2016

An Assessment Model to Improve National Cyber Security Governance

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

Unal Tatar
Old Dominion University

Adrian Gheorghe
Old Dominion University

Recommended Citation
Karabacak, B., Tatar, U., & Gheorghe, A. (2016). An Assessment Model to Improve National Cyber Security Governance. *11th International Conference on Cyber Warfare and Security* Retrieved from https://fuse.franklin.edu/facstaff-pub/37

An Assessment Model to Improve National Cyber Security Governance

Unal Tatar[1], Bilge Karabacak[2] and Adrian Gheorghe[1]
[1]Engineering Management and Systems Engineering Department, Old Dominion University, Norfolk, USA
[2]Graduate School of Informatics, Middle East Technical University, Ankara, Turkey
utatar@odu.edu
bilgek@gmail.com
agheorgh@odu.edu

Abstract: Today, cyber space has been embraced by individuals, organizations and nations as an indispensable instrument of daily life. Accordingly, impact of cyber threats has continuously been increasing. Critical infrastructure protection and fighting against cyber threats are crucial elements of national security agendas of governments. In this regard, governments need to assess the roles and responsibilities of public and private organizations to address the problems of current cyber protection postures and to respond with reorganization and reauthorization of these postures. A risk management approach is critical in placing these efforts in an ongoing lifecycle process. In this paper, a model is proposed to be used in national cyber security risk management processes. We argue that this model simplifies and streamlines national risk management processes. For this purpose, a matrix is created to partition the problem space. Cyber threat detection and response activities constitute one dimension of the matrix. The second dimension divides the timeline of cyber incidents into three: before, during and after incidents. The resulting matrix is then populated with responsible bodies which need to address each case. As a result, a national cyber security responsibility model is proposed for policy/decision makers and academics. We believe that the proposed model would be useful for governments in analyzing their national responsibility distribution to address gaps and conflicts in their current cyber security postures and for academics in analyzing natural cyber security systems and comparative studies.

Keywords: national security, national governance, national cyber security roles and responsibilities, cyber thresholds, risk analysis, risk management

1. Introduction

Critical infrastructures are vital assets whose destruction or impairment would cause loss of life, damage to the economy, and/or debilitation in national security (USA 2001). For proper maintenance and operation of national economy, public order and national security, critical infrastructures are required to be protected against physical or cyber threats in accordance with certain strategies, policies and procedures.

Today, cyber systems are extensively utilized in the operation of critical infrastructures. In addition to finance and telecommunications infrastructures that have long been integrated with information technologies, the ones such as smart electric networks, transportation and intercity gas distribution systems which are operated via full remote control, are also now part of our lives. It is easy to access the news about cyber-attacks against nuclear plants, electric networks, sewerage systems, flight control systems and seaports (Farwell & Rohozinski 2011; Condron 2007).

The intense employment of cyber systems in critical infrastructures obliges countries to discover effective fighting methods against cyber-attacks. In this context, developed countries have begun to consider critical infrastructure protection efforts as a subset of the high-level national security studies, and carry out their arrangements, studies and audit mechanisms accordingly (Harrop & Matteson 2013).

This article concentrates on two issues in the effective fighting of countries against cyber threats: the threshold-based risk management approach, and roles and responsibilities matrix. The propositions regarding these issues are anticipated to contribute to the programs for the protection of critical infrastructures, already seen as a subset of national security studies.

The second part of the article is the literature review, which summarizes the concept of threshold level in cyber security, the concept of risk management, and the challenges in fighting against cyber threats. The third part is dedicated to problem statement, and the fourth part covers the proposed model that includes roles and responsibilities matrix. The fifth and final sixth parts of the article are evaluation and future work, respectively.

2. Literature review

This section focuses on the major challenges in fighting against cyber threats to critical infrastructures. As a second point, the concept of risk management in the literature and its reflections onto the national security are discussed. Finally, threshold concept is summarized.

2.1 Major challenges

There are challenges which hinder the effective fighting against targeted and coordinated cyber attacks which are directed towards critical infrastructures of a country. These challenges can be specified as follows:

- Horizontal usage of cyber systems
- Technical incapacity of Computer Security Incident Response Teams (CSIRTs)
- Lack of maturity in international information sharing and cooperation mechanisms
- Dominance of private sector ownership of critical infrastructures
- Deficiencies in the holistic approach of countries towards the security of critical infrastructures and weakly-defined roles and responsibilities
- Poorly-explained relationships and dependencies between critical infrastructures
- Asymmetric nature of cyber threats and cyber attackers.
- Lack of situational awareness mechanisms.

Operating in critical sectors ranging from health to transportation, from public services to energy, public institutions and private firms have their own objectives, sizes, and operation processes and modes. Thus, it is inevitable that these institutions have different views on cyber technologies and cyber security. Different definitions and understandings of risks appear to obstruct the protection of critical infrastructures (Canada 2009). It is not a simple task to gather all such different institutions under one umbrella and to maintain the cooperation among them (Klimburg 2012).

Many countries have their own national CSIRT structures for coordination task, which is significant in detection of cyber threats against national security and counteraction against them. On the other hand, not all countries reach the sufficient capacity levels of CSIRT structures, which require allocated resources and technical capacities (OECD 2007).

Information sharing is one of the key studies to be performed within the scope of fighting against cyber threats to national security (Bahsi & Karabacak 2008). Information sharing at the national level may be carried out on a limited scale, due to the lack of a national information classification systems, variation of the classification schemes among institutions and countries, and legal restrictions within the countries. Therefore, the lack of information sharing becomes a significant obstacle in protection of critical infrastructures (OECD 2007).

In most of the developed countries, private sector occupies a considerable place in finance, energy, transportation, and telecommunications sectors. In the US, 85% of the critical infrastructures are operated by private sector (US-GAO 2006; Pounder 2002). Specifically for the developed countries, it is true that global / international / foreign companies may also operate critical infrastructures as a result of privatizations. Countries struggle to find the best strategy and regulation for critical infrastructures owned by private sector (Hiller & Russell 2013).

Considering that the first formal document regarding critical infrastructure protection was Executive Order which was signed by the US President Bill Clinton and published in 1996, this field is clearly seen to be a completely new topic for most of the countries. Cyber security management of critical infrastructures and critical infrastructures protection are composed of a series of complex studies as critical infrastructures themselves are enormous and complicated; and those disciplines are novel for the countries.

Roles and responsibilities for the field are not yet fully-defined. That is why, in the course of the time, countries may alter their governance models for critical infrastructure protection. For instance, in 2013, the US assigned US Cyber Command the task of support for critical infrastructures protection, which was formerly only under responsibility of Department of Homeland Security (DHS).

Other elements that inhibit fight against cyber threats are inter and intra-sectoral interdependencies and relationships among critical infrastructures. There have been several academic studies that concentrate on relationships among critical infrastructures (Balducelli et al. 2008; Little 2002; Luiijf et al. 2009; Rinaldi et al. 2001). Although those studies have been conducted to clarify the systemic interdependencies, some of interdependencies may still remain unnoticed until when a cyber / physical incident occurs and infrastructures become debilitated.

Cyber threats are asymmetric by their nature. The following are the factors that contribute to fairly broad concept of asymmetry:

- It is hard to identify the source of cyber threat, most of cyber threats remain anonymous
- Attribution of a cyber-attack is hard because of the difficulty of detecting a cyber-threat and tracing it back
- Cyber threats are affordable and have low costs
- Cyber tools are prevalent and easy to use
- Cyber-attacks can easily be outsourced

Another obstruction in critical infrastructure protection is that information derived from many different sources cannot be coherently combined to reveal a meaning by using a situational awareness mechanism (Canada 2009). Current situational awareness mechanisms lack adequate amount of information, infrastructure and equipment.

2.2 Cyber security risk management for national security

When critical infrastructure protection literature and studies of developed countries are reviewed, it is observed that they locate risk management approach at the center of fighting against threats. Risk analysis is one of the primary studies conducted within the process of risk management.

Risk is dependent on three variables: asset, vulnerability and threat (NIST 2012; Farn et al. 2004; Moteff & Ave 2005; ISO/IEC 2008). Amount of risk is directly proportional to value of assets, criticality of vulnerabilities, and motivation of threats. In a risk analysis study of a critical infrastructure, critical infrastructure operator should undertake the criticality of possible vulnerabilities of the critical infrastructure. National intelligence units and governmental units that have responsibilities in critical infrastructure protection program should provide inputs associated with the motivation of threats against that critical infrastructure (US-GAO 2013). In a simple quantitative risk analysis process, the impact and likelihood values of a threat are multiplied (NIST 2012). Values of assets and criticalities of vulnerabilities are also taken into account during the prediction stage of these two parameters of threat. If predicted risk value is identified to be high following the assessment of the variables, necessary countermeasures are taken and thus, the risk management process is initiated.

Prepared by National Institute of Standards and Technology (NIST), Guide for Conducting Risk Assessments, an advisory document, appears to be one of the leading sources in the field of risk management. In this advisory document, it is stated that effective risk management should be fully integrated into the system development life cycle process and that risk management is an iterative process which has to be performed in any main phase of system development life cycle process.

Life cycle model, practiced in risk management process, can also be applied to the other fields of cyber security. To give an example, European Network and Information Security Agency prepared a guidebook for the formation of a national cyber security strategy, based on the “plan-do-check-act” model (ENISA 2012).

As required by the Executive Order 13636 named “Improving Critical Infrastructure Cybersecurity”, published by White House in February 12, 2013, a cyber security framework was developed in coordination with NIST (NIST 2014). The framework states that it uses all risk management processes, has an iterative structure, is open to constant improvement and enhancement, and conforms to the lifecycle in the institution.

The approach towards the risk management process as an ever-improving lifecycle is directly compatible with the nature of cyber systems and cyber threats. Along the rapid developments in technology, cyber systems have become extensively used. A number of applications are released into the market every day. This fact enforces the presence of an iterative and ever-improving risk management process.

In the last years, academic circles have done studies in the fields of sectoral risk analysis and risk management processes, both of which include critical infrastructure sectors (Adler & Fuller 2007; Flammini et al. 2008; Adar & Wuchner 2005; Luiijf et al. 2011). Sectoral risk studies try to measure the risk of a critical sector by performing a holistic risk analysis.

Cyber security risk management at national level is a fairly new subject, brought up into the agenda by security experts. No academic study on this subject was encountered during the preparation of the article. The governmental studies conducted on the subject belongs only to the US government. One of those studies is The Strategic National Risk Assessment (SNRA), carried out by DHS Office of Risk Management and Analysis, under the reinforcement of Presidential Policy Directive 8 (PPD-8). And again, within the scope of National Infrastructure Protection Plan (NIPP), applied by DHS, there have been studies conducted within the context of National Risk Management (DHS 2013).

2.3 Cyber security incidents as a national security issue

Before the activation of a national response mechanisms against a cyber threat, the impact (or possible impact) of cyber threat must be resolved through a threshold value, which should be determined by the government.

The objective of the article is not the specification of such a threshold level. It rather touches upon the studies in the literature that might provide an insight into the threshold mechanism, as one of the first stages of a response against national-level cyber security incidents. A threshold definition by government is crucial to determine whether the actual incident (or a possible one) has a national security dimension. The US has conducted a series of studies on the determination of a national impact threshold. As for the damages to critical infrastructures, “consequence-based criteria” and “relative threshold levels” were formulated in the document prepared by US Government Accountability Office and sent to the US Congress (US-GAO 2013). According to the document, the study for the determination of a threshold level was not carried out only for cyber threats, but it was designed to address all types of threat. Accoırding to the document, consequence-based criteria are prompt fatalities, economic consequences, mass evacuation length, and national security. Two thresholds, Level 1 and Level 2, were defined for the first three of the criteria. However, due to the confidentiality constraints, no more details were publicized. And there has been no defined threshold for the criterion of national security.

Twenty-three threats to the homeland security of the US nation and National-level Event Descriptions for those threats were defined as part of the SNRA (US 2011). Two of the threats in SNRA are cyber-based: Cyber Attack against Data and Cyber Attack against Physical Infrastructure. While “National-level Event Description” for cyber-attack against data is defined as “economic losses of a billion dollars and greater”, that for cyber-attack against physical infrastructure is one casualty (or more) or 100 million (or more) dollars of economic loss. SNRA study dwelled more on the facts that cyber threats might have possible serious specific outcomes, that cyber threats might result in failures in power grid and financial systems, which increases the potential impact of a cyber incident.

Threshold value should be identified not by individual critical infrastructure operators, but by a higher authority. Thus, in “Efforts to Identify Critical Infrastructure Assets and Systems” by DHS, it is stated that the criticality criteria have been defined by state authorities and critical sector operators, however threshold values have been defined by DHS Office of Infrastructure Protection (DHS-OIG 2009).

3. Problem statement

In this article, authors answer the following question: Despite the challenges of dealing with cyber threats, how can a national cyber security governance be set up and assessed in a relatively straightforward manner? Several countries address to the topic of national governance when they prepare their national cyber security strategies, action plans or policies. The Action Item 29 in “National Cyber Security Strategy and 2012-2013 Action Plan” of Turkey constitutes the main source of motivation for the development of the model presented in this article (Ministry of Telecommunications 2013). In the action item in question, the following phrase is used under the title of “Integrating national cyber security concepts into the national security context”: “Determining the responsibilities of public organizations in case of cyber security incidents in the cyber space and how to ensure coordination at national level.”

For the Action Item 29, the brainstorming activity, including the national stakeholders, has demonstrated that the most crucial point in the formation of national governance is the identification of roles and responsibilities at the national level. And during the national governance studies, the following two points were regarded worthy of consideration: a) Setting up threshold levels for the possible impact level of a cyber incident, and b) Integrating risk management approach.

An applied field study in the area of national governance is estimated to find answers to following three questions:

- Whether the responsible bodies for critical infrastructure protection and their responsibilities defined?
- Whether there are any conflicting roles and responsibilities?
- Whether there are any gaps in defined roles and responsibilities?

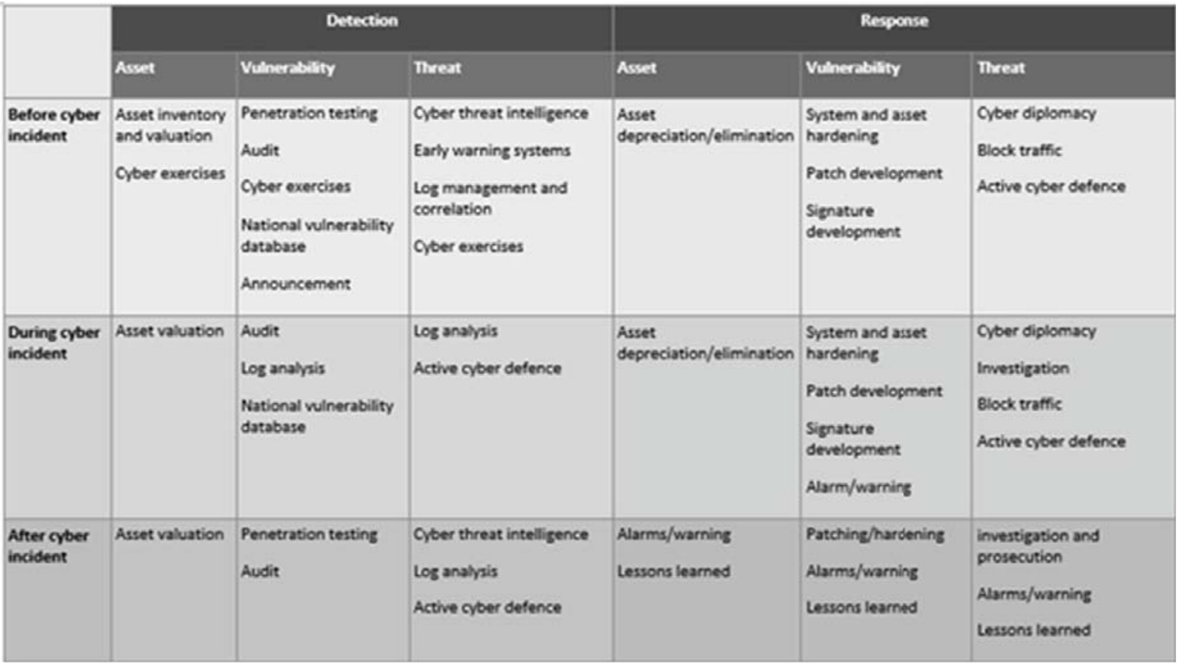
4. Proposed model

Based on systemic thinking, the model proposed in the article intends to streamline the processes of national-scale planning and policy-making of cyber security. Proposed model does not allege to find new action points.

The intense usage of cyber systems in critical infrastructures points out to the fact that cyber threats should be evaluated within the framework of national security. The rapid and efficient response to cyber threats possesses a vital importance in that it helps to minimize harmful consequences. Literature review section underlines the difficulties of fighting against cyber threats. When these difficulties are taken into consideration, it becomes clear that roles and responsibilities at national level should be defined and the tasks should be properly assigned as almost all the obstacles, not necessarily the technical ones, can be overcome through participation, cooperation, information sharing and coordination.

The scope of national security should be examined in subsets, for the cyber security roles and responsibilities to be defined at the national level. By this method, as a version of “divide and conquer” approach, it becomes possible to both deal with each and every issue and to be able to see the big picture in details. For this purpose, a matrix with three dimensions were used as shown in Table-1. The first dimension of the matrix is timeline, and it includes three stages: before, during and after cyber incident. The second dimension is fundamental action type and two fundamental actions mentioned in the dimension are detection and response. And the third dimension of the matrix is the parameters of asset, vulnerability and threat. These three parameters are taken into account in information security risk management process and are mentioned in many resources as three basic inputs of information security risk analysis.

Table 1: Roles and responsibilities matrix



	Detection			Response		
	Asset	Vulnerability	Threat	Asset	Vulnerability	Threat
Before cyber incident	Asset inventory and valuation Cyber exercises	Penetration testing Audit Cyber exercises National vulnerability database Announcement	Cyber threat intelligence Early warning systems Log management and correlation Cyber exercises	Asset depreciation/elimination	System and asset hardening Patch development Signature development	Cyber diplomacy Block traffic Active cyber defence
During cyber incident	Asset valuation	Audit Log analysis National vulnerability database	Log analysis Active cyber defence	Asset depreciation/elimination	System and asset hardening Patch development Signature development Alarm/warning	Cyber diplomacy Investigation Block traffic Active cyber defence
After cyber incident	Asset valuation	Penetration testing Audit	Cyber threat intelligence Log analysis Active cyber defence	Alarms/warning Lessons learned	Patching/hardening Alarms/warning Lessons learned	investigation and prosecution Alarms/warning Lessons learned

The cells of the Table-1 should be completed with the actions that are to be taken in the face of a possible cyber security incident. The actions are determined within the given periods (before, during and after the cyber incident), and in accordance with the fundamental action types (detection or response) and in relation to the risk parameters (asset, vulnerability, threat) and placed in the corresponding cells. Experience regarding previous incidents, expert opinion, or the information gathered from the literature could be utilized during the formation of the action list to be placed into the cells. The cells in Table-1 are partially filled as to offer a general idea about the topic.

The completion of the cells with the actions marks the end of the first stage. As seen in the Table 1, the result is 18 national-level cyber security roles and responsibilities. While some of those have to be performed by every individual critical infrastructure operator, some others need to be examined only by the higher level governmental units for cyber security coordination or intelligence units. For instance, vulnerability detection examination is a security activity that has to be conducted by every operator before any cyber attack, which indicates a preparatory process against any possible cyber attack. But response against a threat during a cyber attack is a critical operation to be conducted only by certain units of a government. Moreover, the operation may also possess offensive aspects.

In the second stage, responsible institutions are listed for the actions in the matrix. Assessments start in this stage. Those assessments are made to clarify the points below:

- whether there is an agency for each action,
- whether it is necessary to eliminate any of them, for efficiency concerns, if there is more than one agency, and
- whether the chosen agency is the best for the purpose.

At the end of the assessments, the resolutions regarding reorganization and reauthorization can effectively be taken.

Cooperation, coordination and communication are vital countermeasures in cyber security (Karabacak & Tatar 2012). The proposed matrix directs us to the necessity of coordination, cooperation and information sharing among many agencies when there is a cyber incident that targets national security. So, roles and responsibilities prove significant for a successful coordination on the macro (national) level. This matrix aims to clarify the roles and responsibilities as the result of a systematic study. And considering the parameters of timeline, fundamental action type and risk management, it should also be kept in mind that there has to be enough communication among the 18 different areas of roles and responsibilities for an effective national cyber security governance. After the determination of the related agencies, during the authorization process, necessary mechanisms should also be set up to sustain the information sharing and coordination among them.

Before processing of the matrix within the context of a cyber incident response, possible impacts of encountered or reported cyber security incident should be assessed by a higher authority. Not all cyber attacks require a coordinated national level response mechanism. This is where we attain the concept of national cyber security threshold. The matrix is to be put into operation when a cyber threat is predicted to have stronger impacts than the predetermined threshold value.

Proposed matrix should be used in a circular manner. The stages that should be periodically and circularly conducted are as follows: the control of the threshold value, the determination of an action for each particular case (each cell in the matrix), the documentation of the related agencies according to the actions, and decision-making process regarding reorganization and reauthorization on grounds of the comparison of the actual situation with an optimal one.

Proposed matrix can be regarded as a national governance matrix, which is necessary for the coordination among many stakeholders from public and private sectors to fight against cyber threats and to deal with cyber threat intelligences. The matrix can also be a guide for fighting against a cyber incident at the national level and can contribute to the definition and determination of the responsibilities of the agencies have roles in critical infrastructure protection program. In addition, it may also constitute a useful means to identify the overlaps, conflicts and gaps in the national level roles and responsibilities.

One should pay attention to the following points during the formation of a matrix.

- Each sector and each critical infrastructure operator should fill in suitable cells in the matrix by considering the assets, vulnerabilities and threats. For comparative and sound outcomes, it is necessary for the sectors to work collaboratively, which could be obtained through inter-sectoral cooperation and partnership structures.
- In the assessment of assets and vulnerabilities, a national framework, which is compliant with the international standards may be needed to serve as guidelines for the agencies.
- A higher governmental authority may have to conduct studies within the context of threat analysis and inform critical infrastructure operators about threats.
- This is a matrix which is prepared for fighting against a national-level incident, covering all the stakeholders that own a role in the critical infrastructure protection program. As the matrix is not a “one-time” and a “finalized” study, it is open to constant developments and updates.
- During the formation of the matrix, assets, vulnerabilities, and threat assessments for each phase and action type must be made by taking the perspective of risk management into consideration. Authors have partially filled in the matrix in accordance with their experience and best practices. However, results might differ for each government.

5. Summary and conclusion

Through the roles and responsibilities matrix, the article offers a solution for effective defense against cyber threats that target national security. With its divide-and-conquer approach, the matrix provides a more feasible infrastructure by dividing the roles and responsibilities in the area of cyber security into 18 parts, and it comes up with a solution based on roles and responsibilities to compensate the lack of holistic perception of cyber security of critical infrastructures. The assignment of roles and responsibilities within the matrix will also provide the private sector with concrete roles and responsibilities. The matrix is predicted to corporally reveal the needs of communication and cooperation among the agencies.

The matrix is also considered to prove beneficial in the exhibition of the relationships and interdependencies among the critical infrastructures. For example, while conducting a pre-incident asset-based study, a critical infrastructure operator might reach the results of other critical infrastructures having relationships and interdependencies with his own. Prevalently-used cyber systems inevitably leave a gap for the asymmetric cyber threats, and the asymmetric threats can only be defeated by a high-level holistic approach of roles and responsibilities. The matrix can also be regarded as the starting point for the bodies like CSIRTs to conduct comprehensive studies such as establishing situational awareness mechanisms.

6. Future work

The matrix, proposed in this article, is a facilitating means for the identification of roles and responsibilities in cyber security governance studies at national level. The action for each cell must be determined for the effective application of the matrix. Although the action provided in the article might give an overall insight into the topic, the table should precisely be filled in by interviewing with national authorities and experts and analyzing previous cyber security incidents. As a future study, the matrix is intended to be applied in Turkey, a developing nation, as to show the way for the other countries and the decision-makers, and share the outcomes. This prospective study is thought to guide the countries with the similar cases in the formation of cyber security policies.

References

Adar, E. & Wuchner, A., 2005. Risk Management for Critical Infrastructure Protection (CIP) Challenges, Best Practices &amp; Tools. *First IEEE International Workshop on Critical Infrastructure Protection (IWCIP’05)*, pp.90–100.

Adler, R.M. & Fuller, J., 2007. An Integrated Framework for Assessing and Mitigating Risks to Maritime Critical Infrastructure. In *2007 IEEE Conference on Technologies for Homeland Security*. Woburn: IEEE, pp. 252–257.

Bahsi, H. & Karabacak, B., 2008. Ulusal Bilgi Sistemleri Güvenlik Programı, In *2008 Ağ ve Bilgi Güvenliği Sempozyumu*.: TMMOB, pp. 144-148.

Balducelli, C. et al., 2008. A Middleware Improved Technology (MIT) to Mitigate Interdependencies between Critical Infrastructures. In R. de Lemos, ed. *Architecting Dependable Systems V*. pp. 28–51.

Canada, 2009. *Action Plan for Critical Infrastructure*, Condron, S.M., 2007. Getting It Right: Protecting American Critical Infrastructure In Cyberspace. *Harvard Journal of Law & Technology*, 20, pp.403–422.

DHS, 2013. *NIPP 2013, Partnering for Critical Infrastructure Security and Resilience*, Available at: http://www.dhs.gov/sites/default/files/publications/NIPP 2013_Partnering for Critical Infrastructure Security and Resilience_508_0.pdf.

DHS-OIG, 2009. *Efforts to Identify Critical Infrastructure Assets and Systems*, Washington.

ENISA, 2012. *National Cyber Security Strategies Practical Guide on Development and Execution*, Heraklion.

Farn, K.-J., Lin, S.-K. & Fung, A.R.-W., 2004. A study on information security management system evaluation—assets, threat and vulnerability. *Computer Standards & Interfaces*, 26(6), pp.501–513.

Farwell, J.P. & Rohozinski, R., 2011. Stuxnet and the Future of Cyber War. *Survival: Global Politics and Strategy*, 53(1), pp.23–40.

Flammini, F., Gaglione, A. & Mazzocca, N., 2008. Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures. In *3rd International Workshop on Critical Information Infrastructure Protection*. Rome, pp. 180–189.

Harrop, W. & Matteson, A., 2013. Cyber resilience : A review of critical national infrastructure and cyber security protection measures applied in the UK and USA. *Journal of Business Continuity & Emergency Planning*, 7(1), pp.149–162.

Hiller, J.S. & Russell, R.S., 2013. The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law and Security Review*, 29(3), pp.236–245.

ISO/IEC, 2008. *ISO/IEC 27005 Information technology — Security techniques — Information security risk management*, Geneva.

Karabacak, B. & Tatar, U., 2012. Strategies to Counter Cyberattacks: Cyber threats and Critical Infrastructure Protection. In M. Edwards, ed. *Critical Infrastructure Protection*. Ankara: IOS Press, pp. 63–74.

Klimburg, A. ed., 2012. *National Cyber Security Framework Manual*, Tallinn: NATO CCD COE Publication.

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

Luiijf, E. et al., 2009. Empirical Findings on Critical Infrastructure Dependencies in Europe. In R. Setola & S. Geretshuber, eds. *CRITIS 2008*. Springer-Verlag, pp. 302–310.

Luiijf, E., Ali, M. & Zielstra, A., 2011. Assessing and improving SCADA security in the Dutch drinking water sector. *International Journal of Critical Infrastructure Protection*, 4(3-4), pp.124–134.

Ministry of Telecommunications, 2013. *National Cyber Security Strategy and 2013-2014 Action Plan*, Available at: https://ccdcoe.org/sites/default/files/strategy/TUR_CyberSecurityEng.pdf.

Moteff, J. & Ave, I., 2005. CRS Report for Congress Received through the CRS Web Risk Management and Critical Infrastructure Protection : Assessing , Integrating , and Managing Threats , Vulnerabilities and Consequences.

NIST, 2014. *Framework for Improving Critical Infrastructure Cybersecurity*, Gaithersburg.

NIST, 2012. *NIST Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments*, Gaithersburg.

OECD, 2007. *Development of Policies for Protection of Critical Information Infrastructures*, Paris.

Pounder, C., 2002. The US's National Strategy for Homeland Security. *Computers & Security*, 21(6), pp.503–505.

Rinaldi, B.S.M., Peerenboom, J.P. & Kelly, T.K., 2001. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, (December), pp.11–25.

US, 2011. *The Strategic National Risk Assessment in Support of PPD 8 : A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation*, Washington.

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

US-GAO, 2006. *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, Washington.

US-GAO, 2013. *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, Washington.