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 Ozkan 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. Isci Bloklari Mah. 1505 Cad. 43/9, Cankaya, Ankara Turkey. Tel.: +1 512 8504300; fax: +1 561 423 6345.
E-mail address: bilgek@gmail.com (B. Karabacak).

http://dx.doi.org/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, 2012).

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; NCAFP, 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