performed after the completion of the PhD research as a follow-up study.

The outcomes of focus group interviews demonstrated that critical infrastructure operators of Turkey support cyber security regulations. The representatives of the private energy firm, the telecommunications and finance sectors stated that regulations ensure an acceptable level of security that is formed by the participation of all operators in a critical sector. They also pointed out that the operators should express their opinions on the processes, engage more in the determination of the regulations, and concur with the regulatory agency. The remaining operators in the sector, which were all public, emphasized the guidance of regulations. They stated that their roles and responsibilities should be defined by laws and regulations so that the managers can allocate sufficient budget and manpower for the purpose.

Turkey has a considerable amount of private operators especially in finance, telecommunications and energy sectors. Because the majority of the current academic studies cover the cases of the developed countries, they mainly argue the importance of market oriented approaches. In this regard, we believe that our study has some unique findings that are the reflection of a peculiar situation of Turkey. Those findings also confirm that there is no unique approach to regulatory approaches for critical infrastructures' cyber security.

The article is organized as follows: The recent discussions on the approaches of cyber security regulation toward critical infrastructures are summarized in the next section. The third section touches upon the legislative and organizational structures of Turkey. The fourth section is dedicated to the details and findings of the three-phased research process. The fifth section is allocated for the discussions of the results. The sixth section is for the assumptions, limitations, and delimitations part of the research. The last section is dedicated to future research implications.

2. Hot topic of the developed world: regulation or innovation?

There are two perspectives on the regulation of the critical infrastructures in terms of cyber security. This situation can sometimes be viewed as a dilemma for the governments (Orlowski, 2001). On one side, some security experts and government officials think that regulations are imperative to protect the critical infrastructures. On the other side, private sector executives claim that regulations are the obstacles in front of the

Please cite this article in press as: Bilge Karabacak, Sevgi O. Yildirim, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005

innovations in cyber security. Executives assert that we should cooperate instead of regulate. The disputes increase in line with the infrastructure ownership of the private sector.

The dilemma was experienced in the proposal of the Cybersecurity Act of 2012 in the US. The original version of the act imposed mandatory security standards on critical infrastructure owners. It also involved information sharing with the military. The private sector criticized the proposal for these obligations. As a result of the critiques, the proposal was altered to reflect changes as the voluntary participation of the private sector and stronger government incentives (Hiller and Russell, 2013). In spite of these changes in favor of the private sector, the Cybersecurity Act of 2012 failed to pass the US Senate, although it was endorsed by the White House (Kelly, 2012). After the dispute of the Cybersecurity Act of 2012, Executive Order 13636 was released by the White House in February 2013 (The White House, 2013). The title of the EO was "Improving Critical Infrastructure Cybersecurity". The main theme of the EO was to increase the public–private partnership. It assigned duties to federal agencies in sharing cyber threat information with the private sector, in coordination with the critical infrastructure owners and in collaboratively developing and implementing risk-based approaches to cyber security (DHS, 2013).

According to the current EU rules, among all critical sectors, only telecommunications sector has to adopt security measures and report significant security incidents to the government bodies (European Commission, 2013b). EU is on the way to impose government provisions on several critical infrastructure sectors of the member countries. On February 2013, European Commission prepared a proposal for a directive "concerning measures to ensure a high common level of network and information security across the Union" (European Commission, 2013a). If it is approved by the European Council and Parliament, Member States will have to implement the directive within 18 months (European Commission, 2013b). As the strongest motive of its latest proposal, the European Commission reminds the previous cyber security gaps that resulted from the voluntary nature of the past efforts. If the proposal is approved, critical infrastructure operators (from the sectors ranging from energy to healthcare) and public administrators will be required to assess the risks they face and to adopt appropriate and proportionate measures to ensure network and information security. These entities will also be required to report incidents with a significant impact on the core services provided for competent authorities (European Commission, 2013a). As a result, the directive will apply to the critical infrastructures owned by the private sector as well (Hiller and Russell, 2013).

Hiller and Russell state that countries struggle to find the best strategy and regulation for the critical infrastructures owned by the private sector (Hiller and Russell, 2013). The authors compare the approaches of the US and the EU in terms of the cyber security rules on the private sector. According to the authors, the US follows a voluntary approach for the private sector, whereas the EU adopts a relatively mandatory approach. This conclusion confirms the latest developments in the US and EU.

The approach of Australia resembles the approach of the US. According to Wilson, the Australian government has a deliberate non-regulatory approach for CIP. The liability of the protection of the infrastructure is left to the owners of the infrastructures (Wilson, 2014). The legal situation is the same for the Australian National Broadband Network, the largest infrastructure project in Australian history. There is no security strategy associated with the national broadband network. Instead of the government rules for the protection of the infrastructures, public–private partnerships as a cost-effective partnering with non-government organizations would produce positive outcomes for cyber resilience (Cook, 2010).

Dunn-Cavelty and Suter emphasize the importance self-regulating and self-organizing networks for the CIP policy. They argue that the role of the government should be far from close supervision and immediate control; rather, the government should coordinate and motivate these networks for the CIP tasks. In their article, they contrast the neoliberal governance theory and the network governance approach and argue that neoliberal governance theory is not suitable for the security-focused CIP policy since its focus is efficiency rather than security.

Assaf does not see the regulation issue of the critical infrastructures as a dilemma. Rather, he considers it a choice of governments. For him, there are two basic models for CIP: the national security model and the business continuity model (Assaf, 2008). Assaf shares an illuminating regulatory continuum to demonstrate the seven different options from the highest government intervention to the lowest. The regulatory approaches from highest government intervention to the lowest are listed as follows:

1) Government ownership
2) Command and control
3) Delegation to agency
4) Delegation to agency + negotiation
5) Enforced self-regulation
6) Voluntary self-regulation
7) Market

Assaf compares the US and Israel in terms of their governmental interventions in cyber security regulations of critical infrastructures. The US adopts the business continuity model with the exceptions in energy and chemistry sectors, whereas Israel adopts the national security model.

According to Luiijf and Klaver, no single governance model for CIP is applicable to all countries. The regulation of CIP in a country depends on its legal system, the trust level between government and private sectors, and its historical and cultural backgrounds (Luiijf and Klaver, 2004). Hence, Luiijf and Klaver corroborate the idea of Assaf. Luiijf and Klaver also mention the importance of the cooperation and collaboration efforts in both national and international domains. They also emphasize the internationally harmonized CIP efforts for multinational operators.

Orlowski also points out the regulatory approaches for the multinational infrastructures. According to Orlowski, there are two types of regulations for the CIP: protective security and criminal laws. Protective regulations should be the last resort for the free market economies. Countries with such economies should cooperate instead of regulate because they may impose different regulations on critical infrastructures according to their constitutional powers. These differences result in

Please cite this article in press as: Bilge Karabacak, Sevgi O. Yildirim, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005

Table 1 – Provisional approaches of three countries and the EU.

	Government Provision	Market Provision
US*		
EU	✓	
Israel	✓	
Australia		✓

* Except for energy and chemistry sectors.

inconsistencies at cross-border management, especially for multinational corporations. On the other hand, fighting against cybercrime is a field where a commonly accepted regulation is needed (Orlowski, 2001). Convention on Cybercrime, also known as the Budapest Convention, is an international treaty to fight against cybercrime by urging the harmonization of the domestic laws (European Council, 2001). It was signed by 33 countries: 32 members of the European Council and the US.

Table 1 summarizes the provision approaches of three countries and the EU according to the articles reviewed. The US and Australia adopt the market provision, which means minimum supervision of the government. However, energy and chemistry sectors are more strictly supervised by the US federal agencies. Israel adopts the government provision; that is, strict supervision of the market by the government. EU recently attempted to shift the paradigm from market to government provision. However, as a result, the approaches on the CIP regulation are a hot topic in the developed world. The strict government intervention and regulations on the CIP efforts is not considered as a suitable option by the academia and governments of developed countries. A number of academic studies that propose security management models for CIP originate in such countries. This topic can be summarized by the following questions: Which is suitable? Regulation or Innovation? These articles place the aspects like cooperation and innovation above regulations.

3. Regulatory and organizational structures of Turkey

In this section, the regulations of Turkey regarding cyber security and critical infrastructure sectors are reviewed.

First of all, Turkey has a civil legal system as opposed to the US and the Commonwealth countries that have a common legal system. In the civil legal system, the rules are written and structured in a hierarchy of norms. Courts give verdicts based on the codes within this enormous hierarchy.

The statute 2011/2237 on Military Forbidden Zones and Security Zones mentions the requirements of the physical security of energy, manufacturing, water management, transportation, telecommunications, intelligence, and military facilities, without using the term critical infrastructure (Turkish Cabinet, 2011). The aforementioned statute does not include any articles about the cyber security.

The Cyber Security Council of Turkey was established in October 2012, with the members from eleven governmental organizations. After the second meeting of the council in June 2013, the telecommunications, energy, water management, public services, transportation, and finance sectors were designated as national critical infrastructures of Turkey. However, the decision remained in the minutes of the meeting, without changing the existing regulations or creating a new one in Turkey (Kaska and Trinberg, 2015).

Turkey has regulatory authorities for the energy, telecommunications and finance sectors. The related agencies are autonomously managed. The government in office can appoint only some members of the boards of these agencies. The water management and transportation sectors do not have regulatory/supervision agencies unlike the energy, telecommunication and finance sectors. Therefore, these sectors are totally deprived of sector-wide rules for physical and cyber aspects.

Until the amendments passed in December 2014, there were no cyber security or information security-related articles in the statutes of the energy sector. The Energy Market Regulatory Authority amended the license regulations of the electricity, natural gas, and petroleum markets in December 2014. According to the amendments, electricity production, transmission, and distribution facilities, natural gas transmission and distribution facilities, and petroleum refineries were required to establish ISO 27001 compliant information security management systems for their information processing departments (EMRA, 2014a; EMRA, 2014b; EMRA, 2014c).

Publishing a legal annunciation, the Information and Communication Technologies Authority urged the operators to comply with ISO 27001 in the telecommunications sector in October 2010. The authority released a new and more stringent regulation for ISO 27001 compliance in July 2014 (ICTA, 2014). The statute of the Network and Information Security in the Telecommunications Sector describes the details on the external and internal audit processes, required security countermeasures and properties of the information systems that should be set up by the operators as well.

Banking Regulation and Supervision Agency published several legislations for the finance sector. In January 2008, BSRA published a legal annunciation on the information security management of the banks. The annunciation contains the provisions about information security risk management, management liabilities, internal audit, outsourcing rules, separation of the duties and several other controls (BRSA, 2007). Another regulation sets the rules for the information systems audits of the banks by the independent external auditors (BRSA, 2010).

In February 2014, the Electronic Communications Law was amended to reflect the cabinet decisions dating back to October 2012 (Turkish Cabinet, 2014). By these amendments:

a) The Cyber Security Council was defined in ECL. The Minister of Transport, Maritime Affairs and Communications was appointed as the president of the Cyber Security Council. One of the responsibilities of the Cyber Security Council was to approve the list of the critical infrastructures.
b) The cyber security roles of the Ministry of Transport, Maritime Affairs and Communications (Ministry) were defined. One of the responsibilities of the ministry was to determine the critical infrastructures, their owners and locations.

Please cite this article in press as: Bilge Karabacak, Sevgi O. Yildirim, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005

Table 2 – The summary of critical sectors of Turkey.

Critical Sector	Prominent Ownership	Has Regulatory Agency?	Has cyber security regulation?	Approach according to Assaf
Energy	Government/private sector	Yes	Limited	Delegation to agency + negotiation
Telecommunications	Private sector	Yes	Comprehensive	Delegation to agency
Finance	Private sector	Yes	Comprehensive	Delegation to agency
Transportation	Government	No	No	-
Water management	Government	No	No	-
Government services	Government	No	No	-

As a critique of the Turkish organizational structure and the legislation, it is possible to say that Turkey lacks an overarching critical infrastructure protection program that handles cyber and physical security together. By considering the establishment of a security zone around the facilities, the decree 2011/2237 considers only the physical security. The recent amendments to the ECL assign some responsibilities to the Ministry and the Cyber Security Council only on cyber security. The term "critical infrastructure" was used explicitly in the amendments. However, the amendments hold neither a definition nor a list of the critical infrastructures. Therefore, they are far from setting up a holistic critical infrastructure protection program. There is neither legislative nor organizational connection between the decree 2011/2237 and the amendments to ECL.

The recent amendments to ECL assigned some roles to the Ministry, but not the required authority. As an example, the Ministry did not have the power to audit the public organizations and the critical sectors, in the context of cyber security. According to the civil legal system, a role that is assigned to a governmental authority by a law has to be elaborated with lower level statutes. By this way, the details of the applications of the law are specified in detail. The recent amendments to ECL have not been detailed by using lower level statutes so far.

A second criticism is for the current mission of the Ministry of Transport, Maritime Affairs and Communications. The Ministry played a pioneering role in the coordination of the national cyber security governance thanks to its technical sufficiency. In most of the developed countries, the governmental agencies that have fundamental duties in national security undertake the responsibility of the coordination of the cyber security (Robinson et al., 2013). In those countries, the agencies with technical capabilities support the agencies like the ministry of interior or defense while specifying and applying the cyber security policies and strategies. In Turkey, the security policies regarding cyber issues are imposed by a non-security ministry. That practice may result in inadequacies, duplications, and leadership problems (Ikitemur, 2014).

Table 2 summarizes six critical sectors of Turkey in terms of ownership status, the existence of regulatory authority, and the existence of cyber security regulations. It is seen that the sectors that are dominated by private operators are the most thoroughly-regulated critical sectors in Turkey. These sectors have regulatory authorities as well. The critical sectors that are dominated by the government have neither cyber security regulations nor associated regulatory authorities. Therefore, it can be stated that the private sector in Turkey is controlled by regulatory authorities in a strict manner.

The telecommunications and finance sectors have the most complete and mature regulations for information security and cyber security. The research showed that there was a salient supremacy and maturity of the cyber security practices in the finance and telecommunications sectors, compared to the other "government-dominated" ones.

4. The research: from the data to the regulatory approaches

The principal author participated in a project named "Information Security Management in Critical Infrastructures" between January 2012 and December 2013. The project was funded by the Ministry of the Development of Turkey. The vulnerabilities that stem from the usage of the cyber systems in critical infrastructures were analyzed in the project. The project showed that cyber systems were used significantly in the energy, telecommunications, finance, government services, transportation, and water management sectors in Turkey. The results of the project also demonstrated that the critical infrastructures had significant vulnerabilities related to the cyber systems, in spite of the recent national efforts such as the establishment of the Cyber Security Council and the National Computer Security Incident Response organization.

The motivation to discover the possible root causes of the susceptibility of the critical infrastructures to cyber threats provided the inspiration for a PhD research. The research question was "What are the possible root causes of the susceptibility of the critical infrastructures of Turkey to cyber threats?" The question was answered by using a qualitative data analysis method named grounded theory. The second research question of the PhD was "What are the set of principles to mitigate these root causes?" The second question was answered by conducting a Delphi survey with six experts.

Ten root causes were extracted after the first phase of the research. Forty principles were extracted after the second phase, Delphi survey. Seven of the forty principles were directly related to the laws and regulations. The third phase of the research was conducted after the completion of the PhD research. At the third phase, a focus group interview was performed with nine employees from six critical sectors to determine the regulatory approaches, which are the most favorable for the operators. The overview of the whole research process is shown in Fig. 1.

Please cite this article in press as: Bilge Karabacak, Sevgi O. Yildirim, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005

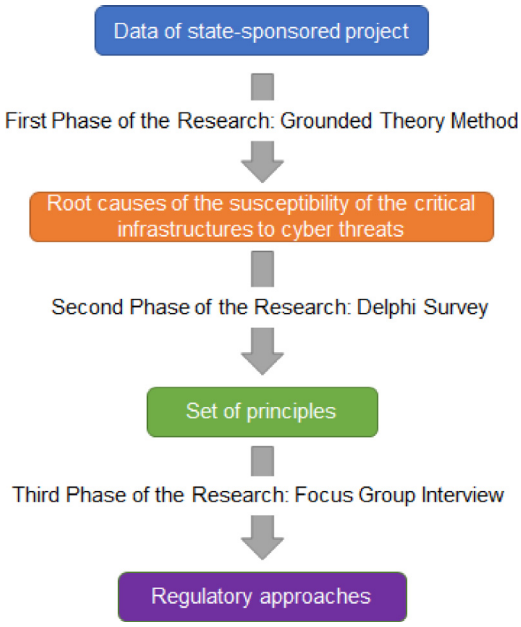

Fig. 1 – Three-phased research process.

4.1. *Grounded theory: determining the root causes of the susceptibility*

At the first phase of the research, the data were analyzed using grounded theory method (GTM), an interpretive, qualitative and inductive data analysis method. Grounded theory was proposed and used by two sociologists, Glaser and Strauss in 1967. It is the discovery of the theory through data analysis, for which it provides a detailed, rigorous, and systematic method (Jones and Alony, 2011; Strauss and Corbin, 2008). In GTM, the researcher does not begin with a hypothesis that has to be proved or disproved, but he begins "with an area of study and allows the theory to emerge from the data" (Strauss and Corbin, 2008). In GTM, the research question is a statement that identifies the phenomenon to be studied. Grounded theory has three basic steps. The qualitative data were rigorously coded and the codes are categorized in the open coding step. Categories were compared to find the themes in the axial coding step. Redundant, trivial and irrelevant themes were eliminated to extract the theory in the selective coding step.

The project data were composed of interview texts and various kinds of documents. Data collection and interviews were performed until theoretical saturation was attained. Nine semi-structured interviews were performed with the critical infrastructure owners. Interviews provided the focused, in-depth and rich data for the phenomenon under analysis. The interviews included open-ended questions about the general security posture, threats, potential vulnerabilities, applied countermeasures, and weaknesses of the interviewed organization and the critical sectors. The questions were reshaped according to the emerging categories and themes, and they were regarded as the initiators and catalyzers of the long lasting and evolving interviews. The interviewees were mid-managers and employees of the information processing departments.

Three hundred nine documents associated with ninety-one different governmental or private organizations were gathered throughout the research process. Most of these organizations were the critical infrastructure operators from the sectors of energy, telecommunications, finance, transportation, water management and government services. There were also documents that belonged to the regulatory authorities and the ministries. The collected documents were classified in five groups. These were:

a) Minutes of meeting
b) Independent evaluation report
c) Regulation text
d) Organizational report
e) News and media report

Minutes of the meeting were the notes taken during the state-sponsored project. Performed by the independent third parties, independent evaluation reports were information security audit and analysis results of the critical infrastructure owners. Regulation texts were the laws and statues that regulate the activities of critical infrastructures operators. Regulation texts provided insight into the security views and practices of the organizations. Organizational reports were the documents prepared by the organizations such as annual activity reports, annual plans, and strategic plans. Organizational reports that contained valuable information on the cyber security perceptions of the organizations were downloaded from the websites of the related organizations. News and media reports were the media excerpts related with the critical infrastructures. The principal author collected the news concerning the critical infrastructures of Turkey between 2011 and 2014. News and media reports included valuable information on the threats, the opinions of the experts, and the government officials. Minutes of meetings and independent evaluation reports were not publicly available documents. The other types of documents were publicly available for the most part.

The triangulation by using different sources of data was performed in this study for the internal validity of the research (Kaplan and Duchon, 1988). Minutes of meetings, news and media reports, and independent evaluation reports were external to the organization; they were prepared by the third parties. Organizational reports and regulation texts were internal documents prepared by the organizations.

Data collection and interviews were performed in four recursions until theoretical saturation was reached. Because grounded theory method is a process of theory discovery rather than a hypothesis testing, theoretical sampling was performed between the recursions rather than between statistical sampling (Denscombe, 2010). Using theoretical sampling, the authors reshaped the interview questions, the interviewees, the types of sectors and organizations, and the types of documents. The fourth recursion was the point where the theoretical saturation occurred. At the theoretical saturation point, the introduced data did not change the discovered theory (Shannak, 2009).

The authors exhibited the results of previous recursions to the participants of the semi-structured interviewees at the next recursion to acquire the reactions like acceptance, rejection,

Please cite this article in press as: Bilge Karabacak, Sevgi O. Yildirim, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005

Table 3 – The details of four recursions of the first phase of the research.

	First recursion	Second recursion	Third recursion	Fourth recursion
The sector of the interviewed organization*	-	Energy (G) Water management (G) Finance (P)	Government services (G) Transportation (G) Telecommunications (G, P)	Energy (P) Finance (G)
Interview questions	-	Initial set of open-ended interview questions	Reshaped and detailed interview question	Same question as the previous recursion
Analyzed document types	Publicly available documents (regulation texts, news – media report, organizational reports)	Internal documents (independent evaluation reports, minutes of meetings) Publicly available documents (regulations, organizational reports)	Internal documents (independent evaluation reports, minutes of meetings) Publicly available documents (regulations, organizational reports)	Internal documents (independent evaluation reports, minutes of meetings)
The number of analyzed documents	109	76	86	38
Coding type	Open coding	Open coding Axial coding Selective coding	Open coding Axial coding Selective coding	Open coding Axial coding Selective coding
Theory	No theory discovered	Discovery of a theory (unsaturated)	Saturation of the theory with some changes	Validation of the theory

* G: governmental organization, P: privately held organization.

and comments (Thai et al., 2012). The summary of the recursions are shown in Table 3.

After the completion of the data analysis, ten root causes were extracted. The root causes were verified by two cyber security experts, both of whom have master's degrees and over ten years of professional experience in cyber security. Expert-1 was the main organizer of the National Cyber Security Exercises in Turkey; he also took part in the esta)blishment of the National CSIRT of Turkey and directed the CSIRT for six years. Expert-2 took part in the risk analysis projects of the governmental organization and critical infrastructure owners. He took part in the national level studies of the adoption of the internationally recognized standard into the national context. The two experts agreed on the final list of root causes with some changes in the wordings of some of the root causes.

1) The cyber security of critical infrastructures is not perceived by national security authorities as a vital part of national security.
2) The culture of information sharing, collaboration and cooperation within the critical sectors and among the sectors is very limited.
3) The private sector is not perceived by the government and critical infrastructure operators as an important stakeholder in national cyber security efforts.
4) The laws of public procurements and civil servants have adverse effects on the cyber security of governmental critical infrastructure owners.
5) The number of qualified cyber security experts is limited.
6) The relationship management practices with the product/service providers are insufficient in governmental critical infrastructure operators.
7) The IT audit mechanism is very limited or does not exist in governmental critical infrastructure owners.
8) The managers of governmental critical infrastructure owners do not perceive the information security as an area of responsibility.
9) The methodical and formal risk management process is not conducted by governmental critical infrastructure owners.
10) Security is considered by governmental critical infrastructure owners as an add-on, and not as a design construct.

The data analysis in the first phase of the research also showed that:

1) Independent of the sectors, private organizations are more mature compared to the governmental organizations. Most of the extracted root causes are mainly associated with the governmental organizations.
2) The security maturity of a sector does not mainly originate from the sectorial security practices. A governmental operator in the finance sector had poor security practices. A private operator in the energy sector had state-of-the art security practices.

As a result, if a sector is dominated by private organizations, the general security posture of the sector is more mature; or vice versa. Therefore, cyber security problems may not originate from the missing cyber security practices in certain sectors; they may rather be associated with the type of organization (government or private). Therefore, the organizational dynamics like security culture and human factors may be more effective for the improvement of security.

4.2. *Delphi survey: determining the set of regulations*

After extracting the root causes, a Delphi survey was conducted by the participation of six experts. Two experts were from the private sector with ten and fifteen years of experience in cyber security. Two experts were from a governmental research institute with five and fourteen years of experience in cyber security. Two experts were from the academia with

Please cite this article in press as: Bilge Karabacak, Sevgi O. Yildirim, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005

Table 4 – Reference table for the weight values of the principles.

Score	Explanation
0	The principle is unrelated.
1	The lack of the principle can be compensated by other principles to some extent. The country improves its critical infrastructure protection efforts more slowly than expected.
2	The maturity principle is important on its own. The lack of the principle cannot be compensated by other principles. The lack of principle indicates an obvious problem for the critical infrastructure protection. Critical infrastructures will not be resilient at some parts.
3	The lack of the maturity principle indicates a major problem for the critical infrastructure protection efforts of the country because of the dependencies of the other principles on this principle. The country cannot improve the cyber resilience of the critical infrastructures.

fifteen years of experience each. The output expected from the survey was the agreement on the set of principles to mitigate the effects of the root causes.

Delphi survey was conducted by sending e-mails to six experts separately to ensure the anonymity (Okoli and Pawlowski, 2004). The survey had five consecutive rounds. Controlled opinion feedback was supplied to the respondents between the rounds by the authors (Hsu and Sandford, 2007).

At the first round, the detailed explanations of the ten root causes were given to the experts. The experts were requested to identify at least one principle for each root cause. The answers of the experts were consolidated into a single document and sent back to the experts at the second round. At the second round, the experts were requested to score the principles according to Table 4. At the next two rounds, the experts were provided the opportunity to review and change their scores by looking at the scores of the other experts. After the fourth round, a significant consensus of experts on the weights of the principles was reached. The weight values of the experts were converged into each other, compared to the results of the second and the third rounds. It is important to obtain the most reliable consensus of the opinions of the experts in Delphi surveys (Chan et al., 2001). Therefore, only the principles, which did not get zero point from any of the experts by the end of the fourth round, were selected as the potential criteria of the maturity model. Although there were fifty-eight principles with average weights between one and three, only forty-one of them got non-zero weights from the six experts by the end of fourth round of Delphi survey. A final round of Delphi survey was performed to obtain a final list of the principles, as some of the principles were close in meaning. There were both some detailed and general principles for the same topic. The experts were requested to decide on whether to eliminate these principles. The consensus of the experts was required in the elimination of a principle, which meant a principle would be eliminated only if all experts agreed on its elimination. As a result, only one principle was omitted at the fifth round. Therefore, forty principles were selected as the principles at the end of the fifth round. Among those principles, the following list of the principles was associated with the rules and regulations.

1) National or sectorial regulations that enforce the internal/external audit for critical infrastructure operators
2) Obligation of a comprehensive security standard, such as ISO 27001, for critical infrastructure owners
3) Minimum security countermeasures that are obliged by regulations for critical infrastructure owners
4) Regulations that set out the properties of information systems and security countermeasures that come into operation in critical infrastructure operators
5) Regulations that specify the inner-inter sector information sharing and cooperation principles
6) Regulations that hold top level management of critical infrastructure operators responsible for cyber security
7) Regulations that enforce critical infrastructure owners to conduct the cyber security risk management process

4.3. *Focus group interview: determining the regulatory approaches*

At the third phase of the research, a focus group interview is performed with nine employees from nine different critical infrastructure operators in six sectors. The information on the interviewees is shown in Table 5. Seven regulatory principles were extracted in the previous phase of the research. The aim of the third phase was to determine the regulatory approaches for those principles. The definitions of the organizations at the second column are written as generically as possible in order not to be revealed to public.

The interviewees were different from the ones in the first phase of the research. They were mid-managers with information assurance responsibilities in the critical infrastructure operators. Each interviewee was asked whether his/her orga-

Table 5 – Profile of interviewees.

Interviewee	Critical infrastructure Operator	Critical sector	Type
1	Electricity distribution company	Energy	Public
2	Electricity production company	Energy	Private
3	Telecommunications company	Telecommunications	Public
4	GSM company	Telecommunications	Private
5	Bank-1	Finance	Public
6	Bank-2	Finance	Private
7	Transportation operator	Transportation	Public
8	Water purification facility within a municipality	Water management	Public
9	Governmental institution (provides a critical e-government service)	Government services	Public

Please cite this article in press as: Bilge Karabacak, Sevgi O. Yildirim, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005

Table 6 – Maturity reference table.

Level	Maturity definition
1	Initial – processes unpredictable, poorly controlled and reactive.
2	Managed – processes characterized for projects and is often reactive.
3	Defined – processes characterized for the organization and is proactive.
4	Quantitatively managed – processes measured and controlled.
5	Optimized – focus on process improvement.

nization is regulated by each regulation, and if not, whether he/she would like to have that regulation. If the organization is in the effect of the similar regulation, the interviewees were asked whether they would like any change in the regulatory approach and which type of a regulatory approach would be more suitable for their organization. Group members were free to interact with each other throughout the whole interview process.

The interviewees were selected by convenience sampling. The researcher contacted with the interviewees who were conveniently accessible rather than barely reachable ones (Marshall, 1996).

The first question directed to each interviewee was "How do you see the maturity of your organization's security practices based on the maturity levels of Capability Maturity Model Integration (CMMI) framework?" The definitions of five CMMI maturity levels are shown in Table 6 (Ahem et al., 2008).

Some of the selected security processes of each critical infrastructure operator are assessed in the light of the CMMI framework. The maturity levels of each operator in Table 7 is agreed upon both by the authors and interviewees.

5. Findings and discussions

One of the findings in the first phase of the research was the higher maturity level of the private critical infrastructure operators in terms of cyber security, compared to the governmental operators. That finding corroborates the maturity values in Table 7. Most of the extracted root causes were mainly associated with the governmental organizations. As an example, during the interviews at the third phase of the research, two interviewees from the finance sector (one from the public, the other from the private sector) pointed out that private banks take the security issues more seriously than the public banks.

Table 7 – Maturity levels of the critical infrastructure operators.

Critical infrastructure operator	Answer of the interviewees
Electricity distribution company	2
Electricity production company	5
Telecommunications company	4
GSM company	5
Bank-1	4
Bank-2	5
Transportation operator	2
Water purification facility within a municipality	2
Governmental institution (provides a critical e-government service)	3
The average of public critical infrastructure operators	2.83
The average of private critical infrastructure operators	5

Table 8 shows the mapping of the security principles and sectors by taking the enacted regulations into account. Checkmarks in the cells mean the partial or full existence of a related regulation in the corresponding sector. In terms of extracted principles, government services, transportation, and water management sectors do not have any cyber security related regulations in effect. Energy, telecommunications, and finance sectors have regulations that enforce the adoption of ISO 27001 or a customized national standard. Risk management process is obliged for those three sectors by the aforementioned standards. The telecommunications and finance sectors have regulations that describe the processes of internal and external security audits in detail. Management responsibility is also specified by the regulations of those two sectors. The telecommunications sector has regulations that specify the details of required security countermeasures and properties of the information systems that should be set up by the operators. None of the sectors have regulations or rules that specify the aspects like information sharing and cooperation.

As the prominent result of the focus group interview, interviewees generally support the regulations. Some sample expressions of the interviewees are as follows:

1) "Information security is not a foremost criterion for our customers. Security is one of the low priority criteria for our customers in selecting the bank. Therefore, market itself cannot promote security" (Bank-2)
2) "Regulations discipline us. For example, periodical external audit processes enforced by the regulations keep us up-to-date in terms of security" (Telecommunications company)
3) "We have to customize several information security standards according to our needs. Then, these standards have to be obliged by directives and guidelines to the critical organizations." (Governmental institution)
4) "Information security is not an agenda item of the general manager of the organization. First thing to do is to set due care principles by regulations for the managers" (Transportation operator)
5) "The usability and security has to be stabilized together. One cannot be sacrificed for the other. That could be done best by a governmental regulatory agency" (GSM company)
6) "Relevant governmental bodies such as Ministry of Transport, Maritime Affairs and Communications or Cyber Security Council do not take the lead in cyber security issues; they should specify and enact what we should do in cyber security. We need that guidance" (Water management)

The opinions of the interviewees are summarized in Table 9. Regulations are considered as an important gadget for the improvement in security. In case of the lack of regulations, interviewees said that they felt they lacked the necessary guid-

Please cite this article in press as: Bilge Karabacak, Sevgi O. Yildirim, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005

Table 8 – Current situation of the critical infrastructure operators in terms of principles.

Principles (output of the second phase of the research)	Energy	Telecommunications	Finance	Transportation	Water management	Government services
1. National or sectorial regulations that enforce the internal/external audit for critical infrastructure operators		✓	✓			
2. Obligation of a comprehensive security standard, such as ISO 27001, for critical infrastructure owners	✓	✓	✓			
3. Minimum security countermeasures that are obliged by regulations for critical infrastructure owners		✓				
4. Regulations that set out the properties of information systems and security countermeasures that come into operation in critical infrastructure operators		✓				
5. Regulations that specify the inner-inter sector information sharing and cooperation principles						
6. Regulations that hold top level management of critical infrastructure operators responsible for cyber security		✓	✓			
7. Regulations that enforce critical infrastructure owners to conduct the cyber security risk management process	✓	✓	✓			

ance. However, two regulatory approaches are clustered after the focus group interview. The first group contains the critical infrastructure operators with a maturity level of less than 3 according to the Table 7. The second group includes the operators with the maturity levels 4 or 5. The first group supports government or regulatory agency provision. None of the interviewees in the first group was from the private sector. In Turkey, government services, transportation, and water management sectors do not have regulatory agencies. They think that government (relevant ministry and cyber security council) should take the lead in the determination of the required regulations. The regulations should be detailed so that they should know what to do. The first group also points out the importance of the regulations for the due care of the managers. They strongly point out that regulations make the managers allocate sufficient budget and manpower to the required cyber security tasks. The second group contains three private and two public operators. The second group also supports the regulations. However, their main focus is the cooperation of the operators in market and the government in the specification of the set of regulations. Although private operators especially would like to be more active in specifying regulations, the current situation in Turkey for these operators is still close to government provision. That means there is no or very limited cooperation between the operators and the government in determining or updating the regulations. That current situation is not what a second group would like to see.

Table 10 shows the ideas of the interviewees on the necessity of each regulation that was identified in the second phase of the research. All interviewees support the regulations that arrange the rules on the audit process, security standards, the properties of information system, risk management, and the top management responsibilities. Only four of the interviewees support the regulations that specify information sharing and cooperation rules. Interviewees who support the regulations for information sharing and cooperation claim that regulations are the enablers of the information sharing and cooperation activities. Interviewees who oppose the regulations stress that the incentives like cooperation, innovation, information sharing, and security culture cannot be acquired through regulations. They underline that all parties in cooperation should be voluntary and they should satisfy the requirements of cooperation and information sharing.

The policy-level issues of critical infrastructure protection as an academic topic is mostly studied in developed countries like the United States, European Union and Oceanian countries. In terms of developing policies and strategies, the governments of the developed countries are ahead of the governments of the less developed ones. Secondly, critical infrastructures are mostly owned and operated by private entities in developed countries. For example, the percentage of private sector ownership of infrastructures in the US is eighty-five percent (de Bruijne and van Eeten, 2007).

Developing countries like Turkey are mostly under way to privatize the infrastructures. For example, the largest and national telecommunications company of Turkey was privatized in 2005 (Turk Telekom, 2015). Share transfer agreements between the government and private organizations that are responsible for electricity distribution were completed as of August 2013 (TEDAS, 2015). Despite the ongoing privatizations,

Please cite this article in press as: Bilge Karabacak, Sevgi O. Yildirim, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005

Table 9 – Summary of the thoughts of the interviewees.

Critical infrastructure operator	Type	Regulation is necessary?	Regulatory approach
Electricity distribution company	Public	Yes	Regulatory agency provision
Electricity production company	Private	Yes	Regulatory agency and market should specify the required regulations together.
Telecommunications company	Public	Yes	
GSM company	Private	Yes	
Bank-1	Public	Yes	
Bank-2	Private	Yes	
Transportation operator	Public	Yes	Government provision
Water purification facility within a municipality	Public	Yes	Government provision
Governmental institution (provides a critical e-government service)	Public	Yes	Government provision

there is still a considerable dominance of the government ownership of the critical infrastructures in Turkey.

The regulation of critical infrastructures has been discussed for at least one decade. However, it is still a hot topic for the academia and the governments. The strict government intervention and regulations in CIP efforts are not considered as a suitable option by the academia and governments in the developed countries. In these countries, there are a number of academic studies that propose security management models for CIP. These articles focus on the importance of the cooperation, innovation, and non-regulation rather than emphasize the importance of the regulations. The idea of non-regulation is accepted more widely in the developed countries.

Although the developed world discusses the topics like innovation, non-regulation, business continuity, voluntary approaches, and network governance, developing countries like Turkey should be prudent while considering these options. As opposed to the developed world, the approaches close to the deregulation of the infrastructures may not be a sound option to establish effective CIP policies for the developing countries like Turkey. The opinions of the employees at the third phase of the research corroborate the situation.

The main problem of Turkey can be regarded as the normlessness or deregulation of the certain sectors like transportation, water management, and government services. As most of the employees in the focus group interview emphasized, written regulations can be considered as imperatives to ensure an acceptable level of cyber security practices within the critical sectors.

6. Assumptions, limitations and delimitations

The limitations and assumptions of a typical qualitative research also apply for this research. It is assumed that interviewees and experts have responded accurately during the interviews, the verification of the extracted theory, and Delphi survey. Extracted from the data by using grounded theory method, the root causes are bound by the opinions of the interviewees, the gathered documents, and the theoretical sensitivity of the authors. The set of principles are depended on the opinions of the experts who have participated in Delphi survey. There were nine interviewees from six different sectors in the first phase of the research. Six experts were utilized in the Delphi survey. Nine participants were incorporated in the focus group interview. Authors succeeded the participation of the experienced employees and experts from divert sectors, so that subjectivity of the qualitative research is lessened.

For this study, the critical infrastructure sectors, determined in the second meeting of the Cyber Security Council of Turkey, are selected as the critical sectors. The analyses are performed by using the gathered data from these sectors, which are energy, telecommunications, finance, transportation, water management, and government services.

As the disciplines of cyber crime fighting, military cyber operations and privacy protection are not directly associated with the cyber security of critical infrastructures (Klimburg, 2012), they are left out of the scope of the research. The vulnerabilities associated with the physical security of the critical infrastructures are left out of the scope of the research.

The interviewees might have avoided giving correct and complete information as not to be responsible for disclosing problems and vulnerabilities. At the beginning of each interview, it was assured that the interviewee and his/her organization would remain anonymous and any vulnerability that may be associated with the organization would not be mentioned within the research. Conducting interviews with nine different organizations from six sectors can be a mitigating factor for this threat.

7. Future research implications

Private sector domination is an important factor for the debates of "regulation versus innovation" in developed countries. Currently, there are no, or very limited, disputes in Turkey on the intervention of the government in the critical infrastructure protection, contrary to the developed countries. Although there are critical sectors that are dominated by private organizations, all of the participants of the focus group interview, including the private-sector ones, supported the regulations. Three factors may result in, or contribute to, this phenomenon. Firstly, there is still a considerable weight of governmental critical infrastructure owners in Turkey. If the proportion of the private sector ownership increases as a result of the privatization and globalization processes in the forthcoming years, some disputes on government intervention may emerge. Sec-

Please cite this article in press as: Bilge Karabacak, Sevgi O. Yildirim, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005

Table 10 – Opinions of the interviewees on the necessity of the principles.

The regulatory tasks	Energy-public	Energy-private	Telecommunications-public	Telecommunications-private	Finance-public	Finance-private	Transportation	Water management	Government services
1. National or sectorial regulations that enforce the internal/external audit for critical infrastructure operators	✓	✓	✓	✓	✓	✓	✓	✓	✓
2. Obligation of a comprehensive security standard, such as ISO 27001, for critical infrastructure owners	✓	✓	✓	✓	✓	✓	✓	✓	✓
3. Minimum security countermeasures that are obliged by regulations for critical infrastructure owners	✓	✓	✓	✓	✓	✓	✓	✓	✓
4. Regulations that set out the properties of information systems and security countermeasures that come into operation in critical infrastructure operators	✓	✓	✓	✓	✓	✓	✓	✓	✓
5. Regulations that specify the inner–inter sector information sharing and cooperation principles	✓	X	X	X	X	X	✓	✓	✓
6. Regulations that render top level management of critical infrastructure operators responsible for cyber security	✓	✓	✓	✓	✓	✓	✓	✓	✓
7. Regulations that enforce critical infrastructure owners to conduct the cyber security risk management process	✓	✓	✓	✓	✓	✓	✓	✓	✓

✓: should have, X: should not have.

Please cite this article in press as: Bilge Karabacak, Sevgi Ö. Yıldırım, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005

ondly, Turkey has a civil legal system unlike the US and the Commonwealth Countries that have common legal system. In civil legal systems; the rules have to be in written forms, which are structured in a hierarchy of norms. Therefore, because of its legal system, a well-defined and complete set of regulations may be necessary for Turkey. Thirdly, the innovation capacity of Turkey is quite low compared to the developed countries (OECD, 2013). Therefore, the private sector may not focus on the innovations at least at the first place.

Our study confirmed that there is no one solution that fits all the situations in terms of cyber security regulations of critical infrastructures. A new research will be conducted to find the possible reasons of supporting the regulations for the security of the critical infrastructures. The authors of the article consider that the factors such as critical infrastructure ownership by governmental organizations, judicial system and innovation capacity of a country may be prominent factors. However a new research is required to ensure the effects of those three and any other factors. The results of the future research may help the countries that resemble Turkey in terms of development level, legal system and critical infrastructure ownerships.

If a similar research is performed in other developing countries, a cross-country comparison can be made and the lessons learned may be more beneficial to other countries when creating awareness for securing critical infrastructures.

Acknowledgements

The data of the project named "Information Security Management of Critical Infrastructures" are used at this research. The project is funded by the Ministry of Development of Turkey with the grant name "BİLGEM-BT Kritik Altyapılarda Bilgi Güv. Yönetimi" and the grant number 2012K120110.

BIBLIOGRAPHY

Ahem DM, Clouse A, Turner R. *CMMI distilled: a practical introduction to integrated process improvement*. 3rd ed. Boston: Addison-Wesley Professional; 2008.

Andress A. *Surviving security: how to integrate people, process, and technology*. 2nd ed. Boca Raton: Auerbach Publications; 2003.

Assaf D. Models of critical information infrastructure protection. *Int J Critical Infrastructure Protection* 2008;1(December):6–14.

Brechbühl H, Bruce R, Dynes S, Johnson ME. Protecting critical information infrastructure: developing cybersecurity policy. *Inf Technol Dev* 2010;16(1):83–91. doi:10.1002/itdj.20075\n. <http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=25891529&site=ehost-live>.

BRSA. The statute on the principles of the information security management of the banks, Turkey, http://www.resmigazete.gov.tr/eskiler/2007/09/20070914-1.htm; 2007.

BRSA. The statute on the audit of information systems and business processes of banks by independent auditors, Turkey, <http://www.resmigazete.gov.tr/eskiler/2010/01/20100113-4.htm>; 2010.

Chan APC, et al. Application of Delphi method in selection of procurement systems for construction projects application of Delphi method in selection of procurement systems for construction projects. *Constr Manage Econ* 2001;19(7):699–718.

Clarke RA, Knake RK. Cyber war: the next threat to national security and what to do about it. *Terrorism and Political Violence* 2010;23(1):304.

Condron SM. Getting it right: protecting American critical infrastructure in cyberspace. *Harv J Law Technol* 2007;20:403–22.

Cook DM. 2010. Mitigating cyber-threats through public–private partnerships: low cost governance with high-impact returns. In Proceedings of the 1st International Cyber Resilience Conference. Perth, Western Australia, pp. 22–30.

de Bruijne M, van Eeten M. Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. *J Contingencies Crisis Management* 2007;15(1):18–29.

Deibert R, Rohozinski R. Liberation vs. control: the future of cyberspace. *J Democr* 2010;21(4):43–57.

Denscombe M. *The good research guide for small-scale social research projects*. 4th ed. Berkshire, UK: Open University Press; 2010.

DHS. NIPP 2013, partnering for critical infrastructure security and resilience, http://www.dhs.gov/sites/default/files/publications/NIPP2013_PartneringforCriticalInfrastructureSecurityandResilience_508_0.pdf; 2013.

EMRA. The license statute of electricity market, Turkey, http://www.epdk.org.tr/documents/elektrik/mevzuat/yonetmelik/elektrik/lisans/Elk_Ynt_Lisans_Son_Hali1.doc; 2014a.

EMRA. The license statute of natural gas market, Turkey, http://www.epdk.org.tr/documents/dogalgaz/mevzuat/yonetmelik/dogalgaz/lisans/Dpd_Ynt_lisans_Son_Hali_19032015.doc; 2014b.

EMRA. The license statute of petroleum market, Turkey, http://www.epdk.org.tr/documents/petrol/mevzuat/yonetmelik/petrol/lisans/PPD_YNT_Lisans_Son_190220151.docx; 2014c.

European Commission. Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf; 2013a.

European Commission. Proposed Directive on Network and Information Security – frequently asked questions, http://europa.eu/rapid/press-release_MEMO-13-71_en.htm; 2013b [accessed 09.06.15].

European Council. Convention on Cybercrime, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm; 2001.

Farwell JP, Rohozinski R. Stuxnet and the future of cyber war. *Survival: Global Politics and Strategy* 2011;53(1):23–40.

Friedman AA. 2013. *Cybersecurity and Trade: National Policies, Global and Local Consequences*.

Hansen L, Nissenbaum H. Digital disaster, cyber security, and the copenhagen school. *Int Stud Q* 2009;53(4):1155–75.

Hiller JS, Russell RS. The challenge and imperative of private sector cybersecurity: an international comparison. *Comput Law Sec Rev* 2013;29(3):236–45.

Hsu C, Sandford B. The delphi technique: making sense of consensus. *Practical Assessment. Res Eval* 2007;12(10):1–8.

ICTA. Statute of Network and Information Security in Telecommunications Sector, Turkey, http://www.resmigazete.gov.tr/eskiler/2014/07/20140713-4.htm; 2014.

Ikitemur G. *Enhancing cyber security in turkey through effective public and private cooperation*. Dallas: The University of Texas; 2014.

Jones M, Alony I. Guiding the use of grounded theory in doctoral studies – an example from the Australian film industry. *Int J Dr Stud* 2011;6:95–114.

Kaplan B, Duchon D. Combining qualitative and quantitative methods in information systems: a case study. *MIS Q* 1988;12(4):571–86.

Kaska K, Trinberg L. *Regulating cross-border dependencies of critical information infrastructure*. Tallinn: 2015.

Kelly BB. Investing in a centralized cybersecurity infrastructure: why "hacktivism" can and should influence cybersecurity reform. *Boston Univ Law Rev* 2012;1:1663–711.

Klimburg A, editor. *National cyber security framework manual*. Tallinn: NATO CCD COE Publication; 2012.

Kramer FD. Cyberpower and national security. *American Foreign Policy Interests* 2013;35(April 2015):45–58. Available from: <http://www.tandfonline.com/doi/abs/10.1080/10803920.2013.757960>.

Luiijf EAM, Klaver MHA. 2004. Protecting a nation's critical infrastructure: the first steps. In 2004 IEEE International Conference on Systems, Man and Cybernetics. pp. 1185–90.

Marshall MN. Sampling for qualitative research. *Fam Pract* 1996;13(6):522–5.

Mitchell PT. Cyberspace and the state: toward a strategy for cyber-power by David J. Betz and Tim Stevens. *J Strategic Stud* 2013;36(5):753–5. Available from: <http://www.tandfonline.com/doi/abs/10.1080/01402390.2013.825434/nfiles/3555/Mitchell-2013-CyberspaceandtheStateTowardaStrategyforCy.pdf>.

Nissenbaum H. Where computer security meets national security. *Ethics Inf Technol* 2005;7:61–73.

OECD. *Comparative performance of national science and innovation systems*. Paris: 2013.

Okoli C, Pawlowski SD. The Delphi method as a research tool: an example, design considerations and applications. *Inf Manage* 2004;42(1):15–29.

Orlowski S. Information management: protecting critical information assets. *Comput Law Sec Rep* 2001;17(3):182–5.

Robinson N, et al., 2013. *Cyber-security threat characterisation: a rapid comparative analysis*.

Shannak RO. Grounded theory as a methodology for theory generation in information systems research. *Eur J Econ Finance Adm Sci* 2009;15(15):32–50.

Stavridis J, Farkas EN. The 21st century force multiplier: public–private collaboration. *Wash Q* 2012;35(2):7–20.

Strauss A, Corbin J. *Basics of qualitative research: techniques and procedures for developing grounded theory*. Thousand Oaks: SAGE Publications; 2008.

Svete U. European e-readiness? Cyber dimension of national security policies. *J. Comp Polit* 2012;5(1):38.

TEDAS. About TEDAS, http://www.tedas.gov.tr/Sayfalar/Hakkimizda.aspx; 2015 [accessed 05.06.15].

Thai MTT, Chong LC, Agrawal NM. Straussian grounded-theory method: an illustration. *Qual Rep* 2012;17(52):1–55.

The White House. *Executive order 13010—critical infrastructure protection*. USA: The White House; 1996.

The White House. *Executive order 13636—improving critical infrastructure cybersecurity*. USA: The White House; 2013.

Turk Telekom. About Türk Telekom, http://www.turktelekom.com.tr/tt/portal/TTHakkinda/KurumsalTanitim/Hakkinda; 2015 [accessed 05.06.15].

Turkish Cabinet. Regulation Amending the Regulation on Military Forbidden Zones and Security Zones, Turkey, http://www.resmigazete.gov.tr/eskiler/2011/10/20111018-4.htm; 2011.

Turkish Cabinet. Aile ve sosyal politikalar bakanlığının teşkilat ve görevleri hakkında kanun hükmünde kararname ile bazı kanun ve kanun hükmünde kararnamelerde değişiklik yapılmasına dair kanun, Turkey, http://www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm; 2014.

USA. USA Patriot Act, USA, http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf; 2001.

Wikipedia Contributors. Cyber-security regulation, Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Cyber-security_regulation; 2015 [accessed 19.11.15].

Wilson N. Australia's national broadband network – a cybersecure critical infrastructure? *Comput Law Sec Rev* 2014;30(6):699–709.

Young MD. United States government cybersecurity relationships. *J Law Policy* 2012.

Please cite this article in press as: Bilge Karabacak, Sevgi O. Yildirim, Nazife Baykal, Regulatory approaches for cyber security of critical infrastructures: The case of Turkey, Computer Law & Security Review: The International Journal of Technology Law and Practice (2016), doi: 10.1016/j.clsr.2016.02.005