ENHANCING CYBER SECURITY IN TURKEY THROUGH EFFECTIVE PUBLIC AND PRIVATE COOPERATION

by

Gokhan Ikitemur

APPROVED BY SUPERVISORY COMMITTEE:

_____
Dr. L. Douglas Kiel, Chair

_____
Dr. Doug Goodman

_____
Dr. R. Paul Battaglio Jr.

_____
Dr. S. Hakan Can

To my wife, Merve; and my child, Emir Talha. It would be impossible to accomplish this milestone in my career without their love and endurance.

To my mother, Sabiha; and my father Sabri for their unconditional love, support and affection throughout my life.

ENHANCING CYBER SECURITY IN TURKEY THROUGH EFFECTIVE PUBLIC AND PRIVATE PARTNERSHIP

by

GOKHAN IKITEMUR, BA, MS

DISSERTATION

Presented to the Faculty of

The University of Texas at Dallas

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY IN

PUBLIC AFFAIRS

THE UNIVERSITY OF TEXAS AT DALLAS

August 2014

ACKNOWLEDGMENTS

This study is a result of contributions from many individuals who provided assistance, guidance, encouragement, and support. I would to like to express my utmost gratitude and appreciation to my committee chairperson, Dr. L. Douglas Kiel, for his unwavering support and patience over the entire course of the doctoral program. Dr. R. Paul Battaglio, Jr., Dr. Goodman and Dr. Can, without your constant assistance and wisdom, I would never have been able to write this dissertation.

Dr. Can, thank you for your suggestions, words of inspiration, and pieces of professional insight you have given me during this work.

I would like to recognize the support that executives from the Cybersecurity Association provided in encouraging its members to participate in this study. Their contributions lifted a heavy burden from my shoulders; thank you so much. I would like to acknowledge those IT experts and IT executives who participated in this study, as your participation enabled me to complete this work. I am deeply indebted to you.

Finally, thank you to officials from the Turkish Ministry of Interior, who encouraged and nominated me for an academic scholarship. It was a great opportunity and privilege for me to pursue a doctoral degree in the U.S. I hope the knowledge and experience I gained in the U.S. will help me better serve my country.

July 2014

ENHANCING CYBER SECURITY IN TURKEY THROUGH EFFECTIVE PUBLIC AND PRIVATE PARTNERSHIP

Publication No. _____

Gokhan Ikitemur, PhD
The University of Texas at Dallas, 2014

Supervising Professor: L. Douglas Kiel

Turkey is experiencing a transition wherein it is trying to adapt its security posture to a dynamic environment filled with numerous cyber threats. Examining governance aspects of cyber security in Turkey, the current study found that public-private cooperation is likely to positively affect national cyber security preparedness; that Turkish private and public organizations have similar preparedness levels; and that both private and public organizations do not accord a high value to democratic concerns. While effective government agencies are critical to enhance national preparedness they are paradoxically unsuccessful in enhancing organizational preparedness. As a result, Turkey must regard cyber security as a governance concern and decide which organizations will lead cyber security efforts: either organizations with highly capable technological infrastructure or organizations with security mandates and experiences.

TABLE OF CONTENTS

ACKNOWLEDGMENTS……..……v
ABSTRACT……...…vi
LIST OF TABLES……..ix
LIST OF ABBREVATIONS……..x
CHAPTER 1 INTRODUCTION 1
Background……..1
Purpose of the study……..…..8
Research Questions 8
Rationale of the Study 9
Key definitions 11
CHAPTER 2 LITERATURE REWIEW 15
Introduction 15
Threats to Governments 15
Threats to Organizations 38
Threats to Democracy 50
CHAPTER 3 STUDY VARIABLES 56
Public-Private Cooperation 56
National Cyber Security Preparedness 59
Differences Between Public and Private Sector Organizations 64
Organizational Cyber Security Preparedness 65
Differences between Public and Private Sector Managers 97
Democratic values 68
CHAPTER 4 METHODOLOGY 70
Research Design 70
Sample 73

Population 73
Measurement 75
Control variables 79
CHAPTER 5 DATA ANALYSIS 80
Descriptive Statistics 80
Descriptive Findings of Demographic Data 81
Descriptive Statistics of Dependent Variables 85
Procedure of Data Analysis 85
Bivariate Analysis 88
Testing of Parallel Regression Assumption 91
Ordinal Logistic regression 92
T-test result for H2 96
T-test result for H3 96
CHAPTER 6 DISCUSSION AND CONCLUSIONS 98
Introduction 98
Summary of Findings 98
Discussion of Findings 100
Policy Recommendations 125
Future Research 132
Limitations 134
Conclusion 135
APPENDIX A IRB APPROVAL FORM 137
APPENDIX B SCALES FOR STUDY VARIABLES 138
APPENDIX C SURVEY QUESTIONNAIRE 139
REFERENCES 159
VITA

LIST OF TABLES

Table 5. 1 Type of organization (N= 115)..... 81

Table 5. 2 Size of the organization (N=111) 82

Table 5. 3 Type of organizational IT structure (N=111) 82

Table 5. 4 Organizational location (N=111) 84

Table 5. 5 Job title/function (N=115) 85

Table 5. 6 Dependent variables (N=111) 86

Table 5. 7 Categories of national cybersecurity preparedness (N=115) 85

Table 5. 8 Correlation matrix 87

Table 5. 9 Brant test of parallel regression assumption (N= 103).....89

Table 5. 10 Model fitting information for national cybersecurity preparedness 91

Table 5. 11 the impact of selected vairables on national cybersecurity preparedness 92

Table 5. 12 T-test for democratic values (N=103) 92

Table 5. 13 T-test for organizational cyber security preparedness (N=109) 94

Table 5.14. T-test for democratic values.....96

Table 5.15. T-test for organizational cyber security preparedness.....97

Table 6. 1 Cyber Power Index 103

Table 6. 2 Global innovation average scores 123

LIST OF ABBREVIATIONS

AusCERT	Austrian Computer Emergency Response Team
BJS	Bureau of Justice Statistics
CIO	Chief Information Officer
CISO	Chief Informational Security Officers
CSIS	Center for Strategic and International Studies
CSA	Cyber Ssecurity Association
DHS	Department of Homeland Security
DIB/ECS	Defense Industrial Base Enhanced Cybersecurity Services
DoD	Department of Defense
DOJ	Department of Justice
DNI	Director of National Intelligence
ENISA	European Network and Information Security Agency
GAO	Government Accountability Office
ISPs	Internet Service Providers
ICT	Information and Communications Technology
IT	Information Technology
ICTA	Information and Communications Technologies Authority
NASCIO	National Association of State Chief Information Officers
NCSS	National Computer Security Survey

NCIRP	National Cyber Incident Response Plan
NEMA	National Emergency Management Association
NIA/MIT	National Intelligence Agency
NIPP	National Infrastructure Protection Plan
NIS	Network and Information Security
NPR	National Preparedness Report
NPR	National Preparedness Goal
NSPD	National Security Presidential Directive
NSS	National Security Strategy
OJP	Office of Justice Programs
PPPs	Public Pprivate Ppartnerships
PTC/TIB	Presidency of Telecommunication and Communication
SOME	Teams for Responding to Cyber Incidents
SPR	State Preparedness Report
USOM	National Center for Cyber Incident Response

CHAPTER 1

INTRODUCTION

"Cyberspace is accepted now as a domain equal to land, air, sea, and space."
Deibert and Rohozinski (2010, 16)

More than half of humanity connects politically, socially, and economically in non-physical, digital space. Being a mainstay of contemporary society, this cyber domain provides "a bright landscape for commerce, science, education, communication, and open and efficient government" (White House 2011, 1). However, not only does cyberspace create unprecedented opportunities in the aforementioned fields, but it also generates threats to security and privacy that can limit its usage and potential (Kramer et al. 2009). National governments cannot withstand ambiguities that can potentially destabilize the previous state-centric system in vast, unregulated spaces (U.S. Department of Homeland Security 2011). Determined to challenge emerging threats from the cyber domain, governments need to reorganize their existing organizational security architecture according to the nature of cyber threats; establish new mechanisms to cooperate with all domestic actors who traditionally do not assume responsibility for security-related issues; and guarantee that heightened security does not harm democratic gains.

There are several explanations regarding the nature of potential threats. The first reason primarily concerns the structure of the cyber domain. For one, it is not patterned after the state-centric system. Emergent spaces that are not fully controlled by states increasingly delude the hegemony attributed to sovereign entities. Moreover, the cyber domain is constructed in such a way that public and private networks (legal and illegal alike) can and do operate in tandem there (Deibert and Rohozinski 2010). As a result, governance of the domain should be horizontally distributed because of the dispersed nature of authority therein (Dutton and Peltu 2007).

The very nature of the cyber domain's contents can also shed light on how threats emerge. Unlike natural spaces such as air, sea, and land, cyberspace is a man-made phenomenon, built upon a worldwide, interconnected informational infrastructure. It continuously expands as a result of "constant flux based on the ingenuity and participation of users themselves" (Deibert and Rohozinski 2010, 18). This constant flux leaves the cyber domain vulnerable to intrusion from individuals and organized groups inimical to sovereign states, which is why securing and safeguarding this domain has increasingly become a concern for national security (Uroš 2012). It is not unknown for even nation-states themselves to exploit weaknesses in the cyber domain to undermine governance and enterprises in other countries. For instance, following tensions in bilateral relations, Russian-based cyber-attacks disabled government, banking, and media sites in Estonia and Georgia (Lene and Nissenbaum 2009). Because of the borderless nature of the cyber domain, then, threats can take a variety of guises, ranging from individuals to groups to even national governments. With every passing day, they place the domain's inherently fragile equilibrium and life structure at increased levels of risk.

A third explanation can be found in Internet users' growing ability to produce asymmetric results. Friedman (2002) claims that unprecedented technological developments create super-empowered cyberspace users who are able to hijack command-and-control system and whose actions can resultantly alter the decision-making capabilities of their targets (U.S. Department of Homeland Security 2011). As a result, economic and political ecosystems are left jeopardized. In a conflict environment, in which actors are able to produce asymmetric results by their actions, the "competitive advantage" shifts from states to individual actors (McCormick 2003, 123). Anonymous, a hactivism movement (Kelly 2012), for example, targeted several Turkish government sites and declared that it would continue to launch similar DDOS attacks until Turkey recognized what the group and others refer to as the Armenian genocide. Through similar actions, organized individuals can simultaneously dictate their beliefs surrounding international issues and exploit the deficiencies of cyberspace, tasks that today's technology landscape has been gradually facilitating.

The worrisome reality that the nature of threats demonstrates is how rapid technological developments have blurred the lines between public and private targets on the Internet. An adversary can cripple a country, for example, by shutting down its financial markets without ever taking aim at a government organization or a military network. No country, even a global superpower like the U.S., is immune from such threats. Furthermore, when it comes to countries' overall capacity to launch a cyber-war, the more wired a nation is, the more vulnerable it is to a cyber-attack, rather than being more prepared to withstand such an attack (Clarke and Knake 2010).

These examples raise questions over the necessary mechanisms used to secure and safeguard cyberspace and to enhance the effectiveness of democratic governance in the cyber domain (U.S. Department of Homeland Security 2010). Failure to respond to cyber threats coming from zealous and deceitful adversaries carries enormous consequences for states that are responsible for both securing their citizens' security and ensuring their vital interests. It is estimated that if necessary steps are not taken to secure online space, the risks of operating in the cyber domain might become completely unjustifiable for most citizens and enterprises, and the integrity of open governments and civil societies could be critically impaired (U.S. Department of Homeland Security 2011, 25). Although there is a need for strong state leadership, a coordinated strategy, appropriately-designed mechanisms, and highly knowledgeable government personnel, the fight against infringing parties (ranging from cyber criminals to cyber terrorists and even to nation-state adversaries) requires us to accept three inevitable components of any response in order for the government to fully protect public and private entities:

1) Cyber security is an organizational - and thus a governance - problem for states (Andreasson 2012; Jansen and Tranvik 2011). Subverting "a system of rulemaking based on borders between physical spaces," cyber threats have weakened traditional forms of political authority (Johnson and Post 1995, 1370). As a response, nation states are increasingly penetrating into the cyber domain by regulative means, seeking to turn libertarians' ungovernable area (Ziewitz and Brown 2013) into a governable one. These intensified efforts to integrate cyber security within states' broader national security and defense frameworks are increasingly becoming less of a technological concern than a governance issue. Dealing with threats and uncertainties in such a constantly-changing environment with new technological

breakthroughs (Kelly 2013) requires dynamic cyber-security capacity across the entire spectrum of a nation's government. This means orchestrated collaboration between state authorities in diverse agencies and their collective ability to adapt to dynamic technological developments (Belk and Noyes 2012) in an increasingly connected world.

Another reason to evaluate cyber security as a governance concern is that it forces government agencies to transform their security mindset and embrace a coherent strategy centered on sharing power with domestic and, in certain cases, individual actors (Betz and Stevens 2011; Kramer et al. 2009). Cornish et al. (2009) also argue that a comprehensive and anticipatory policy response in cyber space should involve all actors who benefit from the global IT infrastructure. Today, cooperation between the state and the private corporate sector is not a choice but a necessity (Quigley and Roy 2012; Dunn-Dunn-Cavelty and Suter 2009). As Harknett and Stever (2009, 2) state, "securing cyberspace can be understood best as resting on three legs of core institutional and process relationship- a cyber-security triad." The first leg is inter-governmental relations, ranging from interagency relations at the federal level to relationships between the federal and local governments. Such relations are seen as a major component of national cyber security preparedness in this present study. The second leg is defined as public-private relations, which this present study defines as cooperation among these actors. The final leg is seen as individuals' integration into security efforts. However, an evaluation of the role of empowered individuals is beyond the scope of this current study.

2) To better analyze national cyber power, there is a need for decision makers creating cyber security structures to know the extent to which each component of cyber power, including private business, is prepared against cyber attacks. Hiller and Russell (2013) correlate the private

sector's preparedness with national security and argue that governments' pledges to secure their respective cyberspaces need to extend to private businesses in order to reduce and prevent increasingly severe threats at both the national and organizational levels. According to the 2010 Government Accountability Office Report, private businesses own and operate almost 85% of critical infrastructures and strategic assets in the United States. Although there are comparatively few examples of such collaboration due to regulatory, cultural, and social factors, the power of the private sector is increasing in developing countries (Kareke and Qasimi 2010). In line with the private sector's increasing presence in the cyber realm, this current study examines organizational competency and vulnerabilities in terms of cyber security preparedness in both the public and private sectors.

3) Finally, democratic values are also becoming a real concern for cyber security governance. The way components of cyber security governance (mainly government, private parties, and individuals) interact with each other increasingly determines regime-type in a state. On the lower end of the cyber security governance spectrum, at the national level, there are authoritarian states controlling Internet access to keep users on state-approved sites (Bremmer 2010). For example, MacKinnon (2011) warned that what technological developments promised about individual empowerment in the democratic world is being turned into a kind of "networked authoritarianism" in China. On the other end of the spectrum, there are democracies promoting the use of an open Internet to let freedom of expression, innovation, and individual empowerment flourish. If democratic values do not find their expression in the cyber domain, the balance between democracy and security may collapse in favor of security.

Brito and Watkins (2012, 46), however, argue that although there has been a push for increased governmental involvement in cyber security, there is not enough verified evidence to substantiate those threats claimed. Furthermore, they claim that "cyber threat inflation parallels what we saw in the run-up to the Iraq War." What is emerging today is an industrial complex reminiscent of the Cold War. According to these authors, the Cyber-Industrial Complex manipulates markets by fully harnessing the spending power of consumers' fear; by their estimates, by 2015, the cost of this "threat inflation" could total as much as $140 billion.

In short, cyber security preparedness depends on the degree to which a government 1) mobilizes private actors to take part in security initiatives against common threats and 2) organizes its interdepartmental model according the needs of public and private entities. This study seeks a more thorough and balanced understanding of cyber security governance at the organizational level. At this time, it would be appropriate to highlight two important principles that guided the development of this work. First, the private sector is no longer the sole consumer of nation states' security blanket. In contrast to traditional security theory, the private sector is a highly empowered and capable agent that and contribute to and produce cyber security and can thus cooperate with governments. Second, while issues of global Internet governance and international cooperation have never been more pressing (Mueller et al. 2007), this study will not address the existing structure of global Internet governance. That way, its scope will remain focused, clear, and tenable.

Purpose of the study

The purpose of this study is to offer insight into the relationship between public- and private-sector cooperation and national cyber security preparedness within the context of the current situation in Turkey. While focusing on domestic network governance, the study will highlight how governments (and, more specifically, governmental institutions responsible for protecting cyber security) should organize themselves and cooperate with the private sector, an entity that owns critical infrastructure which must be protected (Douglas 2012; Koski 2011). Using points taken from the official Turkish National Cyber Security framework, the study will also examine the public and private sectors' preparedness levels against cyber threats and the value that organizations attribute to the equilibrium between democracy and security.

Research Questions

This study arose from the following primary questions:

1. Does cooperation between public institutions and private companies increase a nation's cyber security preparedness?;

2. Is the level of preparedness against cyber security threats higher in the government agencies than in private sector?; and

3. Do government officials allow the cyber domain to operate under more democratic frameworks than they do the private sector?

Rationale of the Study

This study takes its place among the growing amount of political science scholarship focusing on cyber security. Although there has been no shortage of attention devoted to cyber security in public affairs literature, existing studies are generally industry surveys that snapshot current IT security governance and provide general recommendations for how to protect critical infrastructure. What they lack, however, is a coherent, consistent analytical framework for enhancing cyber security at the organizational and national levels (Belk and Noyes 2012).

Cyber security governance as a matter of inter-organizational dialogue and action has largely been absent from the canon, as well as insights into how different models of collaboration – intra-governmental and between governmental agencies and the public sector – can help safeguard against cyber threats. My proposed research will address these gaps in public affairs scholarship and provide a more concentrated focus on cyber security as a question of inter-organizational cooperation. My research will also contribute to existing dialogue on cyber security through its appraisal of democratic values as critical components of cyber security governance. Furthermore, from a practical standpoint, study findings would theoretically allow the likes of such bodies as the Turkish Ministry of Interior to map out the current status of national cyber security governance and reposition themselves accordingly.

The choice of Turkey as a focus is not arbitrary. Turkey accords the utmost importance to developing its digital information and communications infrastructure. The Turkish National Security Council approved a defense strategy in 2012 that listed cyber security threats among national security concerns for the first time. In a similar line of reasoning, Turkey's military

strategy was revised in October 2010 to include cyber threats among other nonconventional threats, such as terrorism, warfare, and natural disasters (Lewis and Timlin 2011). More importantly, in its 2013-2014 National Cyber Security Action Plan, Turkey acknowledged that without effective coordination and collaboration among its public and private sector organizations, the nation will not be able to secure its cyber domains, at least from the point of view of critical infrastructure (Kurt 2012). As such, Turkey represents a nation interested in developing its cyber security governance and protecting itself against exponential cyber threats, thereby making it an intriguing case study for this research.

Although Turkey's intention to secure its populace's cyber security is admirable, the organizational tasks assumed by Turkish authorities following the National Cyber Security framework are problematic. For one, the current distribution of cyber defense responsibilities among public agencies is based on agencies' technical capacities, with more capable institutions assuming more central roles in the National Cyber Security framework. The Ministry of Transportation, Maritime Affairs and Communications, for example, has the leading role among governmental organizations, even though in the past it has played a minimal role in guaranteeing security. In most developed countries, however, organs who are already responsible for security measures are the ones occupying lead positions. Moreover, Turkey's security blueprint does not fully take into account the vulnerability of the private sector, which is just as important as the public sector in guaranteeing online safety. Analyzing these problems will help us better examine the importance of inter-agency and inter-sectorial (public-private) collaboration in efforts to protect the nation against threats. Turkish policymakers will thus be able to more fully grasp the

scope of the problem, execute appropriate policies against cyber threats, and reorganize agencies' roles in Turkey's interdepartmental security framework.

Key definitions

For the purposes of this study, defining key concepts is crucial since literature on cyber security governance, although produced in mass quantities, often lacks uniform, conceptual clarity (Jong and Lim 2014). First, an important term used in this current study is cyberspace, a term that the 2008 National Security Presidential Directive defines as

"the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people" (54).

Hathaway and Klimburg (2013) argue that the phrase "interactions between people" needs to be emphasized more, since it highlights how cyberspace entails not only hardware, software, and informational systems, but also human interactions captured through digital networks. Examples of such interactions range from cyber self-expression to criminal activities and national cyber space defense (in the event of cyber wars). Rather than focusing on nuances differentiating criminal activities in cyber space, this study presupposes that an effective model of cyber security governance should be structured to protect the nation from any and all threats and should not exclude possible scenarios based on their (non-)compliance with a set definition.

Klimburg and Mirti (2012, 13) conceptualize cyberspace in terms of "multiple interdependent layers of activities" and introduce a four-layer model of cyberspace consisting of:

1. A physical layer, which includes all hardware devices;

2. A logical layer, which generally refers to software;.

3. A content layer, which is defined as all the information created, captured, stored, and processed within the cyber domain; and

4. A social layer, which designates the human factor and human presence in the cyber domain. As a principle, the social layer contains governments, private sector, and individuals as well (14).

There are two key characteristics which layers demonstrate in the aforementioned model. First, each layer is just as important as the next. Second, circumstances arising in any layer ultimately seek to influence the "social layer." For example, hardware – technically speaking, a component of the physical layer – can be used to monitor dissidents' actions and movements, thereby tracking their activity in the social layer. These features of cyber space make it a complex, dynamic environment.

Regarding cyber security, this study will use the definition from the International Telecommunications Union (ITU), which states that

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

This definition also reflects that people, processes, and technology are interwoven together into the cyber domain (Andress 2003). Due to its linkage between non-state actors, such as individuals and private organizations, and state security (Hansen and Nissenbaum 2009), cyber security involves protecting assets (including individuals) besides information (von Solms and van Niekerk 2013). Due to the rapport between these actors, national security is becoming increasingly synonymous with private-public sector security.

As far as threats to cyber security are concerned, Ammori and Poellet (2010) classify them into three main categories. The first category is espionage that involves accessing government, financial, or corporate information. The second category is comprised of cyber assaults entailing much broader threats, ranging from denial of service attacks to sabotaging electrical grids, air traffic controls, and military command communications. The third category involves criminal activities such as online identity theft and fraud. Nye (2010), on the other hand, breaks down cyber threats to national security into four major categories: economic espionage, online crime, cyber war, and cyber terrorism. This study will use Nye's categorization of cyber threats because of the increasing prevalence and relevance of cyber terrorism.

The final term to be discussed in this section is national cybersecurity. Even though governments' respective definitions of 'national cyber security' vary, Hathaway and Klimburg (2013) define the concept for NATO's cybersecurity framework manual as

"the focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security" (29).

Klimburg and Mirti (2012, 15) state that national cybersecurity is not one single subject area; rather, it is generally divided into five distinct "mandates." Each of these mandates is normally covered by different organs and agencies within a given government. This split in organizational responsibilities is largely caused by both the cyber domain's borderless, complex nature and by some agencies' desire to retain their real-world authority in the cyber domain. These mandates are:

1. Military Cyberactivities,
2. Counter-Cybercrime,
3. Intelligence and Counter-intelligence,
4. Critical Infrastructure Protection and National Crisis Management, and
5. Cyber diplomacy and Internet Governance.

The primary organizational challenge triggered by such a split in roles and responsibilities is the significant lack of coordination among governmental bodies in protecting national cyber security, even when agencies' concerns largely overlap. The solution here is to engage these mandates in tandem with each other; otherwise, it is difficult to develop a comprehensive and effective national cyber security strategy while focusing on only one mandate at a time (Hathaway and Klimburg 2013; Klimburg and Mirti 2012).

CHAPTER 2

LITERATURE REVIEW

Introduction

The following literature review is divided into three sections. The first section explains how severe cyber threats can be for governments; the second section focuses on specific threats that public and private organizations face in the cyber domain; and the third section discusses democratic values under constant threat from heightened security measures in the cyber domain.

Threats to Governments

Cyber security concerns increase when national political processes cease to function as undisputed centers of societal governance (Skelcher and Torfing 2010). According to Mayer-Schönberger and Lazer (2007):

"All government is, in part, about acquiring, processing, storing, and deciding upon information…The ability to acquire and disseminate information, to control the flow of information, has often been described as a source of power…To be sure, modern information and communication technologies frequently change the flows of information" (6).

So diffused are informational flows between governmental bodies, as well as between the government itself and the citizenry, that regulating change in today's digital age is beyond the scope of any government. Therefore, traditional forms of government need to adapt to the ever-

changing dynamics of the cyber domain. Furthermore, today's governments face the amorphous nature of cyber threats, i.e. the fact that

"…the cybersecurity problem does not fit conventional or traditional security categories based on individual security responsibilities, economic or corporate security issues, military security problems, as well as domestic versus international problems" (Harknett and Stever 2011, 456-456).

Schmitt (1999) agrees that cyber threats differ from traditional threats in that the former generally involve data manipulations or service disruptions. However, he also adds that they have the capacity of wreaking as much harm as physical weapons. Additionally, the most important aspect of cyber threats is that they can be launched from "anywhere in the world, at low cost, and with incredible speed" (Warner 2012, 5). The escalating nature of cyber threats, carries implications for policymakers and institutions (Dunn-Dunn-Cavelty 2008).

As a result, there is a growing need to incorporate institutional and political aspects of cyber security into those techno-centric approaches which currently dominate discourse on the topic. Shackelford (2012) emphasizes that without addressing the myriad governance gaps at the national level, security in cyber space cannot truly be enhanced. According to him, in order to effectively fill the governance gaps, it is a necessity to establish a cyber security strategy that is enforceable at the national level and that is compatible with global governance structures. A coherent national strategy will thus be able to guide operational organizational structures in providing cyber security (Ghernouti, 2010). However, while analyzing 19 countries' national strategies, Luiijf et al. (2013) argue that although states aim to address a uniform set of cyber

security threats, their issues of national importance and resultant problem-solving approaches differ substantially.

Dunn-Dunn-Cavelty and Suter (2009) examine governments' security role in cyber space through the lens of governance theory. They compare classic neo-liberal concepts of governance with the so-called "network governance approach." In their mind, while the former is based on a loose monitoring system of actors who collaborate with the government, the latter is based on a notion of self-regulating networks. Self-regulation involves coordinating and stimulating functional networks in such a way that state-ordained tasks are carried out as effectively and economically as possible. According to the authors, although a network government approach results in an increased role for government, it is nonetheless a useful method to engage private actors in collaborative projects.

In a case study carried out by the RAND Corporation (2013), researchers analyzed how European countries characterized cyber threats and what national-level response mechanisms they had created. The study revealed that although examined countries were in different stages of developing and implementing their respective security strategies, they all integrated cyber security into their broader national frameworks. The study also found that some countries maintained "existing 'real world' remits in the cyber world: for example, police managing cybercrime investigations and security services tackling espionage" (9). As such, the study underscored the need to find appropriate policies and avenues of communication to coordinate and organize responses to security threats and to ensure uniform responses from engaged domestic actors.

In the highly complex and intertwined environment of cyber space, extra-governmental entities play an increasingly influential role (or at least demonstrate a heightened interest) in stabilizing the dynamics of national security (Brechbühl et al. 2010; Stavridis and Farkas 2012). On the one hand, private businesses ranging from social media sites such as Facebook and Twitter to financial institutions such as Citibank, Nasdaq, and Mastercard are all vulnerable to cyber attacks. As such, every effort governments take to arm the private sector against attacks will contribute to national security and promote economic stability in an unsecure digital world (Hiller and Russell 2013). Germany, France, and the UK followed this line of reasoning when they included cyber threats as national security threats (Clement 2013). On the other hand, since most critical services are owned or provided by private sector firms, their decisions and abilities to maintain organizational security can directly impact public vulnerability. For that reason, when protecting critical infrastructure, corporate owners should focus not only on organizational costs, but also on potential "social costs" in the event of a cyber attack (Auerswald et al. 2006, 8).

Friedman (2013) touches upon another significant aspect of the interdependency between the government and the private sector and argues that although safeguarding the citizenry's security and stability against threats is the universally-understood function of government, the cyber era opens new horizons allowing governments to include private sector actors in their efforts to provide security. For example, fostering non-commercial relationships between government agencies and private organizations takes the traditional, interagency ''whole-of-government'' approach to security one step closer towards a new "whole-of-society" paradigm (Klimburg 2011, Stavridis and Farkas 2012, 8). In contrast to the "whole-of-government"

approach, the "whole-of-society" approach embraces the involvement of actors besides those in government agencies in the planning and implementation of policy and operations.

The "whole-of-society" approach is increasingly becoming a necessity for governments "because the ownership, operation, and supply of the critical systems are largely in the hands of the private sector, the distinction between the private and public spheres of action is dissolved" (Dunn-Dunn-Cavelty 132). This imposes new roles and responsibilities for government agencies (Robinson et al. 2013; Colarik and Janczewski 2012), forcing them to abandon traditional notions of security and to cooperate with non-state actors. Even, then, in the face of vague threats, this new combined approach will help better ensure that national assets are protected more completely, circumventing possible coverage gaps.

Anderson and Moore (2006, 610) emphasize the importance of governance by arguing that security failures are often caused by poor planning. Nielsen (2012) focuses on cyber security governance at the national level and argues that cyber threats, like other national security challenges, require a comprehensive approach that galvanizes all instruments of national power: diplomatic, informational, military, and economic. However, such a large-scale mobilization means confronting organizational challenges and uniting actors with varying incentives to respond to identical threats (Mitropoulos 2006). This is a quite challenging task and will not be as easy to overcome as those technical in nature, because it involves finding a common ground among actors with different priorities and motivations (Kelly 2013; Belk and Noyes 2012).

Literature has seized upon the question of managing cooperation between the public and private sectors to bolster security (Goldsmith and Eggers 2004). Dunn-Cavelty and Suter (2009)

analyze governance concerns from a similar perspective and argue that there is no uniform solution in terms of how inter organizational relations should be arranged. Policymakers must consider such questions about structure and motivation as they craft their plans for collaboration between the private and public sectors.

The problem at the intersection of governance and cyber security is mainly two-dimensional. The first dimension relates to how cooperation can be achieved among government agencies. Hathaway and Klimburg (2013) emphasize this point and argue that complex problems warrant complex solutions. In the prism of cyber governance, government departments and agencies assume a number of particularly-defined roles (e.g. judiciary, law-enforcement, legislative, etc.) due to the multi-tiered nature of national cyber security. Even as recently as in 2010, as a Government Accountability Office (GAO) report from that year states, "roles and responsibilities for participating agencies have not always been clearly defined" (4), even after the White House had appointed a cyber czar in 2009. Experts recognize the difficulty inherent to effectively planning and implementing a national cyber security policy, acquiescing that "government institutions are now struggling to define a problem that has no precedent and to craft a policy that will frame an ongoing organizational solution" (Harknett and Stever 2009, 456; Terrance and Hunker 2012). All the same, because cyber security is a "collective concern" (Brechbühl et al. 2010, 84), agencies' intertwined roles and responsibilities require the establishment of a coherent, coordinated action-plan involving close collaboration and the reorganization of governance structures (Hunker 2012).

The second dimension to the problem concerns the mobilization of private actors. Government engagement with security contractors and critical infrastructure companies has

always played a vital role in protecting national security (Douglas 2012; Koski 2011; Coyne and Leeson 2008). However, today's engagement strategy needs to include more than just contractors and critical infrastructure companies and incorporate other private businesses. Once these entities are able to fully combine their respective strengths, they can better provide national security and mitigate cyber threats across a wider playing-field (Asllani et al. 2013). A 2009 Cyberspace Policy Review emphasizes that it is a necessity to mobilize private organizations to lay the groundwork for consistent cyber defense mechanisms (Goodyear et al. 2010). True, organizations enter into relationships with others for several reasons (Croteau and Bergeron 2009); for example, they may wish to gain access to new resources, reach economies of scale, and/or share associated risks and costs. All the same, as Hare concluded in his 2009 study of private sector contributions to national cyber security efforts, it is crucial to empower the private sector to contribute to the development of cyber security enhancement measures, especially in view of its mass ownership of critical infrastructure. Inter-organizational relationships, then, just like inter-agency relationships, require coordination and interdependence, which are in turn dependent on how the relationships themselves are established and governed.

Even if government partnership with the private and public sectors is taken as a consensus, the form such a partnership takes is not uniform from country to country. For example, the United States has a dual network security approach that "relies predominantly on private investment in prevention and public investment in prosecution" (Smith 2005). Contrastingly, Herrington and Aldrich (2013, 299), upon examining cyber-resiliency efforts in the United Kingdom, concluded that what resulted there is a hybridized conglomeration of intelligence, security, risk, and resilience. They still found that the private sector played a

significant role in this hybridized realm due to its considerable amount of critical infrastructure ownership (i.e. approximately 80% of the entire market). However, despite differences in approaches, what unites these two systems is a governance problem: managing inter-organizational and inter-agency relationships through cooperation.

These two dimensions will be discussed under three lenses, which will aid in understanding the nature and depth of cyber security governance. Each section that follows in the literature review will provide detailed information regarding cyber security mechanisms, where governance theory claims the need for private-public cooperation is at its highest.

Public Private Partnerships (PPPs)

Dunn-Dunn-Cavelty and Suter (2009,1) argue that since "the state is incapable of providing the public good of security on its own," public-private partnerships (PPPs) become necessary to facilitate cooperation between the state and private actors. Stavridis and Farkas (2012) highlight that in order to enhance efficiency in public-private collaboration, government agencies need to prioritize mechanisms such as PPPs. In a similar vein, Rosenzweig (2010) argues that governments are unlikely to achieve high levels of cyber defense and resilience without resorting to PPPs. As such, PPPs' role in bolstering cyber security merit special attention.

PPPs comprise several forms, such as service contracts, ad hoc partnerships, and civic switchboard partnerships (Goldsmith and Eggers 2004). Although government-business relationships are generally formalized contractually (Kouwenhoven 1993), they can take several other guises based on the nature of specific goals or sets of objectives. Hathaway and Klimburg

(2013) touch upon this issue, arguing that the way to encourage private businesses to adopt a "whole-nation-approach" is to provide them with various incentives, ranging from enhanced security support to indirect commercial benefits.

The concept of PPPs became popular in the late 1970s in line with efforts to lessen bureaucracy in developed countries' government structures (Dunn-Cavelty and Suter 2009). The PPP was envisioned as a promising means to enhance personnel numbers, resource-sharing, staff specialization, and trust across sectors, thereby generating social benefits that neither the public nor private sector could do independently (Busch and Givens 2012). PPPs in the field of cyber security, however, are a relatively new phenomena which emerged in the 1990s. This new approach, with the advent of information sharing, captured the idea that there must be less government regulation in the cyber domain and that the private sector should take the lead in developing the Internet (CFR Task Force Report 2013). Since the cyber domain has unique features such as shorter time scales, domain-ownership issues, and "established regulatory structures" (INSA 2009, 4), PPPs in cyber domains have differed from previous partnership models; still, under proper, regulated application, they can yield similar results.

Even if situations on the ground vary from country to country, PPPs remain an effective framework for streamlining activity, maximizing potential between actors, and achieving comparable security goals. The U.S. 2010 National Security Strategy places particular emphasis on PPPs and exhorts the executive branch to collaborate with the private sector. Government agencies such as the Department of Defense (DOD), the Department of Homeland Security (DHS), the Office of the Director of National Intelligence (DNI), and the State Department are working to deliberately harness the private sector's capabilities in their efforts to achieve

national security (Stavridis and Farkas 2012). The same remains applicable to the EU. In his 2013 study, Irion focuses on Network and Information Security (NIS) governance in the EU and examines cooperation between public and private organizations that operate information and communications technology (ICT) networks. He concludes that effective NIS governance can be achieved through taking advantage of PPPs together with clearly-defined governance mechanisms.

Even if experts agree that PPPs can be used as an effective tool to ward off cyber threats, the question remains: should private enterprises enter into PPPs voluntarily or involuntarily? A 2011 white paper by industry groups and the U.S. Chamber of Commerce concludes that "an effective and sustainable system of cybersecurity requires a fuller implementation of the voluntary industry-government partnership" (4). Stavridis and Farkas (2012) define public-private collaboration as voluntary interaction between governments and private organizations to achieve resource efficiency. According to the authors, cooperation with the private sector does not necessarily involve financial transactions or even contracts; it can be fully voluntary. Furthermore, Lewis (2005) argues that while strict government regulation is necessary in such fields as banking, commerce, and transportation, when it comes to regulating cyber domains, a voluntary partnership model suffices. Still, certain experts oppose the assumption that voluntary partnerships are the primary means to enhance resiliency and cyber security and contend that governments should utilize other tools such as regulatory measures to fully take advantage of available resources (Harknett and Stever 2009; Shackelford and Craig 2014). If we accept the premise that the private sector is an indispensable actor in the cyber security framework, its

participation therein cannot be a completely voluntary matter. Otherwise, it may not engage to the full extent possible, and national cyber security architecture could resultantly fail.

Even if the government provides incentives for partnerships with the private sector, cooperation between private and public entities is often complicated by parties' diverging interests. While the private sector perceives security as a question of ensuring commercial continuity, the public sector views it as a public good that the government inherently generates (Dunn-Dunn-Cavelty and Suter 2009; Chesterman 2008) Therefore, mobilizing cooperation between these two sectors turns into a significant challenge for governments. To overcome this challenge, governments have several options outside the volunteer model: namely, they can coerce, co-opt, or simply convince non-state actors to support their policy objectives. Even though commercial instruments can motivate private businesses to join forces with the state, many governments generally prefer legal means such as regulations to coerce their subjects (Klimburg 2011).

The extent to which a government will embrace either a voluntary or involuntary model to PPPs depends on its ability to offer incentives to private actors. Clinton (2011) explains PPPs in the cyber domain through the prism of social change theory, predicated on the presumption that a relationship arises if rewards outweigh costs. Should this be the case, the private sector has incentives to cooperate with the government and jointly fortify security efforts. Moreover, Clinton argues that the government should compensate private businesses for cyber security investments exceeding their commercial needs. Otherwise, private sector contributions to national cyber security defense would be transformed into a subsidy to the government, a subsidy for a task which inherently falls to the government. Such a subsidy could further result in

a dysfunctional, uneven relationship marked by a lack of commitment and proactive behavior from the private sector.

As high as the government's expectations may be for the private sector, the private sector has still demonstrated a want and a need to combine forces with the government. The U.S. National Infrastructure Protection Plan (2006) posits that private sector owners and operators determine how much to invest in security defense based on an analysis of risks versus consequences. Although they are responsible for taking necessary steps to manage risks and for investing in security, private sector owners still "rely on government entities to address risks outside of their property or in situations in which the current threat exceeds an enterprise's capability to protect itself or mitigate risk" (National Infrastructure Protection Plan 2006, 26). Even technology firms may seek government assistance to tackle imminent threats coming from the cyber domain. For instance, Google and the National Security Agency formed an alliance to secure Google's digital infrastructure and to protect its intellectual property in response to highly sophisticated and targeted cyber-attacks allegedly coming from China. (DeVos 2011). These examples clearly demonstrate how if left to their own devices, private organizations would be unable to wholly protect their digital infrastructure; as such, they are reliant on government partnerships, even if the impetus for such a partnership could possibly arise "from the top to the bottom."

A 2009 INSA report entitled "Addressing Cyber Security through Public-Private Partnership" analyses existing partnership models implemented in the U.S. and specifically focuses on the role that government agencies play in cyber security PPPs. According to the report, since the government has legitimate authority to enforce laws regulating markets, its

agencies become an essential component of PPPs. They assume significant and distinct roles in overseeing and regulating Internet security, ranging from investigating cyber incidents to punishing violations.

The roles that government agencies play in PPPs catalyze a redistribution of responsibilities among public and private entities. Mueller and Kuehn (2013) focus on whether the federal government's cyber security initiatives alter organizational relationships between government agencies and affiliated private organizations in terms of lines of responsibility, management, and control. Their study's examination of the Einstein program and the Defense Industrial Base Enhanced Cybersecurity Services (DIB/ECS) program demonstrated how collaboration between federal agencies and departmental networks led to increased security and centralization in the cyber realm. In order for engaged actors to effectively protect the cyber domain under these new circumstances, then, it was essential for them to fully grasp changes not only in their operating environment, but also in their operating relationships.

As roles and responsibilities are redefined, they ultimately create a more stratified, hierarchical playing field. Madnick et al. (2011, 3) examine key organizations at the national, international, and intergovernmental levels to evaluate the strengths and weaknesses of their institutional and operational cyber security frameworks. Their study indicates that the cyber security 'institutional eco-system' is a complex mix of national, international, and private organizations with unclear mandates and/or overlapping spheres of influence. Relationships among independent actors in the cyber domain mimic the same groups' relationships in the physical world and transform into organized hierarchies.

The government's involvement in defending cyber safety, however, raises questions about the nature of emergent hierarchies. For instance, are hierarchies productive or even desirable when it comes to maintaining and promoting cyber security? Goldsmith and Eggers (2004) argue that hierarchic government mechanisms are fundamental elements of complex governance systems. According to these authors, governments can take advantage of networks in the name of societal good under the condition that networks do not replace elected leaders responsible for formulating public policy. However, Quigley and Roy (2011) observe the political, organizational, and societal dimensions of cyber security in order to evaluate how risk perceptions are shaped in a highly dynamic and fragile cyber domain. They contend that as far as the public sector's capacity for recognizing, mitigating, and responding to cyber risks is concerned, governments' hierarchal tendencies are insufficient at maximizing systemic resilience in an increasingly interdependent environment such as cyber space.

There are several reasons that experts advance to explain why hierarchies are insufficient for establishing security in the cyber realm. For example, the U.S. Chamber of Commerce, in its 2011 white paper "Improving our Nation's Cybersecurity through the Public-Private Partnership," underlines that "more government-centric set of mandates would be counterproductive" to guaranteeing economic and national security. From their point of view, more cyber regulations mean more burdens for American companies in the private sector, rendering them uncompetitive in the marketplace. As a result, they claim that hierarches must be replaced with alternate structures capable of promoting security, competition, and collaboration across multiple fronts.

Networks comprised of public and private organizations seem to be the best alternative to hierarchies. Critical of hierarchal structures, Rhodes (1996, 666) challenges the supremacy of the central government, arguing instead that the state has turned into a polycentric entity. Therefore, in this new political environment, the state functions as "a collection of inter-organizational networks made up of governmental and societal actors with no sovereign actor able to steer or regulate." Following such high fragmentation, a specific, tailored form of governance must emerge that takes into consideration this new polycentric structure (Dunn-Cavelty and Suter 2009). Even if networks are to be used as a means to promote security and collaboration, though, they must not replace elected leaders responsible for formulating public policy (Goldsmith and Eggers, 2004).

PPPs can function under the network model that the aforementioned studies conceive, especially since the need for private sector engagement is most acutely felt in cyber defense (Stavridis and Farkas 2012). Focusing on the organizational design of PPPs that protect critical infrastructure, Dunn-Cavelty and Suter (2009) recommend that partnerships be based on self-regulating and self-organizing networks as much as possible. Such partnership models necessitate a highly constrained role for the government. With the government no longer the only actor in the public sphere (Krahmann 2003), what occurs next is a transition towards increased private-public sector collaboration (Goldsmith and Eggers 2004; Donahue and Zeckhauser 2006). Network governance theory, for example, posit that over time, traditional homeland security organizations with their traditional "top-down" structures become increasingly flat and yield to more joint engagement with non-state actors. This means that government agencies will generate public value through partnership mechanisms while solving complex horizontal

problems, having abandoned old-fashioned vertical models (Busch and Givens 2012). As such, networks – specifically, under the guise of PPPs – are increasingly emerging as alternatives to hierarchical government structures in the cyber domain as the natures of the cyber and governance landscapes shift.

Even if they have the capacity to function as successful networks, PPPs are not flawless structures in and of themselves. Koski (2013) examines U.S. Government Accountability Office reports to chart variations in PPPs' success rates at protecting critical infrastructure. More specifically, his study assesses the extent to which DHS has addressed key components of partnership planning and established structures that encourage collaboration and trust-building. His findings highlight how PPPs are limited in addressing complex problems, due to their lack of strong leadership and clear policy goals. Similarly, a 2008 report by the Center for Strategic and International Studies (CSIS) entitled "Securing Cyberspace for the 44th Presidency" points out that many cyber security PPPs have suffered as a result of poorly-defined goals and objectives, as well as from a lack of coherently-defined strategies and partnership plans. On the one hand, public and private organizations need to collaborate across a host of issues such as research, education, and human resource development (Lewis 2010; Kostyuk 2013), thereby ensuring interoperability among partnering entities and establishing frameworks for national and international policy (Lord and Sharp 2011). On the other hand, public and private entities sometimes view PPPs only as avenues for information sharing and thus limit their ultimate potential. CSIS thus concludes that PPPs are failed solutions that should be replaced by newer, more effective entities and strategies.

On the one hand, failures in PPP structure and operation are not unique to the US context. In their analysis of cyber governance in New Zealand, Shore et al. (2011) noted only marginal success in terms of PPPs' abilities to protect critical infrastructure, due to similar reasons as those noted in American case studies. On the other hand, there exist possible solutions for those flaws which experts have identified. For example, a 2010 Government Accountability Office (GAO) report on critical infrastructure protection suggests that in order for a PPP model to be fully adequate, it must account for divergent expectations from both public and private organizations. Similarly, Scully (2014) argues that instead of waiting for the government to assume leadership on policy, strategy, and/or PPP coordination, the private sector should take the first initiative on these fronts. Finally, Zarvic et al. (2012) state that both public and private organizations must establish practices that support and align joint objectives. Otherwise, partnerships are prone to failure, and the cyber domain could remain as vulnerable as it was before, if not more so.

Information Sharing

Information sharing is an effective practice for achieving cyber security (Gordon et al. 2003). It is one of several avenues used to improve homeland security by streamlining cooperation among governmental agencies, as well as between businesses and the government (Givens and Busch 2013). Although a lot of scholarship fails to capture the extent to which information sharing can effectively mitigate cyber threats (Fleming et al. 2014), there are several explanations as to why both government agencies and private sector organizations are increasingly participating in information sharing mechanisms.

First, information sharing is cost effective. Gordon et al. (2003, 461) examined economic implications of information sharing for businesses and found that in the absence of information sharing, each business independently set its IT expenditures at "a level where the marginal benefits equal the marginal costs." However, they established that private businesses can attain optimal informational security at lower costs when information is shared through appropriate incentive mechanisms. To corroborate these findings, Gal-Or and Ghose (2005) used a game-theoretic model to examine the competitive implications of how organizations share information about security breaches and investments in informational security technologies. According to their analytical framework, by joining industry-based Information Sharing and Analysis Centers (ISACs) established under Presidential Decision Directive-63, businesses can enjoy strong economic incentives and thereby alleviate the burden of price competition. Furthermore, information sharing could increase social welfare by decreasing businesses' expenditures on informational security software (Kesan and Hayes 2011). Such cost effectiveness makes information sharing an appealing practice for the private sector, and it also helps public agencies achieve their security goals within their budgetary limits.

Second, information sharing lets private businesses access information that they cannot reach on their own. Kesan and Hayes (2011) stress the private sector's limited access to information and argue that through information, sharing private sector can access data that only governmental agencies can reach through intelligence tactics and law enforcement capabilities. This helps private enterprises understand the scale and scope of threats they could possibly face.

Third, relevant, timely, and accurate information sharing helps cyber defenders reduce the number and/or severity of cyber attacks. In their empirical study, Fleming et al. (2014) found

that as information sharing among relevant actors increases, the severity of cyber attacks decreases. More specifically, since private organizations are highly reliant on readily-available public information about cyber threats they face, governments can further enhance security by providing private organizations additional information about threats. Rowe and Gallaher (2006) empirically analyze the correlation between organizations' cyber security strategies and their reliance on public information. According to their study, although their tools are limited, governments can provide organizations with reliable, cost-effective information besides that which is readily available to the public so that private businesses can make informed investment decisions in the cyber domain. As such, organizations can take necessary precautions and establish effective response mechanisms for threats based on information shared between them and based on information the government provides.

However, it should be noted that there are commercial, legal, and/or strategic setbacks preventing organizations from sharing critical information in the cyber realm (Dynes et al., 2007). For example, if it is revealed that a private organization has lax cyber security, it will suffer from a blow to its reputation, and its market value will be compromised. This issue is also emphasized in a 2010 Government Accountability Office (GAO) report entitled "Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed." According to the report, there is limited information sharing among public and private entities due to private businesses' reluctance to share sensitive and exclusive information. The same report, on the other hand, criticizes government agencies for not providing the private sector with "usable, timely, and actionable" information. The reluctance of both parties to share information creates a major barrier that ultimately sacrifices overall security.

To remove barriers that negatively affect information sharing activities among public and private actors, government agencies first should ensure their own trustworthiness. Any relationship between public and private actors must be based on both trust and an understanding of the limits outside of which private businesses will not collaborate and/or share information with other entities (Goldsmith and Eggers 2004). Otherwise, as Busch and Givens (2013) argue, a lack of trust between the public and private organizations would impede cross-sector information sharing, failing to satisfy both parties' already-divergent security expectations (Busch and Givens 2012, Thomas 2013) and to largely impact national cyber defense. Governments must create an environment in which information sharing can flourish. To illustrate this point, while analyzing existing problems the EU faces while implementing its own information sharing policies, Robinson and Disley (2010) argue that national governments, as well as the EU, are responsible for ensuring their legal framework's compatibility with cross-sector cooperation and information exchange. By implementing the two fundamental steps of fostering trust and creating a cooperative environment, governments can better enhance information sharing, resultantly enhancing national preparedness levels.

Cybersecurity Incident Response

Governments cannot entirely delegate the role of securing their cyber domain assets to any third party. Nor, however, can they ensure cyber security on their own. To address criminal activities in the digital realm, both private and public entities need to play complementary roles, share information, and establish effective response mechanisms, (Choo, 2011a), thereby collectively mitigating cyber insecurities (Asllani et al. 2013).

However, the argument can be made that current response strategies are built upon "disconnected siloes of domain expertise" (Connell et al., 2013, 241). This set-up creates deficiencies in providing security, especially as cyber threats become more coordinated, large-scaled, and sophisticated. Therefore, individual organizations' reliance on their intrusion detection systems and on highly specialized IT personnel is not enough to mitigate threats which organizations face. For instance, Skopik et al. (2012) propose a framework for a national cyber security awareness mechanism based on coordinated efforts between all engaged stakeholders. According to them, in order to efficiently execute a response strategy on a national level, it is crucial for public and private actors to effectively collaborate across all domains of cyberspace while collectively combatting cyber threats. As a consequence, organizations must address cyber threats with responses that are just as coordinated as the threats themselves and that engage multiple public and private organizations.

Collective cyber security mechanisms, however, require effective governance mechanisms that can 1) take advantage of component organizations' experience, human resources, and threat information and 2) enhance their levels of cyber security preparedness. Levi and Williams (2014), for example, examine the UK's national cyber security strategy and partnership structures in its collective informational security efforts. According to their study, multi-agency cooperation aimed at reducing and reporting cyber crimes suffers from a lack of cooperation and coordination amongst organizations. In another empirical study, Chong and Tan (2012) examine three fundamental elements of IT governance – structure, process, and relational mechanism – in collaborative networks. Their study also emphasizes governance aspects of responses to cyber incidents and reveals that in order for collaborative IT governance to be

effective, there must be an active governing body that is able to stimulate high levels of communication among component organizations. As such, without effective governance, any collaborative cyber security mechanism aimed at responding to online incidents fails.

Cyber incident response mechanisms may be the initiatives of government or non-government actors alike. On the one hand, a study by RAND Europe, written on behalf of The European Network and Information Security Agency (ENISA), found that leading European countries operationalize cooperation among government agencies and the private sector through national initiatives, such as the Austrian Computer Emergency Response Team (AusCERT). On the other hand, the Computer Emergency Response Team/Coordination Center (CERT/CC) at Carnegie Melon University, a non-state mechanism, has greatly aided U.S. efforts to respond to incidents of cyber attacks (Mitropoulos 2006). While this body cooperates with US-CERT, it does not serve as an alternative to it. Governments must encourage non-government initiatives to take advantage of their expertise and harmonize cyber security efforts based on national goals.

In the ENISA's "Practical Guide on Development and Execution of National Cyber Security Strategies," it is also recommended that cyber incident response mechanisms play a key role in coordinating incident management tactics among relevant stakeholders at the national level. These mechanisms should also guide organizations on how to enhance their levels of cyber security preparedness. For example, Baskerville et al. (2014) conducted a comparative case study with three European organizations to analyze whether organizations struck a proper balance between preventative and responsive informational security activities. To illustrate the difference between these activities, while preventative measures such as intrusion detection are employed to deal with forecasted security threats, responsive measures such as password access controls seek

to manage unpredicted threats. This study empirically confirmed that organizations still needed guidance from a national body on reaching equilibrium between prevention and response strategies in order to be fully secure, since utilizing one of these measures does not eliminate threats thwarted by the other. By guiding private organizations, incident response mechanisms will relieve them of the heavy burden of independently 1) analyzing the threat environment and 2) adopting security structures accordingly.

Another key role that incident response mechanisms can assume is that of triggering and solidifying dialogue among IT professionals. Werlinger et al. (2010) conducted an empirical study to examine the tasks, skills, strategies, and tools that information security practitioners use to diagnose security incidents in public and private organizations. The study analyzes informational security practices as diagnostic work processes comprising three phases: preparation, detection, and anomaly analysis. According to this study, responses to informational security threats are complex, as practitioners tend to largely rely on their own tacit knowledge. The complexity of diagnostic work in some organizations is also exacerbated by practitioners' ignorance about advanced security tools. The most important finding of the study, though, is that effective responses to informational security breaches necessitate high levels of collaboration among IT practitioners that can be attained through professional engagement, such as IT professionals' sharing best practices. National cyber security thus requires a human resources pool composed of informed and knowledgeable experts. By creating opportunities to bring them together, incident response mechanisms may serve as a platform for enhancing IT experts' knowledge and information.

As a final point, it is worth mentioning that public policing agencies are of the utmost importance in terms of responding to cyber criminal activities and enhancing overall national cyber security preparedness (Choo 2011b). However, it is critical to mention that governments will not be able to challenge and investigate cyber crimes by utilizing traditional policing mechanisms. Law enforcement agencies need to go beyond established practices and reassess their policing strategies and techniques. They can then effectively participate in public-private cooperation mechanisms and facilitate information sharing across stakeholders in order to mitigate cyber threats (Choo 2011a) and contribute to cyber security response efforts.

Threats to Organizations

Given the world's rapidly-changing technology environment and a host of highly-capable adversaries, cyber threats have become more increasingly complex, unpredictable, and damaging for organizations. Moreover, public and private organizations' informational security statuses increasingly deteriorate because of their excessive reliance on information infrastructure (Khoo et al. 2010; Posthumus and von Solms 2004). This situation is exacerbated by the rise of cyber security attacks against both public and private sector organizations (Chabinsky 2009; Prieto and Bucci 2010; Hayes and Ebinger 2011). The benchmark study on the cost of cyber crimes, "The Cost of Cyber Crime Study: Global Report" (Ponemon Institute, 2013), examines the economic impact of cyber attacks and the costs organizations incur when they are targeted. According to field-based research findings, cyber attacks cost organizations an average of $7.2 million per year. This amount reaches as much as approximately $58 million for some organizations. Another striking finding from the study is that cyber attacks have become frequent occurrences, especially in developed countries such as the US, the UK, and Germany. Organizations

participating in the study experienced 343 cyber attacks per week, i.e. an increase of 20 percent from the number of attacks carried out during the previous year. Another survey conducted by the Ponemon Institute, "The Reputation Impact of Data Breach," found that brand and reputation values can decline from 17 to 31% after a security breach and that private business may need more than a year to recover its corporate image. This deteriorating security atmosphere requires organizations to navigate through a sea change and to adapt to their environment by taking necessary security measures.

In such a high-threat environment, protecting information is "as valuable and influential in the post-industrial era as capital and labor have been in the industrial age" (Arquilla and Ronfeldt 1993). This reality puts public and private organizations under high pressure to efficiently protect their information assets (Smith et al. 2010). Otherwise, security breaches would carry negative implications for organizations, implications bearing on such issues as customer privacy, intellectual property, industry competitiveness, and customer/citizen satisfaction (Hiller and Russell 2013).

Securing information, i.e. one of the most valued organizational assets, is primarily an organizational governance concern rather than a technical issue to be handled solely by specialized IT personnel (von Solms 2006). Von Solms (2005) argues in an earlier study that organizational management should treat information security as a strategic concern that is ultimately tightly linked to the organization's very existence. Therefore, boards of directors and executives, who are ultimately held accountable for any failure, are responsible for protecting information assets. Their task is to establish a corporate informational security policy, identify roles and responsibilities across all organizational levels (Solms and Solms 2004), establish risk

management measures and preparedness efforts (Mehravari 2013), and oversee these policies' implementation.

As mentioned above, IT governance must sustain and extend an organization's strategy and objectives; for that reason, it must be a high priority on executive leadership's agenda (De Haes et al. 2009). In practice, this can be achieved by either including chief information officer (CIO) in the executive-level decision-making process or by setting procedures to let the CIO report directly to the executive board or CEO. This will help better align business objectives and IT governance (Weill and Ross 2004). Furthermore, management structures in organizations should encourage CIOs to act as bridges between IT departments and all other branches of the organization, since IT governance is a collective responsibility. Heightened levels of engagement and responsibility will make all employees aware of their company's informational security goals and policies and will fortify partnership among IT department and other organizational units (Hardy 2006, 59; Weill and Ross 2005).

Organizations that differentiate informational security from other strategic management tasks create divides between organizational governance and informational security management. Such a disconnect can yield harmful results, as organizational leadership and employees may undervalue appropriate security actions (Johnston and Hale 2009; DaVeiga and Eloff 2007) and demonstrate insufficient commitment to protect valuable information assets (Posthumus and von Solmes 2004). Treating informational security issues as questions and tasks for organizational management is still a new concept (Ransbotham and Mitra 2009, 122). That said, concerns regarding information security governance have started to attract more attention across the world, especially as a result of large-scales corporate failures such as Enron, Arthur Andersen,

and WorldCom (Robles et al. 2008). With awareness on information security increasing, it is generally accepted that "the likely problem today is not the lack of technology, but its intelligent application" (Straub et al. 2008, 5). The recipe for intelligent applications of technology to secure information assets at the organizational level is governance that includes informational security in its mandates and that draws on all organizational assets, including human resources.

Julisch (2013) focuses on this emerging field of cybersecurity governance and examines cyber threats at the organizational level. He argues that "governance gaps are a common problem in cyber security" (2210) and emphasizes three governance problems that impede organizations' cyber security preparedness. First is the lack of clearly-defined roles, responsibilities, and processes to be observed following cyber attacks. Second is weak governance caused by poor decision making. In some instances, important security decisions are being made ad hoc. Or in other cases, organizations simply fail to make any decision at all because management does not consider certain decisions to within its mandate. Third, in theory, measures providing informational security normally should reach all management levels beyond IT departments; however, in practice, this does not happen frequently, and information security becomes an issue solely for IT departments. In conclusion, any weaknesses stemming from organizational governance may hinder attempts to solve inter-departmental disagreements and to align security needs across all organizational vectors.

Governance gaps are also apparent in cyber risk management. As organizational environments and systems (such as due procedures, technologies, and structures) become increasingly complex, proper risk management (including cyber risk management) becomes a precondition for ensuring businesses' continuity (Bonabeau 2007; Jirasek 2012). Equating low

levels of risk with enterprise security, Beasley (2007, 26) argues that risk management involves identifying potential events that may affect the business entity, mitigating their potential risks and providing reasonable assurance regarding the achievement of business objectives. Risk management is also an integral part of organizations' cyber security preparedness, as it allows an organization to minimize organizational vulnerability to cyber threats (Feng et al, 2014). Proper risk management thus serves as a road map that guides an organization in navigating through crises, yet not all organizations have such procedures readily in place.

There are several reasons why organizations experience governance gaps and do not attach utmost importance to risk management. Etzioni (2011) provides philosophical and practical considerations creating this deficiency. From a philosophical point of view, corporate executives entrust responsibility to their shareholders (who, in turn, own the corporations) and not to the common good. Their basic assumption is that if the market is not excessively regulated, private businesses would increase their stakeholders' profits. In line with this assumption, President Obama stated the following in 2009, when he commented on his administration's cyber security policy: "Let me be very clear: my administration will not dictate security standards for private companies." Highly motivated to generate higher profits through cost-saving, private sector executives care little to protect their most valuable asset – that is, information – by enhancing cyber security, which is an integral aspect of corporate governance's risk reduction strategy (Robles et al. 2008; Beasley et al. 2007; 2009 Lieberman Survey).

In addition to philosophical motivations for inaction, there are several practical ones, such as budget concerns, the vague nature of threat, competing goals, and a lack of appropriate incentives (Etzioni 2011). Furthermore, Abu-Musa (2010, 228) argues that risks to informational

security are not often sufficiently "understood by the board of directors and executive management." For that reason, the scope of countermeasures adopted by enterprises is not proportionate to the severity of perceived cyber threats, reflecting a gap between management perceptions and threat severity (Quey and Chang 2013). Moreover, in most private businesses, corporate cyber security policies often leave cyber risk assessment to midlevel managers who are neither familiar with overall organizational risk assessment nor have sufficient access to high executives (Kemp 2010). This deficiency prevents the establishment of effective information protection strategies that need to be tailored according to business objectives at the corporate governance level (Jirasek 2012).

In his discussion of practical considerations, Etzioni (2011) emphasizes current levels of incentives and argues that they do not promote voluntarily action from private organizations in the marketplace. This makes organizations more susceptible to cyber attacks. Focusing on the role of incentives in promoting security in the cyber domain, emerging literature links economics and cyber security and investigates how individuals' incentives shape security and, thus, network resilience (Acemoglu et al. 2013). Bauer and vanEeten (2009), for example, examine the co-evolution of cyber crime and cyber security markets. Their study reveals that incentives such as organizational reputation and revenue changes, as well as stakeholders' interpersonal relations, enhance security levels in the informational ecosystem. However, since differing security decisions disperse throughout the ecosystem, additional voluntary and/or government-led collaboration is necessary to achieve a secured cyber domain and to correct externalities.

Externalities occur whenever an actor's activity either generates security benefits that "the actor is unable to internalize" (Elkin-Koren and Salzberger 1999, 563) or imposes security

costs on non-consenting third parties in the market. Externalities represent a form of market failure (Coyne and Leeson 2008) caused by actors' incentives. Negative externalities result when actors "internalize all the benefits of [security] activities but not all of the costs" (Coyne and Leeson 2008, 479). Since not all parties share the entirety of the burden, markets fall short of providing security for organizations. The typical government response to such a market dysfunction is to discourage externality-causing behaviors by using mechanisms such as taxation or regulation. On the other hand, according to economic theory predictions, positive externalities occur when third parties with weaker incentives to adopt their own defense mechanisms latch onto investing firms' expenditures and therefore underinvest in security (Anderson and Moore 2006). As opposed to its reaction to negative externalities, the anticipated government response to positive externalities is to encourage externality-causing behavior by using subsidies as a leverage (Coyne and Leeson 2008). Acemoglu et al. (2013, 1) oppose general presumptions about positive externalities and argue that they lack complete reasoning in that they fail to consider that "security investments are also strategic substitutes." According to these authors, underinvestment by some agents will encourage overinvestment by others. In the end, regardless of whether externalities are positive or negative, national cyber security governance requires a full understanding of the market so as to ultimately eradicate their negative effects.

Organizations' decisions on cyber security are not only affected by problems associated with market externalities, but also by organizationally-perceived similarities between cyber security and public goods (e.g. neither one nor the other excludes consumers or organizations from consumption or from policy applicability). Because cyber security is "non-rivalrous" and "non-excludable" (Elkin- Koren and Salzberger 1999, 559) and organizations that seek profit

maximization believe cyber security is the responsibility of the government alone (Murray 2007), the market, according to economic theory, will tend to under-produce it (Powell 2005). The government should thus convince all relevant actors that cyber security as a public good can be obtained by sharing its entire burden among every agent that benefits from it (Nojeim 2010).

Similarly, a 2009 report by the Center for Strategic and International Studies (CSIS) states that since externalities and perceived similarities between security and public goods impede cyber protection, government agencies should fill the gap and incentivize the private sector to achieve national security objectives through regulations. Dourado (2012) supports this idea and points out that market failures justify regulatory interventions in the cyber domain. Jirasek (2012) also argues that without multiple driving factors, organizations would not invest in information security. According to him, the major drivers that incentivize organizations to invest in security are laws and regulations, business objectives, and security threats. Similarly, von Solms (2006) mentions that major motivations for securing information at the organizational level are regulatory compliance, legal liability, and reputation protection. (Luthy and Forcht 2006) In their empirical study, Johnston and Hale (2009) surveyed 700 security practitioners from the government and private businesses and established that legal requirements and regulatory compliance are the most important drivers for organizations to invest in information security at the strategic level. Concerns about privacy, legal liability, organizational reputation, and regulatory compliance prove to be secondary factors in decisions on whether or not to invest in informational security.

The Council of Europe's Convention on Cybercrime, which has been signed by 47 countries and ratified by 33, took practical steps to create private sector incentives based on

regulatory compliance. As such, the convention holds private businesses administratively or criminally liable for their actions in the cyber domain. In any case where a cyber crime benefits a company or where a lack of supervision or control from senior management results in a cyber crime, European private organizations will be held liable for their both wrongdoings and for inaction to take necessary steps in securing informational protection. Such a model of regulatory incentives could spread to other regions and take the place of voluntary incentives, which often fall short of eradicating market failures.

Although government regulation is an effective way to force private businesses to enhance security measures, it may cause substantial unintended consequences and undesirable behaviors, such as a decline in market competition and even an overall reduction in social welfare (Shore et al. 2011; Ghose and Rajan 2006). Furthermore, it may create a "culture… focused on compliance with cyber security require¬ments, rather than a culture focused on achieving comprehensive and effective cyber security" (U.S. Government Accountability Office 2013, 16). For that reason, many governments prefer to apply voluntary rather than mandatory provisions for the private sector, in part because using voluntary provisions enables governments to develop flexible legal standards for cyber security (Smedinghoff 2003; Shackelford and Craig 2014).

However, as far as compliance is concerned, public agencies may differ from private businesses in terms of their reactions to regulations. Smith et al. (2010) argue that if there is a mandate issued from senior officials, all government agencies must comply with this national de jure informational security standard. In another study, Quigley et al. (2013) asked decision-makers from Canadian and British public sector organizations about their approaches to

managing cyber risks and determined that participants were largely concerned with compliance with current legislation and policy. Jansen and Tranvik (2011, 121), though, found that government agencies in Norway have different approaches for IT governance. For one, the ministries the study examined generally have the authority to choose their own ICT governance models from a wide range of possibilities, including the instrumental model, the cultural model, the networked model, and the market oriented model. In addition, these ministries differ among themselves in terms of their IT structures, their use of outsourcing, and their levels of in-house IT capacity. Although a set of common procedures was introduced to harmonize ICT security implementation, because of the aforementioned differences in ministries' models and structures, such implementation was not been uniform and did not produce intended results. These ministries continued to see ICT as a tool to achieve traditional goals and did not embrace new types of ICT governance. As this Norwegian example shows, when complying with legislation focusing on higher security standards, public organizations tend to embrace different cyber security governance arrangements based on structural differences (Weill and Ross 2005, 29). Although public agencies, as opposed to private businesses, are legally bound to set their security standards in line with government targets, cyber governance must take into consideration differences in the public sector's IT protection strategies and organizational structures in efforts to enhance national security.

Another factor contributing to failures in cyber security governance is decision makers' insufficient knowledge about cyber threats. Managing organizational cyber risks requires knowledge about current vulnerabilities, about the nature of the threat in question, about preventive measures, and about costs associated with potential outcomes (Brechbühl et al. 2010).

However, there are not sufficient studies on factors affecting cyber security policies in government agencies and their readiness to defend against cyber threats (Caruson et al. 2012). Furthermore, although executive decision makers in the private sector increasingly strive to make informed decisions in order to raise security standards and meet organizational objectives, they have little guidance and/or experience to follow that would help them protect themselves against attacks (Ransbotham and Mitra 2009). This results in uninformed decisions in attempts to protect organizations' informational assets against highly sophisticated threats, thereby rendering organizations more vulnerable than before.

This situation is exacerbated by the fact that qualitative measuring systems for cyber security are not as advanced as they are in other domains, such as accounting and human resources; as a result, they are less able to guide decision makers. While there exist analyses and metrics that are crucial in helping identify "organizational and departmental weaknesses and shortcomings (Kemp 2010,10), they do not fully supplant the need for qualitative cyber security measurements. It is worth mentioning that efforts are underway to measure the efficacy of countermeasures taken against cyber threats (Garvey et al. 2013; Cavusoglu et al. 2004; Khansa and Liginlal 2009; Tanaka et al. 2005; and Liu et al. 2008); still, these studies are not sufficient for guiding decision makers in planning organizational cyber security policies. Before making any kind of investment, rarely does an organization have at its disposal a quantitative analysis, such as a cost-benefit analysis, to evaluate costs incurred and benefits received from cyber security expenditures. Rather, in many instances, decision makers rely on qualitative assessments based on attack and vulnerability statistics that capture current levels of threat and costs associated with past attacks. Additional factors determining appropriate levels of investment are

organizational characteristics, such as existing information technology (IT) infrastructure; the security needs of those products and services the organization provides; and customers' preferences and perceptions (Rowe and Gallaher 2006). All the same, these factors and qualitative assessments do not show threats' nature and potential; since, generally speaking, non-technical decision makers are unaware of threats, their reliance on these non-quantitative sources creates vulnerabilities in their organizations' security structures (Caruson et al 2012).

A final important concern that may impede cybersecurity governance is organizational culture. More specifically, an organization must establish "a culture of security in the organization's conduct-beliefs, behaviors, capabilities, and actions" (Allen and Westby 2007, 2), otherwise it will fall victim to cyber threats. To prevent this, organizational security culture can be developed through its leadership. The board of directors and high executives implement measures and policies aimed at protecting informational security, which ultimately guide interactions among employees and working procedures (Da Veiga and Eloff 2007). Moreover, training develops a culture that eventually shelters an organization from cyber-attacks (Trim and Upton, 2013). Following this reasoning, organizations should consider the complexity of cyber attacks and use different approaches, such as scenario-based planning and training, to enact security policies through culture change. If organizational culture lacks these components and approaches, all technological investments geared towards securing informational assets will fall short of providing efficient protection in the cyber realm, since even the simplest mistake from an untrained employee is enough to cause any defense plan to fail.

As we have seen, organizations are fundamental to national security. They face highly competent threats and need to protect their informational assets against them, yet they lack

appropriate levels of information on their adversaries based on scientific analysis. To manage cyber risks in a dynamic environment, they must be structurally, culturally, and strategically ready. Preparedness in all these areas is a governance concern for organizations and must be handled at the executive levels. When preparedness fails, organizations are destined to be victims of cyber threats and to incur ever-rising associated costs. It is not just organizations that must be prepared, but also democracies as a whole. Threats to democratic values and societies will be discussed in the following section.

Threats to Democracy

The Internet promotes a new kind of public sphere for public and private activities (Schwartz 1999) in which democratic freedoms can flourish. In the digital domain, people connect with others globally and share ideas through social networking sites such as Facebook and Twitter that are increasingly seen as tools to promote democratic governance (Hill 2012). Furthermore, people take advantage of such social networks to promote political accountability, to mobilize the public against oppressive regimes, and to express personal sentiments regarding political processes. Such examples of dynamic civic mobilization enabled by technological developments have the potential to greatly affect the political landscape (Diamond and Plattner 2012) and even serve as rallying points for revolutions and calls for social justice (Abdulhamid 2011).

The more information technologies "erode hierarchies, collapse time and distance, and empower networks" (Arquilla and Ronfeldt 1993), the more these changes' resultant social implications will force governments to adapt to emerging forms of direct democracy, replacing

their previous sources of power with models that are much more representative in nature (Lake and Sosin, 2002). Similarly, Naim (2013) argues that power is under attack in an unprecedented way that weakens the status quo it helped create. Micro actors are increasingly constraining the formerly almost-absolute authority of such entities as states and corporations, meaning that power now manifests itself in new ways in new spheres. Naím cites Wikileaks as an example of new actors who contributed to the transformation of our modern-day concept of power. By exposing government secrets via the Internet, Wikileaks showed that non-state actors can exercise more influence than states and can constrain the latter's power. This shift has inevitable repercussions on domestic politics, repercussions which emerge as political gridlock and/or policy paralysis.

Rapid changes triggered by technological developments will further challenge "the ascendancy of public management" (Stivers 2000, 12), changing how government agencies are operated. For example, Kernaghan (2000) compares bureaucratic organizations such as the Department of Defense with post-bureaucratic organizations such as the Passport Office. He profiles the former as an organization-centered, status quo-oriented, centralized entity. Such organizations take independent actions. The latter, on the other hand, is a citizen-centered, change-oriented, decentralized body. Post bureaucratic organizations are much more open to collaboration. He also argues that many public organizations around the world are following a reform path towards the post bureaucratic model so that they can keep up with the pace at which people and their demands change.

This transformation is of great importance, since it will lead to heightened implementation of private sector values (i.e. customer satisfaction) in the public sector.

Kernaghan (2000) divides public sector values (i.e. values oriented towards enhancing public goods) into three major categories: democratic, ethical, and professional values. Democratic values include accountability, responsiveness, and impartiality. Within this framework, bureaucracies normally consider their prime responsibility to be to elected officials (Sayre 1997); under this value transformation, public organizations are increasingly forced to become more directly accountable to the people, incorporating more private sector values and challenging the spaces they (i.e. public organizations) once occupied.

States' responses to this transformation are not limited to transforming how agencies and departments operate to better meet people's needs, but rather they also increase the power they exert in the cyber domain so as to enhance their control over digital networks. The Internet as an open, innovative, and dynamic environment is not designed for states' interference therein (Ziewitz and Brown, 2013). The trend of minimal state involvement, however, is increasingly changing. Bessant (2012) argues that despite all reasons for optimism, the digital domain also has a dark side that worries governments. Governments' anxiety, triggered by the diffusion of power from information and communication technologies, leads to heightened government control over the Internet (Deibert and Rohozinski 2010). Enhanced state involvement comes at the expense of values once promoted by the Internet.

Although imminent threats exist for every state, cyber space governance has evolved along two lines. While some countries want to establish a globally-institutionalized digital structure able to balance competing national interests, non-democratic regimes envision a fragmented, tightly controlled Internet that is susceptible to the desires and whims of the state. Such government interference has assumed many forms. Although a variety of measures are

viewed as legitimate (even by and in democratic nations), such as those protecting children from online predators, other acts, such as censoring political discourse and idea exchange online, are more controversial (Hill 2012). On the one hand, countries such as the United Kingdom maintain equilibrium between security and democratic values by limiting the government's own role and reassure citizens about their basic democratic rights (Luiijf, 2013). Such countries focus on preventing threats to economic growth and on instilling a sense of confidence in the Internet (Kelly 2012). On the other hand, states such as China and Russia seek to exert more authority over online networks (Lewis 2010) and exploit cyberspace for purposes of national security (Cornish 2009). They are even ready to consider shutting down the Internet as an option in situations where oppression is not enough to silence the masses. For example, the Egyptian government shut down the Internet to prevent peaceful demonstrators from uniting through social media and claiming their democratic rights (Thompson 2011). These latter states' combined motives and actions inevitably raise concerns about their commitments to core democratic values.

Nojeim (2010) argues that although cyber security has become a significant national concern, measures aimed at enhancing cyber security, such as having law enforcement officers monitor the Internet and conduct targeted surveillance (Deibert and Rohozinski 2010), they must not harm online freedoms such as privacy, the free flow of information, and the right to express ideas anonymously (Aquilina 2013). In concert with developments in information technologies, privacy protection has become the most pressing social issue (Nissenbaum 2004). This becomes all the more relevant as private information gathered by private companies and public agencies is being monitored and investigated by governments (Solove 2006). However, information

technologies' negative effects on online freedoms have been generally neglected in scholarship (Citron 2009). To keep online freedoms intact, a cyber security strategy needs to accord the utmost importance to transparency so as to build confidence and trust among societal actors. Cyber transparency is also a necessity if a government wishes to be held accountable for its measures' effectiveness and for any abuses that might occur.

The cyber domain is not immune to regulation. Contrary to general belief, it is overregulated by a multitude of public and private actors in ways that lack transparency and public accountability. This leads to concerns surrounding the private sector's role in providing Internet security, namely the role played by Internet Service Providers (ISPs). ISPs have the technical capacity to monitor traffic patterns across a wide number of connected computers. Therefore, they can act as law enforcement while tackling the more technical aspects of cyber attacks (e.g. identifying computers and botnets that spam). Although they might act as an additional layer of protection for the digital domain, if ISPs are given enough power to block potentially dangerous websites, fundamental freedoms and privacy rights could very well be challenged. Such actions from ISPs would also raise liability concerns from possible privacy violations and resultantly cause large-scale customer dissatisfaction (Ammori and Poellet 2010). In sum, the rapid technological developments triggered by the Internet will inevitably change how government agencies operate and will force them to be more responsive to democratic values, which are increasingly becoming more of an issue of concern for the digital domain. Governments that tend to exploit cyber space for the purposes of national security are inclined to neglect the equilibrium between the aforementioned and democratic values (Cornish 2009, Luiijf, 2013). Securing national assets through a heightened presence in the cyber domain must

utilize transparent means that promote accountability (Ziewitz and Brown 2013; Deibert and Rohozinski, 2010)); otherwise, security would be achieved at the expense of basic, fundamental rights.

CHAPTER 3

STUDY VARIABLES

Public-Private Cooperation

Since there is no uniform definition for the term cooperation in cyber security literature, conceptualizing public-private cooperation is of the utmost importance. To reach an all-inclusive conceptualization for the main independent variable (i.e. public-private cooperation) that meets this study's general framework, it is helpful to see how two terms – collaboration and cooperation – and their respective connotations are used within the broader spectrum of inter-organizational relations. Perry and Miller (2007, 3) provide a detailed definition of collaboration as

"…a process in which autonomous or semi-autonomous actors interacts through formal and informal negotiation, jointly creating rules and structures governing their relationships and ways to act or decide on the issues that brought them together; it is a process involving shared norms and mutually beneficial interactions."

According to Bardach (1998, 8), such joint activities are "intended to increase public value by their working together rather than separately." In light of this definition, literature holds that private and public entities decrease organizational expenditures. The value attributed to collaboration is on the rise due to its cost effectiveness (Mankin et al 2004). However, inter-organizational collaboration is most beneficial when parties are interdependent, relying on each

other to achieve a common goal or task (Thomas et al. 2006). Gray (1989, 232) argues that organizations' preexisting mutual reliance has reduced "the capacity of any organization to act unilaterally" in the current organizational ecosystem. Such a dependence on other parties, however, enables each agent to "search for solutions that go beyond their own limited vision of what is possible" (Gray 1989, 5) in this ecosystem.

Mattesich, et al. (2001), on the other hand, define cooperation as a set of

"informal relationships that exist without any commonly defined mission, structure, or planning effort. Information is shared as needed, and authority is retained by each organization so there is virtually no risk. Resources are separate as are rewards."

Klimburg (2012) points out the significance of cooperation among relevant stakeholders, arguing that it is central to all types of national cyber security issues. Examining Turkey's national cyber strategies, Senturk et al. (2012) argue that to ensure cyber security at the national level, it is necessary for Turkey to achieve a higher level of cooperation among public and private organizations. The Organization for Economic Co-Operation and Development's 2012 publication "Cybersecurity Policy Making at a Turning Point" examines cyber security strategies in ten countries (including Canada, France, Germany, and Japan) to identify commonalties and differences in national approaches to cyber threats. The study reveals that governments prioritize cooperation both to regenerate inter-agency operations and to reinforce public and private actors' relations, the ultimate goal being to enhance levels of national cyber security. As these studies demonstrate, literature emphasizes that cooperation between the public and private sectors is becoming a prerequisite for national cyber security governance.

With their respective strengths and limitations (Zarvic et al. 2012), both collaboration and cooperation represent distinct points on the spectrum of inter-organizational relationships. Collaboration generally represents more formalized relationships, whereas cooperation may include informal interactions. However, because reciprocal interactions between public and private entities may range from "formal institutionalized relationships" to "informal trade-offs" in the absence of rule-based relations (Gray 1989, 13), this study will use both terms interchangeably (Zarvic et al. 2012) so as not to exclude any possible form of interaction between public and private actors.

In general, Stavridis and Farkas (2012) argue that public-private cooperation generally falls into three broad categories of activities: sharing expertise, exchanging information, and executing projects and operations. However, cooperation among public and private actors varies across countries, together with cultural differences and governance styles. Furthermore, in their study, Narasimhan et al. (2010, 4) use game theory to present a cooperative model of defense against cyber attacks, wherein participants form coalitions and invest in joint protection. In this model, cooperation is defined as "the willingness of players to form a coalition and contribute to the cost of protection of the entire coalition." An analysis of their model reveals that the success of cooperative security measures depends on the nature of the attack and on the attitude of those defending the network. As a result, cooperation does not assume a uniform structure, and its success mostly depends on the extent of participants' contributions to meeting shared objectives.

As used in this present study, the first variable (i.e. public-private cooperation) means voluntarily interactions among public and private actors which are not aimed at generating profit, ranging from security consultations to joint participation in ad hoc or institutionalized

mechanisms. By engaging in such activities, public and private entities contribute to national security and resilience in the cyber domain. This concept of cooperation reflects the current study's broader focus on cyber security as a matter of governance (Donahue and Zeckhauser, 2006) and thus helps to solidify a more general understanding of the term.

National Cyber Security Preparedness

When we discuss national cyber security preparedness, i.e. the dependent variable that will be used in the first hypothesis (see H1, directly preceding the "Differences Between Public and Private Sector Organizations" explanation), it is necessary to carefully establish semantic boundaries around the term preparedness. Public affairs literature has defined preparedness as one of the four phases of emergency management, together with mitigation, response, and recovery. As a major component of emergency management, preparedness means taking necessary preemptive measures so as to enable social units to organize and respond actively when a disaster strikes. When prompt and effective responses are needed, preparedness entails both coordination among public agencies and cooperation among public and private entities (Lindell and Perry 2009), thereby bridging the gap between a diverse set of communities.

As far as threats to the state are concerned, preparedness must be administered at the national level so their scale can be fully gauged. To guide all levels of the US government in handling preparedness, the Eighth Presidential Policy Directive defines it as "…actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect gains, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the nation." The threats mentioned in this Presidential

Policy Directive include cyber threats. This is highly important, since it means that current efforts to boost national preparedness in the physical domain will be transferred to cyber space as they are tailored to meet the latter's unique features.

Preparedness, which is a relatively new concept, has increasingly been used in cyber security literature to mean planning ahead for cyber incidents with physical consequences to critical infrastructure. According to the CAN, a non-profit research organization, "cyber preparedness is the process of ensuring that an agency, organization, or jurisdiction has developed, tested, and validated its capability to protect against, prevent, mitigate, respond to, and recover from a significant cyber incident." This definition reflects the complex and multi-dimensional nature of preparedness efforts wherein coordination takes place among various stakeholders, such as informational security officers and owners/operators of critical infrastructure.

According to a 2010 task force report to Congress entitled "Perspective on Preparedness: Taking Stock Since 9/11," cyber security preparedness is a critical goal for governments at the local, state, and federal levels. The report also stresses the dependency of many homeland security operations on cyber-based systems, such as public messaging, emergency dispatch, incident management, and even recovery efforts. If any of these security operations were compromised by a malicious attack, emergency response and recovery efforts would greatly suffer. Although cyber security is a priority across all levels of the government, the report reveals that cyber preparedness lags behind other preparedness efforts launched since 9/11. The report recommends that cyber security be incorporated into the existing national emergency management framework rather than being relegated to a separate sphere. By devising a more

holistic approach to subsequent preparedness efforts, the US will be able to bolster cyber security and resilience in a more effective, streamlined manner.

This recommendation is also proposed in the 2010 National Cyber Incident Response Plan. The plan treats preparedness as a basic emergency responsibility of federal, state, local, tribal, and territorial governments and of the private sector. It also requires that cyber security professionals be prepared for incidents that may necessitate coordinated actions for response and recovery. According to the Plan, organizations are responsible for fulfilling all components of preparedness: evaluation, improvement, exercising, training, equipping, organizing, planning, and engagement. The Plan appoints the Department of Homeland Security (DHS) as the national coordinator responding to cyber incidents and tasks it with establishing and maintaining collaborative frameworks between the public and private sectors. Cyber preparedness efforts carried out according to the Plan provide public organizations with a more robust cyber security posture that lays the groundwork for collaborative operations against threats by taking advantage of all relevant stakeholders' collective experience and knowledge.

The US's 2013 National Preparedness Report (NPR) greatly helps stakeholders assess current levels of cyber preparedness in comparison with other core governance and defense capacities outlined in the National Preparedness Goal (NPG). The report analyzes approximately 1,400 sources and 3,200 measures and metrics in order to ascertain qualitative and quantitative preparedness across all 31 core capacities. The NPR defines five preparedness mission areas for each core capacity: prevention, protection, mitigation, response, and recovery. Using such data gleaned from a national assessment of preparedness across core, policy-makers can gauge areas of strength and areas for improvement from year to year. As a preliminary study to the NPR, the

2012 State Preparedness Report (SPR) assessed states' and territories' preparedness across core capacities. When the NPR aggregated individual states and territories' preparedness levels from the SPR to determine national levels, cyber security proved to be the lowest-rated core capacity.

The usage of preparedness in the above-mentioned studies, i.e. in the context of cyber incidents with physical consequences, is too limited when one considers the entire scope of threat originating from the cyber domain. For that reason, the current study distinguishes cyber preparedness from cyber security preparedness. Whereas the former term as used in the NPG study primarily focuses on protection strategies from the perspective of critical infrastructure, the latter term as used in the current study has a broader meaning that captures all aspects of the cyber security issue, including technical and governance aspects that are critical in combatting cyber threats effectively. For the sake of this study, therefore, it is important to focus on another concept, cyber power, in order to fully conceptualize national cyber security preparedness in a broader sense than it is used in other studies, i.e. solely within the context of cyber incidents with physical consequences.

Klimburg (2011, 43) argues that cyber power has three dimensions: "coordination of operational and policy aspects across governmental structures, coherency of policy through international alliances and legal frameworks, and cooperation of non-state actors- business and civil society." Each dimension provided by Klimburg links cyber power to governance. Most notably, establishing coordination among government entities and involving the private sector through cooperation can be achieved through effective governance strategies. Similarly, the Economist Intelligence Unit developed a cyber-power index on behalf of Booz Allen Hamilton that focuses on how countries defend against cyber attacks and on the extent to which they utilize

informational technology infrastructures to secure a robust economy. The index uses G20 countries' cyber protection abilities as a benchmark and constructs a quantitative and qualitative scoring model that consists of four categories (legal and regulatory framework; economic and social context; technology infrastructure; and industry application) and 39 sub-indicators to evaluate specific features of cyber power. The legal and regulatory framework category uses a composite indicator to measure countries' cyber capacity and focuses on the development of states' national cyber protection plans and levels of engagement in cyber PPPs. The legal and regulatory framework section lists the following additional means by which nations can enhance cyber power: creating a body enforcing cyber legislation and facilitating interdepartmental dialogue; passing laws on cyber security that guarantee data privacy; and institutionalizing appropriate mechanisms to respond to cyber-crimes and attacks. Such measures reveal that cyber power requires a multi-dimensional approach in the cyber realm.

Resultantly, taking into consideration states' abilities to respond to cyber incidents and their levels of cyber power, this study conceptualizes national cyber security preparedness as the capacity to recognize, mitigate, and respond to threats (Quigley and Roy 2012). As part of their cyber security preparedness mandates, states use effective governance mechanisms to enhance their resilience to cyber threats and to plot strategies based on the needs of both public and private organizations and on the nature of imminent attacks.

Based, then, on the aforementioned definitions and research summaries, this present study proposes its first hypothesis, i.e.

H1. Cooperation between public institutions and private companies is more likely to increase national cyber security preparedness.

This study will employ three sub-hypothesis that will help present a more through picture of association between public private cooperation and national cyber security preparedness:

1a. Organizational preparedness is more likely to increase national cyber security preparedness.

1b. The institutional effectiveness of government agencies with cyber security roles and responsibilities is more likely to increase national cyber security preparedness.

1c. The value attributed to the democratic gains is more likely to increase national cyber security preparedness.

Differences between Public and Private Sector Organizations

Marshall (2007, 41) argues that current literature on public and private organizations is grounded in "a tradition of industrial democracy." The main assumption of this tradition, according to Moore (1995, 28), is that "the aim of managerial work in the public sector is to create public value just as the aim of managerial work in the private sector is to create private value." This present study thus distinguishes between the public and private sector with respect to their motives, accepting that fundamental differences are reflected in organizations' cyber security approaches. As such, the second independent variable of this study's second hypothesis (see the end of the following explanation on organizational cyber security preparedness) is the difference between public and private sector organizations.

Organizational Cyber Security Preparedness

Caruson et al. (2012) argue that government agencies are reactive when implementing their cyber security policies. However, according to a 2012 survey study by InformationWeek, cyber security is among the top priorities of federal IT professionals, and federal government agencies' cyber security preparedness has significantly improved over the last five years, although it still remains low. Another 2012 study by Deloitte- Nascio, which assesses the status of states' cyber security programs, reveals that efforts to bolster cyber security preparedness have diffused all the way down to government agencies at the local levels. However, according to the 2013 National Preparedness Report, 52 percent of local governments at the state, local, tribal, and territorial levels are mostly or wholly reliant on the Federal Government for closing gaps in cyber capabilities, although they are responsible for securing their own networks. Compared to the public sector, on the other hand, the private sector's cyber security preparedness lags behind due to the high costs of essential measures undertaken to protect against threats (Hataway and Klimburg 2012).

In today's literature, scholars employ numerous terms to describe various aspects of cyber threat prevention. Although they overlap, they have distinct meanings that differentiate them from cyber security preparedness (Hansen and Nissenbaum 2009). For instance, Robles et al. (2008, 68) define information technology governance as "a subset discipline of corporate governance focused on information technology (IT) systems and their performance and risk management." Their definition entails two primary goals for organizations, which are 1) investing in IT to generate business value and 2) mitigating the risks that are associated with IT. Greene and Graubart's (2010) cyber preparedness methodology is also important to analyze

before treating this present study's own conceptualization of cyber security preparedness. According to their methodological framework, preparedness enables organizations to characterize cyber threats and to determine preparedness levels at which organizational security is ensured. Based on threat characterization and response analysis, organizations determine their cyber security objectives and establish managerial priorities for cyber security investments as part of their overall strategic planning.

Both the definition from Robles et al. and the methodology from Greene and Graubart imply that IT security is a responsibility for corporate governance (Solms and Solms 2004) and that the problem of informational security is relegated to internal processes within individual organizations. Such an approach, however, neglects three elements of cyber security governance: structure, process, and relational mechanisms (Chong and Tan 2012), some of which are inevitably related with factors external to the organization, such as its operating environment (Quey and Chang 2013). Therefore, like national cyber security preparedness, this study conceptualizes organizational cyber security preparedness as building capacity for recognizing, mitigating, and responding to cyber threats (Quigley and Roy, 2012), as well as enhancing organizational resilience to withstand them through effective governance mechanisms determined by organizational needs and the nature of imminent threats.

Following its conceptualization of variables from the previous discussion, the present survey now introduces the following second hypothesis:

H2. Levels of organizational cyber security preparedness are higher in the government agencies than in private businesses.

Differences between Public and Private Sector Managers

Quigley et al. (2013) argue that in comparison with private sector IT managers, public sector IT managers are more concerned with privacy and data integrity issues, particularly concerning publically-accessible information. Furthermore, the biggest cyber security risk for public sector IT managers is privacy protection rather than cyber terrorism, sabotage, and vandalism. According to them, these managers' focus likely results from legislation holding public employees accountable for any disclosure of personal information. In an effort to elaborate upon these findings, Macmanus et al. (2013) measure how interest groups – public, private, and nonprofit alike – pressure public agencies into protecting individuals' (including government employees') private information. The study's authors argue that IT professionals in the public sector are more proactive when it comes to protecting privacy than their colleagues in the private sector. However, according to the study, public organizations still lack clear standards and procedures that balance privacy protection and transparency while enacting cyber security policy. The aforementioned studies demonstrate how protecting privacy through laws and regulations yields positive results in public agencies, leaving them more sensitive to such concerns than private organizations are.

Another highly significant study, the World Values Survey, was conducted in in six wealthy democracies to compare private and public sector employees' commitment to democratic values. The survey found that public sector employees exhibit a significantly greater commitment to democratic governance than those in the private sector (Brown 1999). Goodyear et al. (2010) examined the extent to which chief informational security officers (CISOs) attribute value to civil liberties and privacy in 29 American states. Their case study revealed that such

issues are increasingly becoming a major concern for CISOs, given their growing understanding that compromising confidential information would make them accountable for such oversights. Although existing literature lacks reasons explaining differing commitments to democratic values among private and public sector employees, Moore (1995) highlights motivational differences in the public and private sectors: whereas the former motivates its employees with creating public value, the latter uses profit maximization to motivate its employees. Basing its arguments on these findings regarding differences in prioritization and motivation, the present study differentiates government officials from their colleagues in the private sector. This distinction serves as the independent variable in the formation of the last hypothesis (see the end of the explanatory section on democratic values below).

Democratic values

The basic definition of democracy states that it is the rule of "government by the majority of people" (Lijphart 2012, 30). Lewis (1965, 64-5), however, criticizes this narrow definition and argues that "all who are affected by a decision should have the chance to participate in the making of that decision either directly or through chosen representatives." Whereas the first definition of democracy views its essence as free, open, and fair elections (Huntington 2012), the second definition embraces a participatory approach and creates room for new mechanisms to promote people's direct representation in governance processes.

The concept of "democratic values" is very broad and includes such varied understandings as individual freedom, active participation, and the role of authority (Selvi 2006). O'Loughlin (2004) points out that definitions of democratic values can vary with time and

context. Dixon (2008, 681), in his quest to examine and compare liberal-democratic values in Turkey and the European Union, defines democratic values as "rule of law versus religious or authoritarian rule, and minority/human rights." Huntington (2012), however, views democratic values as governments' responsiveness to their citizens' needs. Although defined differently, there is a common belief that democratic values in traditional majoritarian democracies are being affected by developments in information and communication technologies. Such developments generate positive impact by alleviating deficiencies (Dahlgren 2005; Nye 2011; Naim 2013) caused by underrepresented populations. As states try to govern and secure their digital domains, democratic values will gain more importance by establishing boundaries that governments should not cross, lest individual rights be comprised in the cyber realm.

This study conceptualizes democratic values in a limited way, focusing solely on values threatened by governments at the expense of security in the cyber domain. In line with literature on democracy (Shane 2004), this study defines democratic values (i.e. the study's third dependent variable) as governments' 1) respect for individuals' privacy (Chawki 2010; Ozer 2012) and freedom of expression online (Muhlberger 2004) and 2) opposition to excessive intervention in the cyber domain. To better understand whether there is a balance between security and democratic values, it is necessary to focus on how democratic values are perceived at the organizational level. For that reason, the study hypothesizes that:

H3. Government officials will more closely abide by democratic values in the cyber domain than will private sector managers.

CHAPTER 4

MEASUREMENT

Research Design

This study employed quantitative research methodology with a self-administered survey questionnaire in order to measure self-imposed variables (i.e. public-private cooperation, national cyber security preparedness, organizational cyber security preparedness, institutional effectiveness, and democratic values) and control variables (i.e. organization type, organization location, organizational IT structure, and organizational size). It relied on survey methodology for collecting data, since this approach is appropriate for exploratory, descriptive, and explanatory studies (Kelly et al. 2003). Employing descriptive and explanatory quantitative methodology approaches in its research (Malhotra and Grover 1998), this study observed whether there is a statistically significant association between the aforementioned variables.

This method of collecting data across sectors enabled the study's author to evaluate factors influencing cyber security preparedness at the national level; to see whether levels of cyber security preparedness are higher in the public sector than in the private sector; and to assess whether values assigned to democratic values are higher in the public sector than in the private sector.

Sampling Strategy

This study's targeted sampling pool was all Turkish public and private organizations employing IT departments to conduct their day-to-day business. Considering the large number of public organizations and private businesses across Turkey, the researcher contacted a Turkish non-profit organization (the Cyber Security Association, or CSA) that specializes in enhancing online security and took advantage of its long-term experience in the field of IT security to gather data from a representative sample.

CSA also provided the research's sampling frame. Since its establishment in 1971, the CSA has seized upon the importance of information technologies' transformative role in our highly connected world and has partnered with public organizations to promote a culture of secure information exchange in Turkish society. To achieve its goals, the CSA has established ties with both the public and private sectors, promoting cyber security on all fronts at the national level. Although the CSA accepts individual members on the condition that applicants prove their status either as IT experts or as IT executives, the CSA is primarily based on organizational membership. To systematize member organizations' activities and create a dynamic environment for knowledge-sharing among public and private entities, the CSA established a mechanism called the Public-Private Cyber Security Initiative (PPCSI). The CSA's cooperation with public agencies and private companies aided this research because it provides the researcher with the opportunity to expand study's chance of capturing a dynamic network of public and private sector representatives. Obtaining a sampling frame and gaining access to potential participants through the CSA facilitated the researcher in collecting data and provided the study a strong, methodologically-sound sample selection.

The Public- Private Cyber Security Initiative is composed of 250 private businesses and 150 public agencies. Following this structure the sample set was subdivided in two mutually exclusive strata: public sector organizations and private sector organizations. With the understanding that the number of private businesses exceeds the number of public agencies, the study used a disproportionately stratified random sampling of actors. Otherwise, statistical estimates derived from proportionately-represented samples from each category would not be reliable.

The researcher cooperated with CSA executives to ensure that each government agency or private company listed in the sampling frame was a member of the CSA. To prevent the inclusion of duplicate organizations and companies in the survey, the researcher asked the CSA to generate a sample list from its institutional records. Similarly, it asked the CSA to treat subsidiaries and divisions of one organization as separate units. To finalize the sample set derived from the CSA's initial list, the researcher also verified that all e-mail addresses provided were institutional rather than personal before the CSA contacted potential participants. Ultimately, those entities which the CSA identified were organizations that also participated in the Public-Private Cyber Security Initiative. While contacting potential participants via email, the CSA explained the research and organizations' participation therein. Their initial email stated that an IT expert, CIO, or other executive knowledgeable about his/her organization's cyber security practices should complete the survey. It was clearly indicated that one response from each organization would be sufficient. Following initial contact from the CSA, the researcher sent invited members of the Public-Private Cyber Initiative to participate in the survey by following a special link he provided. On visiting the survey website, potential respondents could

read a cover letter that highlighted the purpose and significance of the study. Survey respondents were also provided a consent form, where the researcher highlighted that participation in the survey was voluntary and that respondents' confidentiality would be guaranteed. After these first exchanges, the CSA and researcher continued their correspondences with survey-takers, sending them reminder e-mails and calling them to confirm and track their participation.

Sample

The study's unit of analysis was Turkish organizations working in either the public or private sector. Rainey and Bozeman (2000) note that the distinction between the public and the private sectors is a generally-accepted principle in organization theory. The study's data were gathered from IT experts, CIOs, and other high executives responsible for IT departments in their respective organizations.

The reason why the researcher specifically targeted experienced and knowledgeable experts and executives is because data gathered in this study required detailed information on organizations' various cyber security practices. This information included organizations' security relations with other entities, especially government agencies, and measures taken to prepare themselves against cyber threats. It is generally accepted that only this demographic possesses knowledge of this kind of information; as such, it was the researcher's primary aim (Huber and Power, 1995).

Population

The targeted population was all Turkish public agencies and private businesses that employ IT departments to conduct their day-to-day business. These organizations created,

captured, stored, and/or processed one of their most highly-valued assets (i.e. information) within the cyber domain. The respondent organizations were all located across Turkey, which signifies the sample's representativeness of the study population.

In total, the researcher received responses from 229 organizations out of 400 between December 24, 2013 and April 2th, 2014, resulting in an estimated response rate of 57%. Although the number of respondents who began the survey was relatively high, not all respondents actually completed the survey. Cyber security governance is an emerging field, and awareness on this issue in developing countries such as Turkey is lower than it is in developed countries. In his empirical study on Saudi Arabia, Abu-Musa (2010), for example, reported that only 40% of Saudi public and private organizations have employed any kind of information security measures. These collective findings demonstrate that low responses rates can be the result of unfamiliarity with the subject at hand.

Public and private organizations participating in this study were expected to accord strategic importance to their cyber security policies as a matter of organizational governance, or to at least implement policies aimed at protecting data and encouraging compliance with laws and regulations. It can be concluded that participant organizations' average sizes were relatively high, as they have IT departments and staff, and that the very presence of IT departments and IT staff demonstrated organizations' concerns for protecting information assets. As far as micro organizations are concerned, they generally lack budgetary resources and expertise for investing in and executing cyber security measures (Gutirez et al. 2009). For that reason, the study population did not include micro organizations that did not have IT departments or at the very least experts employed to secure organizational data.

The researcher also expected a low response rate in this study due to the sensitivity of this issue for organizations. Previous research revealed that executives with similar positions, expertise, and qualifications were unwilling to disclosure sensitive organizational information (Abu Musa 2010, Kotulic and Clark 2004). However, guaranteeing participants' privacy and confidentiality helped the researcher gain a sense of subjects' trust and gather as much comprehensive data as possible.

Measurement

The questionnaire used in this study was developed by combining questions from previous studies that examined cyber security efforts at organizational and national levels. The survey's content and format were also developed based on reviews of existing empirical literature and industry surveys (Abu Musa 2010). In the end, the survey collected detailed information concerning several areas, namely: PPPs; information-sharing across organizations; public agencies' contributions to national cyber defense mechanisms; inter-organizational relationships; democratic values; and demographic information. In addition, it utilized a five-point Likert scale and a Yes/No/Don't Know scale.

To establish validity in terms of data quality and accuracy (Creswell and Clark 2007), a draft of the survey was sent to two Turkish cyber security experts and to three academics. Based on feedback and recommendations from these panelists, the researcher made revisions to the survey to better examine and capture the Turkish context. The survey also included questions from previous research that will be mentioned below. The survey itself was divided into three main sections and employed a total of 78 questions, including 10 demographic questions.

The first section aimed to test the study's principal hypothesis and three sub-hypotheses and collected detailed information about variables (e.g. cooperation among public organizations and private businesses, and national cyber security preparedness) by asking participants 40 questions. The first independent variable, i.e. public- private cooperation, was operationalized by formulating The National Emergency Management Association's (NEMA) 2012 Public-Private Partnership Survey, since it gathered representative and relevant data on collaborative emergency response from 47 states and eight territories across the US. While loosely defining the term emergency to include natural disasters and security threats alike, NEMA's nationwide study gave practitioners invaluable insight into the establishment and function of effective cooperation between the public and private sectors.

To operationalize the dependent variable, i.e. national cyber security preparedness, several previous studies were used. The first study was the 2006 National Computer Security Survey (NCSS) conducted by the RAND organization on behalf of the Bureau of Justice Statistics (BJS), located in the U.S. Department of Justice's (DOJ) Office of Justice Programs (OJP), and the U.S. Department of Homeland Security (DHS). The NCSS gathered data on the nature, extent, and consequences of digital security incidents in the U.S. The survey also collected data on costs these businesses incurred following cyber attacks and digital security measures these companies employed. 36,000 businesses across 36 industry sectors participated in the NCSS, which resulted in a representative nationwide sample that allowed experts to generalize results. The questions contained in the NCSS helped determine what cyber security measures are currently in place and how cyber security incidents are reported to appropriate government agencies.

The second study the researcher used was the Global State of Information Security Survey (2013), conducted by PwC, CIO magazine, and CSO magazine. Although the study demonstrated a certain selection bias (as it surveyed the readership of CIO and CSO magazines and PwC clients from 128 countries), survey co-sponsors still reached a high response rate, with more than 9,300 high executives and information security officers participating. This worldwide study was highly representative of international executives and had a margin of error of less than 1%, thereby making it a solid point of departure for survey design.

The third study was one conducted by Deloitte, a private consulting company, in tandem with the National Association of State Chief Information Officers (NASCIO), a nonprofit association, in order to assist decision makers determine and execute policy in the face of cyber threats. The resulting 2010 Deloitte-NASCIO Cybersecurity Survey was also highly representative, due to the fact that 49 out of 50 US states participated. The items formulated in this survey strengthened the current study's ability to reflect cyber security preparedness from a governance perspective.

The fourth survey to be utilized was a 2012 Federal Cybersecurity Survey conducted by the online journal InformationWeek. This survey examined the extent to which federal agencies have improved their efforts to meet national cyber security objectives. The current study reformulated several items from this 2012 survey, namely those dealing with agencies' barriers to progress, threat perception, and cyber security readiness.

Finally, a 2010 survey conducted by the EastWest Institute, a nonpartisan security think tank, in conjunction with its worldwide cyber-security summit, helped inform other pieces of

content on the present study's questionnaire. Participants of the EastWest Institute's online survey included government officials, business officials, and experts from the U.S., China, Russia, and India. Its focus on their perceptions of cyber threats and those measures that various sectors enacted to secure their assets helped guide the researcher in the creation of his own survey.

The second section of the survey featured 20 questions aimed to measure variables for the second hypothesis, i.e. differences in cyber security preparedness levels between public agencies and private businesses. It did so primarily via a self-assessment checklist. There were also additional questions on cyber security governance that measured the extent to which security practices and business/agency objectives align. Two highly-reliable studies informed the set-up of this particular section. The first was Abu-Musa's (2010) empirical study that implemented a seven-point Likert instrument and a set of simple yes/no questions for ascertaining informational security governance practices at the organizational level in Saudi Arabia. His questionnaire's high alpha score (.88) underscores its overall reliability. Moreover, the study's total accumulated factor analysis variance rate was 81.224 percent. As such, one can conclude that the research instrument Abu Musa used in his study was consistent, reliable, and valid.

The second survey employed in this section was a 2013 PwC State of Cybercrime Survey, developed by CSO magazine, PwC, the U.S. Secret Service, the Federal Bureau of Investigation, and the Software Engineering Institute CERT Program at Carnegie Mellon University. Over 500 US executives and security experts from both the private and public sectors participated in the study and provided researchers raw data on cyber crimes in America and on factors impacting an organization's stance on cyber security. Since this survey focused on

commonalities and differences in public and private organizations' cyber security postures, the researcher was able to use specific questions from it to examine organizational preparedness.

The final section of the questionnaire sought to test the third hypothesis utilizing comparatively fewer questions than in previous sections. Seven questions in this section gathered data on how government officials and private company managers demonstrate their commitments to democratic values. Questionnaire items in this section were mainly adopted from the survey "The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online (2010)," which Dutta prepared as a contribution to the World Economic Forum's annual Global Information Technology Report. This study focused on the core Internet values of freedom of expression, privacy, trust, and security. Using an online survey questionnaire, Dutta's cross-cultural study reached 5,400 adult Internet users in 13 countries.

As we will later see, the response rate for each question varied; as such, the final scales measuring each variable can be found in appendix B.

Control variables

Company size, which is defined as the number of employees; the type of organization; its IT structure; and its location were all used as control variables in the study (Caruson et al. 2012; RAND 2006).

CHAPTER 5

DATA ANALYSIS

This study examines the relationship between public-private cooperation and national cyber security preparedness within the context of Turkey. Taking into consideration the Turkish National Cyber security Strategy Document, this study also observes public and private sector organizations' preparedness levels against cyber threats and the value they attribute to the equilibrium between democracy and security. This chapter presents the results of descriptive, correlation, bivariate, and ordinal logistic regression analyses in three sections. The first section provides information on the procedure of data analysis applied in the study, along with the results of descriptive analyses of both demographic and dependent variables. The next section presents direct correlations between independent and dependent variables. The final section provides the results of an ordinal logistic regression model and t-test results to evaluate the study's proposed hypotheses.

Descriptive Statistics

This section provides a demographic overview of both respondents and the organizations they represent, along with a descriptive analysis of dependent variables, namely national cyber security preparedness, organizational cyber security preparedness, and democratic values.

Descriptive Findings of Demographic Data

The results of a demographic questionnaire demonstrate that among the 115 total participating organizations, 61 (53.04%) were private businesses and 54 (46.96%) were public agencies (see Table 5.1).

Table 5.1. Type of Organization (N=115)

Variables	Frequency	Percent
Public Sector Organizations	64	53.04
Private Sector Organizations	54	46.96

A wide variety of industrial sectors were represented in this study; 25 (%) respondents were IT companies, meaning this sector was particularly well-represented. The governmental sector was also well-represented, with 29 (33%) civilian public institutions, and 10 (11%) security services participating. In addition, there were 7 (8%) banking and financial institutions; 6 (10%) manufacturing companies; 10 (11%) educational institutions (e.g. colleges, universities, etc.); and 4 (5%) energy sector companies. 15 (17%) organizations belonged to other sectors, such as media (2, 2 %), transportation (2, 2%), health (1, 1%), communication (1, 1%), and wholesale/retail (2, 2%) (see Table 5.2).

Table 5.2. Type of Organizational Sector (N=115)

Variables	Frequency	Percent
Government Agencies	29	33.35
Banking/Finance	7	8.05
IT Sector	25	28.75
Security Services	10	11.5
Manufacturing	6	10.35
Energy	4	4.6
Media	2	2.3
Education	10	11.5
Wholesale/Retail	13	14.95
Transportation	2	2.3
Communication	1	1.15
Health	1	1.15
Others	15	17.25

A total of 34 (30.63%) participant organizations were small-sized entities with less than 100 employees; 8 (7.21%) organizations were medium-sized entities with between 100 and 1,000 employees; 23 (20.72%) organizations were large-sized entities with between 1,000 and 5,000 employees; and 46 (41.44%) were very large sized organizations with more than 5,000 employees (see Table 5.3).

Table 5.3. Size of the Organization (N=111)

Variables	Frequency	Percent
Small	34	30.63
Medium	8	7.21
Large	23	20.72
Very Large	46	41.44

Regarding types of organizational IT structure, a total of 50 (45.05 %) participant entities had centralized IT structure; 36 (32.43 %) entities had hybrid IT structure; 8 (7.21 %) entities had decentralized IT structure; and 17 had independent IT structure, meaning they had no separate IT branch or division (see Table 5.4).

Table 5.4. Type of Organizational IT Structure (N=111)

Variables	Frequency	Percent
Centralized	50	45.05
Hybrid	36	32.43
Decentralized	8	7.21
Independent	17	15.32

Organizations were asked to indicate their geographical location, as it was envisaged that this might have an impact on their need for a formal cyber security policy. Turkey is geographically divided into seven regions. However, the study used a separate methodology and treated five of these seven regions (i.e. the Mediterranean region, the Black Sea region, the Southeastern Anatolia region, the Eastern Anatolia region, and the Aegean region) as one unit, "Others." Since the capital is located in Central Anatolia, it is treated as a separate unit. Finally, the Marmara region, being the financial hub and industrial heartland of the country, is accepted as a third unit. A total of 52 (60.22 %) participant entities were located in the Marmara region, 8 (6.96 %) in the Central Anatolia region, and 19 (%) in other regions (see Table 5.5).

Table 5.5. Organizational Location (N=111)

Variables	Frequency	Percent
Marmara Region	63	57.27
Central Anatolia Region	27	24.55
Others	21	18.28

The majority of respondents were either IT directors/managers (CIOs), with a total of 29 (36.13%) participants. This is followed by IT experts, with a total of 25 (22.52%) participants. A total of 11 (9.91%) respondents were CEOs/presidents in their organizations. Moreover, 13 (11.78%) respondents were directors/managers; 6 (5.40) were law enforcement/military officers; 2 (1.80%) were district/deputy governors; 2 (1.80%) were IT security consultants; 1 (0.90%) was a professor; and 20 (18.52%) were holding other positions in their organizations (see Table 5.6).

Table 5.6. Job Title/Function (N=111)

Variables	Frequency	Percent
CEO/President	11	9.91
Deputy President	2	1.80
IT Manager/Director (CIO)	29	36.13
IT Expert	25	22.52
IT Security Consultant	2	1.80
Professor	1	0.90
District/Deputy Governor	2	1.80
Law Enforcement/Military Officer	6	5.40
Manager/Director	13	11.71
Others	20	18.02

Descriptive Statistics of Dependent Variables

On a scale of 1 to 5 (1 = not effective at all, 5 = very effective), the mean national cyber security preparedness rate was 3.56, while the mean organizational preparedness score was 2.99. This shows that participants agree that preparedness at the national level is higher than it is at the organizational level (see Table 5.6), although overall preparedness levels are fairly low. On a scale of 1 to 5 (1 = not agreed at all, 5 = strongly agreed), an analysis of mean democratic values scores shows that it is also moderate, being at 3.55.

Table 4.6 shows that dependent variables' standard deviations are close to each other. Thus, it might be argued that preparedness scores are evenly distributed and that their sample estimates are close to those of the study population. Table 4.6 displays the mean and standard deviation of demographic and dependent variables. (see Table 5.7)

Table 5.7. Dependent Variables (N=111)

Variables	Mean	Std. Dev.	Min	Max
National Cyber Security . Preparedness	3.56	.601	1.83	4.6
Organizational Cyber Security Preparedness	2.99	.589	1.6	5
Democratic Values	3.55	.614	2.16	5

Procedure of Data Analysis

Before employing statistical analysis methods, the researcher screened his collected data for missing values, outliers, and ordinal logistic regression assumptions.

First, the study's target population was all public and private organizations in Turkey that employed IT department to conduct their day-to-day business. The study's sampling frame was provided by the Cyber Security Association of Turkey (CSA), an organization that includes 250 private businesses and 150 public agencies. Of these 400 public and private organizations, a total of 229 began the survey. However, only 148 respondents completed the survey; moreover, STATA 13 (a statistical computer program where responses were entered) performs listwise deletions on data, resulting in altered response rates for each question used in scales. With these considerations in mind, STATA 13 recorded a total response rate of 115 for scales used in this study.

Second, some questions in the second part of the survey instrument had to be recoded in reverse order. Therefore, items 29 and 30 (regarding levels of vulnerability in government and business IT systems stemming from a shortage of qualified IT professionals) and items 31_1 to 31_12 (regarding levels of vulnerability in different sectors in case of coordinated and targeted cyber attacks) were recoded in reverse order.

Third, item 78 (regarding the size of participant organizations) was recoded. Organizations with employees under 100 were recoded as small; organizations with between 100 and 1,000 employees were recoded as medium; organizations with between 1,000 and 5,000 employees were recoded as large; and organizations with more than 5,000 employees were recoded as very large. Additionally, item 77 (regarding participating organizations' physical location) was recoded as three categories: the Central Anatolia region, the Marmara region, and others.

Fourth, there is normally no diagnostic test specifically designed for ordinal logistics models (Long and Freese 2006). However, researchers (Long and Freese 2006; Hoffmann 2004; Osborne 2014) suggest that diagnostic tests designed for binary logistic regression models can be applied to ordinal logistic regression models. In accordance with procedures suggested by Long and Freese (2006) and Osborne (2014), two binary variables (n-1) – one representing medium perceived levels of national cyber security preparedness and one representing high perceived levels – were constructed from the original dependent variable that has three categories: low, medium, and high. Then, two logistic regression models were run with the same independent variables included. For each model, influence and fit statistics were retrieved. Examining the diagnostic statistics and plots led the researcher to detect four outliers which were removed from the analysis in order to make data as clean and representative as possible.

Before running an ordinal logistic regression analysis, it was necessary to alter the main dependent variable of the study, i.e. national cyber security preparedness. To appropriately account for the ordinal nature of the dependent variable in the regression model, it was collapsed into the following three categories: low preparedness, medium preparedness, and high preparedness. The categories were created by taking into consideration the number of participant organizations and dividing the total number into three almost equal groups. (see Table 5.8)

Table 5.8. Categories of National Cybersecurity Preparedness Level (N=115)

Variables	**Frequency**	**Percent**
Low Preparedness Level	52	45.22
Medium Preparedness Level	36	31.30
High Preparedness Level	19	16.52

Multicollinearity was checked to screen for unacceptably high levels of intercorrelation among independent variables through collinearity diagnostics. The mutlicollinearity test indicated that the variance inflation factors (VIF) for all independent variables were much smaller than 10, i.e. they ranged from 1.10 to 1.73 with a mean of 1.2. All 'tolerance' values were also well above 0.1. Therefore, it can be argued that the multicollinearity assumption was not violated by data used in the study.

As a result, all assumptions for conducting a regression analysis were met, and the data were ready to run on an ordinal logistics regression model without further alterations.

Bivariate Analysis

Due to the ordinal nature of the dependent variable, Spearman's rho (ρ) was used to measure the strength of the relationship between dependent and independent variables. The Spearman's rho correlation analysis displayed relationships between dependent and independent variables as ranked values. It is important to note that a newly-created ordered dependent variable was used in this bivariate analysis.

Results from this bivariate correlation analysis between dependent and independent variables are illustrated in Table 5.9.

.

Table 5.9. Correlation Matrix

Variables	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
(1) National C. preparedness	1.0000							
(2) Public Private Cooperation	0.5234**	1.0000						
(3) Institutional effectiveness	0.3429**	0.1795	1.0000					
(4) Democratic values	0.2260*	0.2398*	0.1094	1.0000				
(5) Organizational preparedness	0.2979**	0.2487*	-0.0066	0.0565	1.0000			
(6) Organization type	0.2263*	0.1610	0.0445	0.1683	-0.0344	1.0000		
(7) Organization size	-0.1508	-0.0251	0.0474	0.1062	-0.1485	0.2019*	1.0000	
(8) Organizational location	0.0840	-0.0518	0.0377	0.0155	0.0118	0.3892**	-0.1934	1.0000

* Correlation is significant at the 0.05 alpha level (2-tailed)

** Correlation is significant at the 0.01 alpha level (2-tailed)

According to this bivariate correlations analysis (Table 5.9), there was a statistically significant positive correlation between perceived national cyber security preparedness and four predictor variables: public private cooperation ($\rho = 0.52$, $p < 0.01$), organizational cyber security preparedness ($\rho = 0.30$, $p<0.01$), institutional effectiveness ($\rho = 0.34$, $p<0.01$), and levels of adherence to democratic values ($\rho = 0.23$, $p<0.05$). However, the correlation between perceived national cyber security preparedness and adherence to democratic values was not as strong as the correlation between the other predictor variables and the outcome variable.

In addition, there was a statistically significant positive correlation between public-private cooperation and two other predictor variables; organizational cyber security preparedness ($r=0.2438$, $p<0.01$) and institutional effectiveness ($r=0.198$, $p<0.01$).

A striking finding from the bivariate analysis was a negative correlation (although not statistically significant) between institutional effectiveness and organizational cyber security preparedness ($r=-0.0066$). This finding will be explained in the "Discussion" section so the reader may better understand the results of the ordinal logistic regression model.

Finally, there was a statistically significant positive correlation between perceived national cyber security preparedness and type of organization ($\rho = 0.23$, $p<0.05$), a control variable. There was no statistically significant correlation between the remaining control variables (i.e. organizational IT structure and organizational location) and perceived levels of national cyber security preparedness.

Testing the Parallel Regression Assumption

The ordinal logistic regression model assumes that the distance between each category of the outcome is proportional. Before interpreting the results of the full model, the assumption of proportional odds was examined in order to test whether the proportional odds assumption would hold for the regression model (Long and Freese 2006).

The Brant test for parallel regression assumptions is shown in Table 5.10.

Table 5.10. Brant Test for Parallel Regression Assumptions (N=103)

Variables	**Chi2**	**p>chi2**	**df**
Public-private Cooperation	.10	.753	1
Institutional Effectiveness	1.93	.165	1
Organizational Cyber Security Preparedness	.002	.899	1
Democratic Values	.10	.747	1
Type of Organization	.49	.482	1
All	2.58	.765	5

The Brant test for parallel regression assumptions yielded chi2 = 2.58 and ($p > .765$), indicating that the proportional odds assumptions for the full model were upheld. Examining results for each individual predictor variable and control variable indicated that Brant tests for parallel regression assumptions were upheld for public-private cooperation, institutional effectiveness, organizational cyber security preparedness, adherence to democratic values, and type of organization (see Table 5.10).

Ordinal Logistic Regression

The dependent variable examined in regression analysis was categorical in nature, meaning that it lacked the continuous normal distribution assumed for Ordinary Least Squares regression (OLS). Therefore, the researcher performed an ordinal logistic regression model to appropriately account for the ordered nature of the outcome variable and to examine the effects of selected variables on perceived national cyber security preparedness.

The ordinal logistic regression model was used to examine relationships between perceived national cyber security preparedness, four independent variables, and a control variable, i.e. organization type. Tables 5.11 and 5.12 show the parameters of model-fitting information and pseudo R-squared values.

Table 5.11. Model Fitting Information

Model	Log Likelihood	Chi2	df	p
Intercept Only	-113.089			
Final	-86.252	53.673	5	.000

Table 5.12. Pseudo R-Squared Values

Model	Cox and Snell	Nagelkerka	McKelvey and Zavonia
Pseudo R-Square	.406	.457	.461

The model fitting information illustrated in Tables 5.11 and 5.12 indicate that with a likelihood chi-square ratio of 53.67 and p value of 0.000, the ordered logistic model as a whole was statistically significant ($p < .001$) and exhibited good fitting. According to the pseudo r-

squared values table (see Table 5.12), predictor variables explained between 40.6 % (Cox and Snell R2), and 45.7 % (Nagelkerke R2) of variations in levels of perceived national cyber security preparedness. There was no exact analog for the R-squared found in OLS. However, Long and Freese (2006) argue that McKelvey and Zavoina R2 is the most approximate indicator of the true R-squared of the OLS regression. This value in this study is .461; therefore, predictor variables explain almost 46% of variations in levels of perceived national cyber security preparedness. Based on results from model-fitting, it can be argued that it is unlikely that result are due to chance (Bradbury et al. 2010).

The results of the ordered logit model examining perceived levels of national cyber security preparedness are presented in Table 5.13.

The model's parameters shown in table (Table 5.13) display the effects of each predictor variable on perceived levels of national cyber security preparedness. The results of the ordered logit model indicate that three out of four independent variables made a statistically significant contribution to the overall model.

First, it can be inferred from results that the main independent variable, i.e. public-private cooperation, is statistically significant (p= .000). For a one-unit increase in levels of public-private cooperation, it is more likely to have a 173.3% increase in log odds of being in higher levels of national cyber security preparedness, given that all other variables in the model are constant. Therefore, hypothesis H1 held true.

Table 5.13. Ordinal Logistic Regression Model for Perceived Levels of National Cyber Security Preparedness

					95% Confidence Interval	
	b	**S.E**	**p**	**%StdX**	**Lower Bound**	**Upper Bound**
Variables						
National Cyber Security Preparedness						
Public-private Cooperation	1.99**	0.50	.000	173.3	1.01	2.96
Organizational Cyb. Preparedness	1.03**	0.39	.008	82.7	0.26	1.80
Institutional Effectiveness	0.91**	0.28	.001	113.6	0.36	1.46
Democratic Values	0.37	0.35	.297	25.4	-0.32	1.06
Organizational Type	0.77	0.42	.070	47.0	-0.06	1.60
cut 1 Constant	13.22**	2.43				
cut 2 Constant	15.33**	2.57				

Note: **N** = 103; **b** = unstandardized coefficient; **%StdX**= percent change in the odds for a one standard deviation increase in the independent variable ****p**<0.01, ***p**<0.05

Second, there is also a significant relationship between organizational cyber security preparedness and national cyber security preparedness (p= .008). For a one-unit increase in levels of organizational cyber security preparedness, it is more likely to have an 82.7% increase in log odds of being in higher levels of national cyber security preparedness, given that all other variables in the model are constant. Therefore, hypothesis H1a held true.

Third, institutional effectiveness is also statistically significant (p= .000). For a one-unit increase in levels of institutional effectiveness, it is more likely to have a 113.6% increase in the log odds of being in higher levels of national cyber security preparedness, given that all other variables in the model are constant. Therefore, hypothesis H1b held true.

Fourth, the results of the ordered logit model demonstrate that there is no statistically significant relationship between adherence to democratic values and national cyber security preparedness (p=.397). Therefore, for a one-unit increase in levels of democratic values, there is not likely to be an increase in the log odds of higher levels of national cyber security preparedness, given that all other variables in the model are constant. Therefore, hypothesis 1c was rejected.

Finally, it is necessary to mention that since correlations between control variables (i.e. organizational size, IT structure, and location) and the outcome variable were not found to be statistically significant, for the sake of model parsimony, they were not included in the regression model. However, the bivariate analysis showed that there was a statistically significant positive correlation between national cyber security preparedness and types of organizations, the remaining control variable ($\rho = 0.23$, $p<0.05$); thus, this correlation was included in the full regression model. Table 4.12 indicates that compared to private organizations, public organizations are not likely to demonstrate increases in log odds of higher levels of national cyber security preparedness, accepting that all other variables are constant (p=.70).

T-test result for H2

An independent t-test was run on a sample of 103 representatives of public and private organizations to determine if there were differences in levels of importance attributed to democratic values based on their respective organizational types. The mean level of importance demonstrated by public sector representatives (3.64, SD=.08) is higher than the mean demonstrated by private sector representatives (3.46, SD=.08). However, the results show that the former did not have attribute statistically higher importance to democratic gains than the latter. The t-statistics is -1.48 with 103 degrees of freedom and the corresponding one tailed p value is .07, which is higher than .05. (see Table 5.14). Therefore, hypothesis H2 is rejected.

Table 5.14.T-test for Democratic Values (N=103)

Variables	**Mean**	**Standard Deviation**
Public Organizations	3.64	.08
Private organizations	3.36	.08

t= -1.48 **df**= 103 **p=.**07

T-test result for H3

An independent t-test was run on a sample of 109 public and private organizations to determine if levels of organizational cyber security preparedness is higher in public organizations or in private organizations. The mean level of preparedness for the public sector (.74, SD=.06) is higher than that for the private sector (.55, SD=.07). However, these results show that public sector organizations do not exhibit statistically significant higher cyber security preparedness than private sector organizations. The t-statistics is 2.1 with 109 degrees of freedom and the

corresponding one tailed p value is .04, which is higher than .05. (see Table 5.15). Therefore, hypothesis H3 is rejected.

Table 5.15. T-test for Organizational Cyber Security Preparedness (N=109)

Variables	**Mean**	**Standard Deviation**
Public Organizations	.74	.06
Private organizations	.55	.07

t= 2.1 **df=** 109 **p=.**04

CHAPTER 6

DISCUSSION AND CONCLUSIONS

Introduction

This study sought to observe the relationship between public-private cooperation and national cyber security preparedness. More specifically, it focused on how government bodies responsible for securing the cyber domain should organize themselves and cooperate with the private sector, which owns a considerable portion (e.g. in some countries, up to 80%) of critical infrastructure that needs to be defended against cyber threats. This research primarily treated this question as a governance concern, using the Turkish National Cyber Security Strategy Document as a point of departure. The study also examined differences in organizations' levels of cyber security preparedness and values attributed to the equilibrium between democracy and security at the organizational level.

Summary of Findings

This study used an ordinal logistic regression model to examine which factors – including independent variables (i.e. public-private cooperation, organizational preparedness, institutional effectiveness, and democratic values) and a demographic variable (i.e. type of organization) – contribute the most to national cybersecurity preparedness. Regression analysis revealed that:

- Three variables significantly influenced preparedness: public-private cooperation, institutional effectiveness, and organizational preparedness.

- Among these three variables, the main independent variable (i.e. public-private cooperation) was the strongest predictor for perceived national cybersecurity preparedness.

- Only democratic values had no impact on the level of perceived national cyber security preparedness.

- The demographic variable (i.e. organization type) had no impact on the level of perceived national cyber security preparedness.

Overall, the study's five-variable model (i.e. four independent variables and one demographic variable) proved to be statistically significant and can thus be expected to explain almost 46% of variations in levels of perceived national cyber security preparedness (McKelvey and Zavoina R2).

Moreover, a bivariate analysis of findings determined that:

- Although it is not statistically significant, there is still a negative correlation between institutional effectiveness and organizational cybersecurity preparedness.

The study also observed 1) differences in levels of value attributed to democratic gains based on organization types and 2) varying levels of organizational cyber security between private and public organizations. Following an independent t-test, it was established that:

- The value which private sector participants attributed to democratic gains was not, from a statistical point of view, significantly higher than that of public sector participants.

- Public sector organizations' cyber security preparedness levels were not, from a statistical point of view, significantly higher than those of private sector organizations.

Discussion of Findings

Before further discussing the findings of this study, the author would like to remind readers of those hypotheses the study aimed to test:

Hypothesis 1. Cooperation between public institutions and private companies increases cyber security preparedness.

1a. Organizational Preparedness is more likely to increase national cyber security preparedness.

1b. Institutional effectiveness is more likely to increases national cyber security preparedness.

1c. The importance attributed to the democratic values is more likely to increase national cyber security preparedness.

Hypothesis 2. Cyber-security threats preparedness is higher in government agencies than in private sector.

Hypothesis 3. Government officials will present a higher level of democratic values in cyber domain than will private sector managers.

Hypothesis 1

While determining the validity of Hypothesis 1, the study established a significant (positive) correlation between the presence of public-private cooperation and levels of national cyber security preparedness. Previous literature supports this finding (Hare 2009; Choo 2011b; Klimburg 2012; Senturk et al. 2012). For instance, Mueller and Kuehn (2013) examine the US

federal government's cyber security monitoring program called Einstein. At the beginning, this US-CERT-led program was designed to improve network monitoring and incident-response capabilities in the federal government's civilian agencies. Subsequently, however, both the number of participating agencies and their spectrum of technical capabilities increased. Moreover, project partners working in the government's Defense Industrial Base (DIB) eventually grew to include private firms. As a result, the US-CERT was able to protect against cyber incidents by including private organizations in its security umbrella, by utilizing federal agencies and department networks, and by establishing centralized control over the cyber realm

This present study supports Mueller and Kuehn's findings within the Turkish context, i.e. a government must go beyond its own infrastructure and cooperate with the private sector to provide its citizens with cyber security.

In parallel with findings from the present study, Senturk et al. (2012) provide a 2009 ICTA collaborative project in Turkey as an example of cooperation among public and private organizations. The ICTA aimed to reduce the amount of spam emails through engaging both public and private institutions in its work. At the end of the project, the number of spam emails transmitted per day declined from 6,5 billion to 394 million. These results thus support Hypothesis 1 in the Turkish context and hint that this form of cooperation is likely to increase levels of national cyber security preparedness.

Literature on cyber security is still in its nascent stages and is therefore still limited in scope. For that reason, the current explanatory study wishes to focus on earlier studies with comparable findings, i.e. that public-private cooperation contributes to national cyber security

preparedness. The author, then, will discuss two previous studies to see how their results support his conclusions about Hypothesis 1 and to show that using cooperation to enhance the private sector's security role is likely to increase a nation's cyber power.

The current study's author uses the term cyber power in his conceptualization of his outcome variable (i.e. national cyber security preparedness). A study by Booz Allen Hamilton and the Economist Intelligence group developed a cyber power index that measures a country's ability to withstand a cyber attack and deploy digital infrastructure essential for economic security. According to their index, the UK (1), the US (2), Australia (3), and Germany (4) are at the forefront of digital security, having scored 76.8, 75.4, 71.0, and 68.2 respectively. Two other world powers, China (13) and Russia (14), scored significantly lower, i.e. 34.6 and 31.7. Following Russia, Turkey placed 15th with a score of 30.4. If the author's hypothesis is correct, then, countries with higher cyber power indices will exhibit increased amounts of private sector participation in their cyber defense strategies.

The second study by The Privacy and Cyber Crime Institute, on the other hand, compares key features of 14 countries' national cyber security strategies. One key characteristic examined in this case study is the private sector's involvement in national cyber security efforts. It used three ratings – minimal, modest, and significant – to define levels of private sector involvement in targeted countries' national cyber security strategies. When one places findings from both studies side by side, one finds that countries with the highest cyber power indices (i.e. the UK, the US, and Australia) also have the highest levels of cyber security contributions from the private sector. While Germany had only modest levels of participation from the private sector, the Booz Allen study mentioned that its cyber power depends on its comprehensive national

cyber plan that prioritizes a legal, regulatory framework based on coercion rather than cooperation. On the other hand, whereas Russia has minimal contributions from the private sector, China exhibits modest levels of contribution (Levin et al 2012). While this second study did not analyze Turkey, its National Cyber Security Document makes limited references to the role of the private sector, i.e. only in terms of its ownership of critical infrastructure. It can thus be said that Turkey has minimal cyber security contributions from the private sector.

These two studies reveal that the larger the role that the state provides to the private sector in maintaining cyber security via cooperative mechanisms, the more cyber power it wields (see Table 6.1). In other words, these previous findings support the author's first hypothesis that public-private cooperation is likely to enhance national cyber security preparedness.

Table 6.1.Cyber power and Private sector Role

Cyber power index Country	**Ranking**	**Score**	**Private sector role in national cybersecurity**
United Kingdom	1	76.8	Significant
United States	2	75.4	Significant
Australia	3	71.0	Significant
Germany	4	68.4	Modest
China	13	34.6	Modest
Russia	14	31.7	Minimal
Turkey	15	30.4	----

While determining the validity of Hypothesis 1a, the present study found that there is a significant (positive) correlation between organizational cyber security preparedness and national cyber security preparedness. This result is expected and supported by current literature (Hare 2009; Choo 2011b), yet there is one specific case study that is worthy of detailed discussion. In 2010, the US Department of Defense (DOD) launched its Defense Industrial Base Cyber Pilot

Program, in which the government shared with private businesses classified intelligence about cyber threats in order to enable them to strengthen their own networks. By providing intelligence directly to the private sector, this pilot project not only helped private businesses prevent hundreds of cyber intrusions, but also revealed that cooperation among parties enhanced US national cyber security by specifically protecting sensitive DOD content in the possession of partnering corporations (Mueller and Kuehn 2013). Even if the DOD is capable of protecting sensitive information, overall national security requires involvement from outside actors. As such, this real-life example corroborates Hypothesis 1a.

For Hypothesis 1b, the present study found a significant (positive) correlation between institutional effectiveness (i.e. institutional capacity to assume roles in cyber defense) and national cyber security preparedness. Existing scholarship corroborates this result. Although states are increasingly adopting national cyber security strategies that task government agencies and departments with enhancing levels of cyber security preparedness (Hathaway and Klimburg 2013; Klimburg and Mirti 2012), their ultimate success on the ground depends on the extent to which they can cooperate with public and private organizations. Government agencies need to effectively engage in preparedness activities together with the private sector to withstand and recover from accidental and/or deliberate attacks with possible negative effects on a global scale (Sommer and Brown 2011). The extent to which they can achieve this depends on their effectiveness in aligning private and public organizational strategies with national security strategies. This link lies at the heart of Hypothesis 1b.

As previously mentioned, during a bivariate analysis, a negative correlation (although not a significant one) was found between institutional effectiveness and organizational cyber

security preparedness. This finding seems to contradict the positive correlation between institutional effectiveness and national cyber security preparedness; after all, the current study views national cyber security preparedness as the sum of organizational preparedness. To fully explain these findings, then, the author will establish the relationship between these two predictor variables (i.e. organizational cyber security preparedness and institutional effectiveness). First, he will discuss why levels of government effectiveness have such low impact on public organizations and their levels of cyber security preparedness in Turkey; then, he will discuss the same issue regarding levels of cyber security preparedness in the private sector. It should become clear at the end of his analyses that the reason behind this contradiction and negative correlation is the overall state of institutional effectiveness in Turkey.

Low Governance Impact on the Public Sector

In Turkey, the Information and Communications Technologies Authority (ICTA), which is affiliated with the Ministry of Interior, serves as the main governmental authority for regulating and controlling the electronic and communications sector. Among its other tasks, the ICTA coordinates and ensures the continuity of electronic communications (Gurkaynak et al. 2014). This sectorial body is also responsible for cyber security, informational security, and data privacy regulations in Turkey. Whereas the Ministry of Transportation, Maritime Affairs and Maritime Affairs is responsible for policy making in the communication sector, regulation power is given to the ICTA (Gurkaynak et al. 2013).

However, although regulatory agencies are well positioned to assume responsibility over large parts of ICT infrastructure, the policies these agencies develop face the risk of being

ineffective against cyber threats. Cyber security governance at the national level entails more than regulating the information and communications sector. It also involves establishing channels of communication with organizations representing law enforcement, the judiciary, intelligence bodies, and the private sector. If tasked with enhancing cyber security, these regulatory agencies will be under pressure to develop capacity stimulating cooperation among public and private actors on issues that are generally beyond their scope (Bauer and Eeten 2009). An indicator of such agencies' effectiveness, then, is their ability to develop dialogue and action on policies touching on spheres outside their mandates, an ability which is rarely encountered.

Due to such organizational challenges and the growing number and variety of cyber threats, the Turkish government took further steps to maintain cyber security by establishing a Cyber Security Board (Gurkaynak et al. 2014). Turkey's Cyber Security Board is authorized to set procedures for cyber security, facilitate coordination among relevant stakeholders, and approve and enact Turkey's national cyber security strategy (Gurkaynak et al. 2014; Gurkaynak et al. 2013). The National Cyber Security Strategy and Action Plan for 2013-2014, published in accordance with a 2012 Cabinet Decision, states that the Cyber Security Board is authorized to maintain the security of critical infrastructure owned by both the public and the private sectors (Gurkaynak et al. 2013). The Cyber Security Board, chaired by the undersecretary of the Ministry of Transportation, Maritime Affairs, and Communication, is comprised of such entities as the Ministry of Foreign Affairs, the Ministry of National Defense, the National Intelligence Agency, the Information and Communication Technologies Authority, and the Telecommunications and Communication Authority. The military is also represented by the head of the Turkish General Staff's Communication, Electronic and Information Systems bureau. All

participating ministries and bodies are represented at the highest official level in the Cyber Security Board.

The establishment of a National Cyber Security Board can be seen as a response to the security aspects of the cyber governance problem (Gurkaynak et al. 2014). However, organizational changes in the realm of cyber security have not fully followed the pattern observed in other countries, where leading agencies already have security backgrounds. In one case study, the Rand Corporation (2013) compares leading cyber security bodies in 10 countries (including the US, the UK, France, and Germany) and their respective responsibilities and scopes. It also examines the role law enforcement agencies play in countries' overall strategies. According to research findings, countries generally prefer inter-departmental models for ensuring cyber security. These models often maintain existing 'real world' remits in the cyber domain. For example, while law enforcement agencies investigate cyber crimes, security services seek to mitigate cyber espionage. Countries in the case study allocated principal leadership roles to coordinating bodies that unite agencies and facilitate collective responses, thereby reducing conflicts concerning overlapping jurisdictions and purviews. In some countries (e.g. Estonia and France), the coordinating body is a newly-established entity; in others (e.g. the UK and Canada), this role is assumed by existing governmental departments. Between countries, there is often little consistency in terms of what department takes the lead for establishing and implementing official cyber security policy, and head organs run the gamut from cabinet offices and interior ministries to defense and/or national security directorates. In the Turkish context, the structure of the National Cyber Security Board is unique in that it is led by the Ministry of Transportation,

Maritime Affairs and Communications, an entity that has not previously played a role in national security.

As previously mentioned, the negative correlation between institutional effectiveness and public organizations' preparedness levels can be found in faulty governance structures. While searching for the causes of such faulty structures, the author of the present study highlighted three possibilities, two of which stem from the National Cyber Security Board's structure itself, another of which stems from task delineation within the Board. The first structural issue is that while the responsibilities of the Ministry of Transportation, Maritime Affairs and Communication (i.e. the leading body in the National Cyber Security Board) are great in cyber security, the authority it can exercise in practice is very limited. Specifically, it does not occupy a higher position in government agencies' hierarchy than other groups participating in the Board, and it is the Turkish Constitution which establishes this framework. Therefore, from a constitutional point of view, it is unclear how much authority the Ministry of Transportation, Maritime Affairs has to enforce security standards, since it is not technically endowed with more authority than its organizational peers. Nielsen (2012) defines such mismatches in cyber security governance as an organizational challenge and argues that it is difficult to execute a whole-of-government approach to cyber security in the absence of centralized direction and control. The same issue holds true in the US context, as a 2009 GAO report demonstrates. It states that the White House (as opposed to other federal agencies) must assume a leadership role in order to establish a streamlined chain of command between authority bodies and implementing bodies. As a result, it can be argued that the structure of the Turkish National Cyber Security Board falls short of centralization and a genuine top-down authority structure. With a strong body in charge,

one of the main organizational challenges to cyber security will be solved, and capabilities and responsibilities across a broad spectrum of government organizations will be aligned.

To further illustrate this point, May and Koski (2013, 142) point out that centralized authority must resolve the problem of overlapping mandates and responsibilities in multi-agency structures. Otherwise, the problem of shared mandates and horizontal hierarchies impede government efforts to address public risks, including cyber threats. Moreover, exacerbating the problem, high-ranking government officials have incentives to preserve their organizations' autonomy, protect their areas of influence, and avoid cooperation in multi-agency structures (Wilson 2000; Klimburg and Mirti 2012). At present, the Turkish administrative system does not grant the Ministry of Transportation, Maritime Affairs the necessary authority to re-establish organizational mandates and solve potential quarrels. As a result, the lack of clearly-defined responsibilities across organizations compromises holistic cyber security governance.

The second structural issue is that the National Cyber Security Board is not compatible to address the question of speed in the cyber domain. Rosenzweig (2010) explains that the speed at which events transpire in the cyber realm is one of its unique features. When a cyber-attack happens over the span of milliseconds, preventative and/or defensive responses must occur within the same span of time. Therefore, in order for organizations to rapidly respond to cyber threats, their structures must account for this aspect of the cyber domain. In the Turkish context, all Ministries and government agencies participating in the National Cyber Security Board are represented at the highest levels. Individuals sitting on this Board are responsible for managing their own organizations outside of the Board's functions. Although the Board was established to enhance the effectiveness of the decision-making process, it is unable to simultaneously

communicate with all high-level officials in situations where rapid responses are crucial. Consequently, Turkish efforts at cyber security lag behind.

The third issue concerns the delineation of responsibilities amongst participating organizations. Namely, those organizations which play the most crucial roles at the heart of the Board (e.g. the Ministry of Transportation, Maritime Affairs, ICTA, and the Presidency of Telecommunication and Communication (PTC)) exhibit more technical than security capacities. As Nielsen (2012) rightfully explains, "technical challenges – as significant as they may be – will probably not be as difficult to overcome as those that are nontechnical in nature" (350). In the Turkish context, important non-technical issues such as law enforcement, judicial concerns, and intelligence gathering are not given their due priority, since the Ministry of Transportation, Maritime Affairs lacks experience and a mandate in these areas. As a result, "government organizations that have…(the necessary) organizational structure, skills, knowledge, (and) relationships within the government and with the private sector" (Kelly and Hunker, 2012, 219) end up playing secondary roles, which negatively affects the implementation of national cybersecurity policy.

The National Cyber Security Strategy and 2013-2014 Action Plan also identifies implementation problems stemming from the Board's structure and responsibility delineation, thereby supporting key findings of this current study. Namely, the plan highlighted how:

1. Implementing organizations lack coordination.

2. Besides lacking a solid structure, public organizations view cyber security as a concern for IT departments only.

To conclude, the current assignment of responsibilities among public agencies is based on technical aspects of cyber security governance. Government bodies with highly sophisticated technical capacities (instead of security capacities) assumed the central roles in the National Cyber Security Board, which has impeded national cyber security efforts. Observing the security situation from a limited perspective will result in negative repercussions within government organizations and will decrease the importance attributed to security-related problems. A centralizing authority at the heart of the Board which would re-distribute roles to implementing bodies is likely to transform the current negative correlation between institutional effectiveness and organizational preparedness to a positive correlation. Government agencies would thus be forced to enhance their preparedness levels and to proactively respond to cyber threats. In the following section, the same concern – with a similar solution – will be discussed from the point of view of the private sector.

Low Governance Impact on the Private Sector

It was expected that the effectiveness of government agencies responsible for securing Turkish cyber space would be positively correlated with private sector organizations' cyber security preparedness, as that constitutes one of the most critical facets f national cyber security preparedness. However, the present study found that while increasing national cyber security preparedness is possible through increasing the effectiveness of relevant government agencies and departments, their influence on private businesses' cyber security preparedness is very limited. What follows is a list of possible explanations for this phenomenon.

First, Kelly and Hunker (2012, 226) argue that "in private sector-related cyber security policy, there is a fundamental mismatch between articulated goals and the authorities, resources, and capabilities of the government to meet them." Adjusting this mismatch is a governance concern, since without a government agency in charge of interacting with the private sector and involving it national cyber security efforts, it will neither invest in new cyber technologies nor engage with the government on sensitive issues such as information sharing and/or PPPs. Coldebella and White (2010) also highlight this governance issue and argue that agencies in positions of leadership need to have statutory authority to cooperate with the private sector on cyber threats. In Turkey, even though the ICTA and PTC have regulative authorities in their respective sectors (i.e. the electronics/communications sector and the informational technologies sector), they hold no authority over other sectors or agencies managing those sectors (e.g. energy and the Department of Energy, Gurkaynak et al. 2014). This causes a mismatch in terms of these regulative agencies' organizational capacities and sectorial cyber security goals, decreasing their effect on private entities in sectors they do not directly control.

As an elaboration to this point, there are several areas where such organizational mismatches prevail in cyber security governance in the Turkish context. First and foremost, as demonstrated above, government agencies with leading roles have more technical capacities than security mandates, which complicates efforts to reach out to the private sector. After all, agencies with high capacities are not necessarily able to bolster efforts in fields directly relating to security. To solve this mismatch, leading organizations should be mandated to help private organizations build capacity for preventing, mitigating, and recovering from cyber attacks, which increasingly have physical consequences (Thomas 2013). Such mandates must focus on security,

and in the Turkish context, such a primary mandate can be assumed by the Ministry of Interior and the Ministry of Defense, rather than by the Ministry of Transportation, Maritime Affairs, at the ministerial level. In addition, the Ministry of Transportation, Maritime Affairs, the Cyber Security Board, the PTC, and the ICTA do not have already-established security partnerships with private organizations, and in the absence of such partnerships, such bodies lack full capacity to cooperate with the private sector. These partnerships have proved to be important in the American context as well. For example, Koski (2011) argues that to a large extent, the DHS has been successful in instilling a sense of commitment among partners to protect critical infrastructure precisely because engaged sectors executed such work under previous frameworks. As a result, the Ministry of Interior would be better placed to handle this work in the Turkish context because of its previous experience in cooperating with the private sector on security.

The second possible explanation for this phenomenon is that the current Turkish inter-departmental security model falls short of creating a cooperative national framework where private businesses are incentivized to contribute to national security through enhancing their own cybersecurity systems (May and Koski 2013, 142). Although government agencies function in an environment where their abilities are too constrained to affect the private sector via economic means, they should still have the organizational capacity to influence the private sector through regulatory means. Therefore, government agencies must be able to remove potential pitfalls in relationships with other agencies and create a positive environment where private organizations receive more rewards for government cooperation than costs. Otherwise, if cooperation does not offer incentives to private organizations, a dysfunctional relationship lacking in commitment and

proactive behavior on the part of the private sector could result (Clinton 2011), thereby exacerbating existing gaps and creating new gaps in cyber governance.

Thirdly, Stavridis and Farkas (2012) argue that the main governance problem is related to mindset, especially the public sector's mindset. According to the authors, government agencies must overcome their institutional mindsets that view national security as a good solely provided by the government and actively encourage officials at all levels to work with the private sector. This task is all the more challenging in the Turkish context, where civil actors, whom the nation's military founders generally distrust (Ozbudun 2011; Grigoriadis 2014), have not been able to play a significant role in providing national security. As a result, national cyber security governance is impeded. To move beyond this state of affairs, there is a need for Turkish public government agencies to be more change-oriented and involved with their partners in the private sector in order to ensure security across multiple levels.

Overall, the present study shows how, despite current governance problems, public-private cooperation is likely to enhance national cyber security preparedness in Turkey. The aforementioned explanations regarding government agencies' low effectiveness at positively influencing private and public organizations' preparedness levels reveal that the negative correlation between organizational preparedness and institutional effectiveness does not contradict the full logistic regression model mentioned in the analysis. With an appropriate governance model designed for cyber space, private-public cooperation would likely have a higher impact on national preparedness levels than it does now. The following question can subsequently arise: despite current governance failures, why is there a positive correlation between institutional effectiveness and national cyber security preparedness? The answer is that

the government's penetration into cyber domain is still in its infancy, and since the cyber domain was not previously regulated, every positive governance measure to secure it counts. Through this prism, current levels of institutional effectiveness in Turkey can be explained.

This present study focused, among other things, on whether or not concerns regarding democratic rights are considered in national cyber security policy in Turkey. In Hypothesis 1c, a significant (positive) correlation was not found between public democratic values and national cyber security preparedness. In literature, however, there is a growing consensus that government measures to maintain national security (including law enforcement and targeted cyber surveillance) do not harm online freedoms such as privacy, free flow of information, and the right to express ideas anonymously (Aquilina 2013; Deibert and Rohozinski 2010; Nojeim 2010; Hill 2012). Despite what literature states, concerns regarding democratic values are not likely to significantly affect national cyber security preparedness in the Turkish context. There are several explanations for this finding.

First, while Turkish society has become much more democratic since the mid-1980s, Seckinelgin (2004, 176) argues that its responsiveness to "the changing nature of the deepening democracy" is still low. As a result, democratization and the fruits it bears are limited. Although the social contract between the state and its populace lets groups become involved in political issues such as advocating for new laws or promoting a more open society, the state does not want civil society to exceed certain boundaries on issues regarding democratic demands. According to a 2013 index by Civicus that measures the state of civil society worldwide, Turkish civil society has been gaining strength in its contributions to democracy and open society. However, its power to establish checks and balances on the state's erosion of democratic values in favor of security is

not as strong as it is in developed countries. For example, privacy protection has become the most enduring social issue in developed world (Nissenbaum 2004) because private information gathered either by private companies or by public agencies is being monitored and investigated by governments (Solove 2006). However, Turkey does not have a privacy law, and this issue still is not high on the national agenda. This shows that although democratization is progressing in Turkey, its institutionalization still confers limited power to the people. This situation has inevitable repercussions in the formulization of cyber security governance, weakening the determining role democratic values play in establishing a cyber security framework.

Second, Turkish society at large has not established a link between online democratic values and cyber security governance. The number of Turkish Internet users reached 35 million in 2011. With 45% of the Turkish population on the Internet (Internet World Stats, 2011), Turkey has the fifth largest Internet penetration rate in Europe and a dynamic segment of the population active in cyber socialization (Alikilic and Atabek 2012). Moreover, Turkish Internet users are the most engaged social media consumers in Europe, constituting the third largest Facebook population in the world (Comscore 2009). It would seem logical that given the Turkish populace's high technology use and cyber-connectedness, it would play a more crucial role in governance processes, especially as the Internet becomes increasingly regulated. In reality, it is not interested in how the cyber domain is regulated. Moreover, although figures on Internet usage reflect a highly dynamic cyber society, current legislation enables Turkish courts to ban access to websites, and the European Court of Human Rights even ruled that the Turkish government violated human rights when it completely banned access to YouTube in the country from March 2007 to October 2010 (CFR 2012). Despite high levels of Internet activity from the

part of the Turkish populace, it is limited in its abilities to influence government agencies' cyber regulations and promote democratic means of governance.

Rogers and his innovation diffusion theory (2003) help put this in perspective by explaining how an innovation (i.e. either an idea or a product) spreads among members of a social system. A successful diffusion means that people adopt the new innovation as part of their social system. However, since people's willingness to adopt innovations varies, they will not appear in all segments of a population simultaneously. Rogers defines five established categories of people who adopt innovations: innovators, early adopters, the early majority, the late majority, and laggards. Whereas early adopters are people who are venturesome and want to be first to try an innovation, laggards can be characterized as conservative, risk averting, and skeptical of change. When we look at the diffusion of communication technologies and the Internet in the Turkish context, it can be argued that Turks are quick to grasp onto new technology, i.e. they are early adopters. However, the speed at which Turkish society adopts values that normally accompany these technologies (such as privacy and freedom of expression) is slow. Therefore, it can be argued that whereas Turks are early adopters when it comes to embracing products, they are generally laggards when it comes to embracing values. The divide between technology adaptation and value adaptation in Turkish society may be one of the reasons why people do not question government measures that may have the potential to affect values associated with new technologies.

Hypothesis 2

Turkey is currently implementing its 2013-14 Action Plan that aims to enhance cyber security preparedness in public agencies and departments. However, despite what the Plan envisions, for hypothesis 2, a t-test which the present study used found there to be no significant differences between public and private organizations' levels of cyber security preparedness. This result contradicts existing literature. Smith et al. (2010), for example, argue that if there is a security measure issued from higher authorities, all government agencies are to comply with this national de jure mandate. Its implementation, though, may change according to the sizes and resources of involved agencies, as well as the structural, cultural, and strategic differences between them (Weill and Ross 2005). The private sector, on the other hand, is inclined to see cyber security as a public good that must be provided by the state, since protecting the nation is an inherently governmental function. This causes an externality in the market that reduces action from the private sector and increases its reliance on the public sector (Coyne and Leeson 2008; Bauer and vanEeten 2009; Acemoglu et al. 2013; Murray 2007). This situation is exacerbated by the fact that private businesses do not invest in essential cyber defense measures because such investments are expensive (Hattaway and Klimburg 2012) and do not sufficiently share information on threats (Kesan and Hayes 2011). The study will thus explain possible reasons as to why public sector readiness in Turkey is not higher than private sector with respect to cyber security preparedness.

Unpreparedness in most Turkish public organizations is probably caused by the same aforementioned governance problems that impede national cyber security preparedness. Additionally, the current legislative process in Turkey has been very slow to pass laws that

would help public organizations boost their preparedness. Although the deadline for legislative amendments on cyber security was September 2013, as of yet, no major steps have been taken to fully prepare Turkish public organizations against cyber threats (Gurkaynak 2013). Moreover, Quigley et al. (2013) argue that decision-makers in public sector organizations are reactive and are largely concerned with complying to existing cyber security measures rather than adopting new measures (Johnston and Hale 2009). This delay may send the wrong signals to high-ranking executives in government agencies and divert them from ensuring organizational preparedness, which, in theory, should be their priority.

Organizational governance failures may also negatively affect organizational preparedness levels in Turkey. Weak governance caused by ill-defined roles, responsibilities, and processes generally result in poor decisions regarding organizational information security. Furthermore, organizational managers who are unaware of the importance of securing their information assets exacerbate governance problems in organizations (von Solms 2005). Caruson et al. (2012, 4) argue that government agencies' unpreparedness for growing cyber threats may be attributed to the prevalent belief among non-IT public officials that "cybersecurity is the sole responsibility of IT technicians" and not a jurisdiction-wide responsibility. Moreover, while Werlinger et al (2010) give reasons for low levels of organizational preparedness, they highlight IT experts' lack of adequate knowledge about cyber security. They argue that organizations with weak security governance systems fall victim to problems caused by systemic control gaps and vulnerabilities (Julisch 2013; Brechbühl et al. 2010). The 2013-2014 Action plan also cites roadblocks hampering Turkish government agencies' cybersecurity preparedness, namely:

- Public organizations lack sufficient infrastructure to manage informational security;
- Public organizations lack sufficient knowledge and awareness about cyber security; and
- Executives in public organizations lack sufficient interest in cyber security (13).

Since securing an organization's informational assets is a direct governance concern, any deficiencies in its governance will ultimately result in lower levels of preparedness.

It is worth mentioning two additional phenomena that may help understand current low levels of preparedness in Turkish private sector organizations, especially as the country's current transitional period in terms of cyber security preparation also affects private organizations (Gurkaynak 2013; Gurkaynak 2014). First, we have to look at how Turkish private organizations adopt new laws and regulations enacted by government agencies; a brief analysis of the Finnish context will guide us. In his 2014 study examining the awareness and willingness of Finnish private organizations to comply with a proposed cyber privacy law, Mikkonen separates organizations into three different groups according to their eagerness to comply with legislation. The study identified groups based on Rogers' adopter categories (2003), likening groups' responsiveness to new legislation to responsiveness to innovation and values.

The first group is "adopters," i.e. private organizations that are aware of forthcoming regulatory reform and are willing to take immediate actions following the passage of proposed legislation. With privacy as the issue at hand, they are typically companies that use and appreciate the value of consumer data and thus pay attention to how it is processed. Many of

these companies have already established privacy programs, with relevant processes and documentation in place. The second group is called "followers." Although companies in this group are somewhat aware of impending reforms, they are not eager to take any actions immediately. However, the fact that these companies are not taking any actions at the given moment does not mean that they are not likely to act all. They will comply with legislation when its implementation becomes more widespread. The third group, on the other hand, is called "laggards," and they are neither aware of the reform, nor are they eager to take any action whatsoever regarding regulatory compliance. Although these organizations process personal data in their daily businesses, they seem unlikely to proceed towards voluntary regulatory compliance, since they lack an understanding about the value of preserving the confidential nature of consumer data in digital domain.

The results of the study indicate that a minority of private organizations in Finland is adopters, the majority being laggards that are not going to take any immediate actions. Mikkonen argues that his findings corroborate results from other European countries, such as the UK, where companies are quite unfamiliar with impending reforms. Therefore, it can be argued that Turkish private companies are following the pattern in Europe and are thus generally laggards when it comes to taking necessary steps in enhancing cyber security in parallel with the Action Plan. In statistical analysis, the mean scores for organizational preparedness in both the Turkish private and public sectors tend to be low, which may explain why the majority of organizations is laggards.

Besides Mikkonen's study, another explanation for low levels of private sector preparedness might be related to private businesses' capacities for innovation. Cyber threats are

increasingly depriving private businesses of intellectual property that they have devoted resources to develop and require nothing but an Internet connection to access this property and transfer it illegally. This ultimately shifts the market advantage from companies spending resources on research and development to others that mainly lack innovative capabilities, because instead of spending resources on research and development, they can conduct business by obtaining and transferring knowledge illegally. For that reason, organizations that produce knowledge will be more aware of protecting themselves against adversaries in cyber space and of enhancing their organizational cyber security preparedness. Similarly, organizations with low innovative capacities may not need to protect their data as much as their competitors. To support this explanation, the author of the present study used the 2013 Global innovation Index to compare the countries he previously analyzed for their respective cyber power indices (i.e. the US, the UK, Germany, China, Australia, and Russia). As it turned out, countries with higher innovation scores were also the same countries with higher cyber power scores. The UK came third in the overall ranking, with a score of 61.2, while the US ranked fifth, with a score of 60.3. Germany (15) and Australia (19) came in slightly lower, scoring 55.8 and 53.1, respectively. China and Russia, however, countries with lower cyber power rankings (i.e. 13 and 14 respectively), also received lower innovation scores, with China (35) coming in at 44.7 and Russia (62) at 37.2. Finally, Turkey ranked 68, with a score of 36.0. (see Table 6.2). This table includes Switzerland, the highest-ranked nation, as a benchmark to facilitate comparison across countries.

Table 6.2. Global Innovation Average Scores

Country	Ranking	Score
Switzerland	1	66.6
United Kingdom	3	61.2
United States	5	60.3
Germany	15	55.8
Australia	19	53.1
China	35	44.7
Russia	62	37.2
Turkey	68	36.0

Taking into consideration two previous studies (i.e. Booz Allen Hamilton and The Privacy and Cyber Crime Institute) and the 2013 Global Innovation Index, it can be argued that the more innovative capacity a country has, the more cyber power and private sector involvement in cyber security it has to protect its assets against cyber threats. Put more concisely, countries with high levels of innovation have a greater amount of material they need to protect. Therefore, the Turkish private sector with its limited innovative capacity is less prepared against cyber threats than innovative businesses, because the former need preventative measures less than the latter.

Hypothesis 3

For Hypothesis 3, an independent t-test revealed that the private sector did not attribute significantly higher values to democratic gains than the public sector. The aforementioned reasons explaining the results for Hypotehsis 1C can also be used to explain results for Hypothesis 3. However, additional insight regarding the nature of the Turkish private sector must be mentioned to better understand the current situation: namely, the Turkish private sector is not sufficiently involved in promoting democratic rights and is overly dependent on the government.

Turkey has the essential components of a market-oriented economy. Moreover, fundamental rules and regulations for such an economic model, including those for corporate governance, have become well embedded in national practice and social interactions (Arat et al. 2001). The Turkish Industrialists' and Businessmen's Association (TÜSİAD), the most influential business association in Turkey, claims that it is committed to its role as a democratizing force in the country, a role that is supremely important in a political and commercial environment where businesses do not feel that the state is responsive to their changing needs. However, according to Yavuz (2012), even the founding members of TÜSİAD, i.e. members of the economic elite, are dependent on the state, and their pro-democratic role is perceived to endure only as long as there are no threats to their capitalist interests. As such, the already-weak leverage of the Turkish private sector is especially pronounced when it comes to pressuring the state to seek a balance between democracy and security in its policies. In line with these findings, a 2006 Civicus report found that the Turkish private sector prefers to assume corporate social responsibilities in safe areas such as environmental issues and education rather than becoming involved in more sensitive issues such as human rights and freedom of expression. For example, the National Cyber Security Strategy and 2013-14 Action Plan do not make any reference to addressing private sector reservations, if there are any, in those areas. Since the private sector in Turkey is relatively weak, their sphere of influence is directly contingent on its relationship with the government, which limits their capacity to oversee the state's cyber security preparation and enforcement of democratic values.

To briefly summarize findings from these three hypotheses, Turkey is experiencing a transition wherein it is trying to adapt its security posture to a dynamic environment filled with

numerous cyber threats. Examining governance aspects of cyber security in Turkey, the current study found that public-private cooperation is likely to positively affect national cyber security preparedness; that Turkish private and public organizations have similar preparedness levels; and that both private and public organizations do not accord a high value to democratic concerns. While effective government agencies are critical to enhance national preparedness they are paradoxically unsuccessful in enhancing organizational preparedness. As a result, Turkey must regard cyber security as a governance concern and decide which organizations will lead cyber security efforts: either organizations with highly capable technological infrastructure or organizations with security mandates and experiences. Its ultimate decision will also affect its cooperation with the private sector, without which national security efforts will lag behind. What follows is a discussion of policy recommendations that could guide Turkey in its governance of the cyber realm, in its reorganization of institutional roles and responsibilities, in its relations with the private sector, and in its consideration of democratic values.

Policy Recommendations

The security of government agencies, private businesses, and citizens are all highly interconnected in the cyber domain. In such an environment, traditional approaches to security that state that it is primarily the government's responsibility to protect citizens and private organizations from illegal activities are not adequate (Hiller and Russell 2013). Following changes in the nature of security threats, Turkey altered some of its security architecture accordingly; for example, its Strategic Defense Document characterized cyber threats as threats to national security (Lewis and Timlin 2011). However, this step alone is not sufficient, and further institutional rearrangements must reflect these new perceptions on cyber threats, deter

cyber criminals, and simultaneously mitigate and respond to the effects of cyber attacks (Guitton 2013). To achieve security in its cyber domain, there are several steps that Turkey should take, steps which will be discussed below.

First of all, the Turkish government's pledge to secure cyber space needs to extend beyond its own agencies and departments and include private businesses in order to reduce risks and promote security. For that reason, appropriate mechanisms based on mutual trust between the public and private sectors should be established to channel private sector resources and expertise in boosting national cyber security preparedness. This engagement should not be limited to the current eight critical spheres listed in Turkey's Cyber Security Strategy Document (i.e. energy, communication), but should rather reach out to all other relevant stakeholders, such as the IT sector. Furthermore, although involving private actors in national securities is a new concept, public agencies should focus on harnessing the private sector's potential to establish public-private partnerships, create rapid response mechanisms for cyber attacks, and facilitate information-sharing. By taking such steps, Turkey would – and should – embrace a model for national cyber security governance based on holistic approaches and thereby include all relevant actors in securing its cyber realm.

In addition, cyber security is likely to alter organizational relationships between civilian and military government agencies, Internet service providers, and private businesses, ultimately affecting national cyber security governance (Mueller and Kuehn 2013). Instead of opposing these changes, Turkey should accept these realities on the ground, reorganize government agencies' roles and responsibilities accordingly, and view this process as strategic and adaptive in nature to maintain and even enhance cyber security (Harknett and Stever 2009). While

reassigning roles and responsibilities, Turkey should place more importance on organizational capacity than on technical competency to ensure tasks are successfully executed. The Turkish government will be much more prepared to defend its networks if the main government agency responsible for cyber security can prevent poor cooperation and duplicated efforts from other government agencies and, most importantly, stimulate private sector contributions through the use of effective mechanisms.

Therefore, while reorganizing its existing interdepartmental model, the Turkish government should transfer the lead role from the Ministry of Transportion, Maritime Affairs and Communications to the Ministry of Interior, which traditionally has assumed security roles in the country. The Ministry of Interior has the administrative and technical capabilities to fulfill such a role, since it has 1) the dynamics to unite all necessary agencies and departments to create a collaborative cyber security strategy and 2) the ability to reach out to the private sector. Having thus altered a part of its interdepartmental model, Turkey will be able to take advantage of siloes of security expertise accumulated in other organizations (such as law enforcement bodies, the Turkish Cyber Command, and Intelligence services) and effectively use them in the cyber domain, strengthening existing close ties between the private sector and the Ministry of Interior.

If the Ministry of Interior assumes a leading role in the interdepartmental framework, it should then elevate the head of its internal IT department to a level that would allow him/her to collaborate with high-level administrators in other government agencies, as is the case for the Directorate General of the Turkish Law Enforcement, who has the authority to work outside the agency. The Ministry of Interior's IT head must directly report to the Minister of Interior; have a permanent seat on the National Security Board, which establishes policy corresponding to its

name; replace the National Cyber Security Board, which is inflexible, slow, and ineffective; and work in tandem with the National Center for Cyber Incident Response (USOM). Under these circumstances, national cyber security governance will become more responsive, and the Ministry of Interior, together with other relevant government agencies, will be able to more quickly respond to possible cyber threats. If such flexibility-enhancing measures are not taken, it is highly probable that any agency at the head of the interdepartmental model will not be able to stay abreast of evolving cyber threats.

Regarding foreign cyber threats, the Ministry of Defense should also assume more responsibility for maintaining a secure Turkish Internet; this is highly important for Turkey's ability to adapt to international developments, wherein cyber threats are increasingly becoming a source of conflict between states. For example, the International Strategy for Cyber Space, which the Obama Administration released in 2011, embraces a deterrence component, stating that the United States "will respond to hostile acts in cyber space as we would to any other threat to our country," i.e. via diplomatic, military, and/or economic means (CFR, 2013). In the Turkish context, the transformation of cyber conflicts into national conflicts will further complicate organizational challenges, since civilian institutions will cooperate with military organizations more frequently than in the past. It is key, then, for the Ministry of Defense to ensure that the Turkish Military Cyber Command works closely with the Ministry of Interior. Under these circumstances, the Turkish government will be able to prevent potential coordination problems between military and civilian agencies and better guarantee the protection of Turkish cyber space from foreign enemies.

Transferring cyber security responsibility from the Ministry of Transportation, Maritime Affairs to the Ministry of Interior, with heightened involvement from the Department of Defense, will also decrease the national security burden on civilian agencies with technical capacities and enable them to focus on their primary cyber security duties, i.e. assisting security organizations from a technological point of view. At present, such agencies have refocused their attention from technology-related tasks to security-related tasks, and this has largely impeded their ability to protect the cyber domain, as they are not working within their specialties. Therefore, legislation should be amended to prevent heightened securitization of civilian government agencies. Under this model, two Ministries, (i.e. the Ministry of Interior and the Ministry of Transportation, Maritime Affairs) and the MIT would be drawing upon the technical capabilities of relevant agencies, such as ICTA, PTC, all the while assuming responsibility for purely security-related concerns.

Another highly significant reorganizational issue is related with the role of the MIT. In 2014, new legislation gave this institution the authority to gather cyber intelligence, which is increasingly becoming an indispensable part of national security. Resultantly, the MIT is legally bound to enhance its organizational and technical capabilities to assume an overarching role in the cyber domain. However, this authorization should not transform the MIT into the lead organization responsible for national cyber security governance. As far as public-private cooperation is concerned, it has been shown that intelligence services fall short of establishing trust with the private sector and mobilizing it to contribute to national cyber security. In the American context, for instance, the private sector did not trust the NSA, which forced the presidential administration to name the civilian Department of Homeland Security as the head

organization overseeing cyber security and mediating between the private and public sectors (Mueller and Kuehn 2013). When this model is applied to Turkey, if the MIT is given control over protecting national cyber security, similar problems regarding trust could emerge, and the MIT would be consequently overburdened. As a result, its cyber intelligence activities will be greatly compromised.

Democratic values should be a key component of Turkish national cyber security governance. Ammori and Poellet (2010) argue that when it comes to securing the cyber realm, government agencies must be provided with a certain degree of discretion, due to the dynamic nature of cyber threats; however, this discretion must be checked with safeguards that ensure trust in these agencies' actions and ultimate objectives. Because cyber security measures universally give states the upper hand with interfering with online privacy, the Turkish government should constrain its power through legislative measures in order to not compromise precious democratic gains for the sake of security. To achieve this goal, Turkey can use its EU accession process as leverage for underscoring the importance of democratic values (Sozen and Shaw 2003; Dogan 2006; Alikilic and Atabek 2012) and for establishing a solid cyber security strategy that finally includes Turkey in the EU's informational security structures (Gurkaynak et al. 2013). Such a position with respect to the EU will guarantee a more democratic cyber security governance framework for Turkey.

Another recommendation is for Turkish private organizations to be given incentives (such as tax breaks) encouraging them to enhance their in-house cyber security capabilities. Such measures should especially enable private businesses to employ additional IT experts, based on the confidentiality of data used in businesses' day-to-day functions. Since the Turkish state has

abandoned large-scale ownership of the economy following liberalization reforms, it can also utilize thorough regulations that empower private businesses to protect their own informational assets and increase their cooperation with government agencies. As such, Turkey can employ a hybrid model of governmental measures to co-opt private organizations in its cyber security policies and boost levels of preparedness and democratic governance.

Finally, educational programs should be developed to train IT personnel to work in both the private and public sectors and to exchange information and best practices with colleagues across organizations and sectors. An important component of these trainings would be a module on preparing for and responding to threats, which would allow IT personnel to collaborate with government agencies in instances where Turkey could experience a massive cyber attack. In instances of such collaboration, specialized IT personnel would be carrying out work on behalf of the government while remaining employed by their respective private organizations; as a result, the government would incur a reduced cost burden, since it would not be paying these specialists. Put differently, these educational programs would create a cadre of IT specialists prepared to respond to crises in a cost-effective manner.

As a conclusion, the Turkish government should keep in mind that cyber security requires a "whole of nation" approach to fully take advantage of all resources, including public agencies, private sector organizations, and individuals. With this in mind, Turkey should especially heighten the involvement of private sector organizations in its cyber security policies, as they would then have an opportunity to voice their concerns to the government regarding democratic governance. The resulting presence of democratic values in Turkish cyber security governance would ultimately determine its authoritarian or libertarian nature.

Future Research

This study is timely in terms of observing Turkey's initial efforts to adopt a national security posture against cyber threats. The government had planned to adopt many preventative measures in 2013 and 2014 according to its 2013-2014 Action Plan; at present, several of these measures remain to be fully enacted. For example, in 2013, so-called sectorial "Teams for Responding to Cyber Incidents (SOME)" were established in each critical infrastructure domain (e.g. energy, communication, banking/financing, etc.) to secure systems and assets owned by both public and private organizations. The Action Plan also allows public agencies and departments to establish their own institutional SOMEs (independent of sectorial SOMEs) in 2014, a move which aims to increase government bodies' in-house cyber security capabilities. While sectorial SOMEs have already been established, it will only be at the end of 2014 that institutional SOMEs will be fully established. Once all SOMEs are operational, a successive study should track how SOMEs have improved Turkey's national cyber security governance based on findings from this current study.

Although public and private organizations invest in cyber security, their informational systems still experience major security breaches. For instance, Turkish public organizations still encounter "Denial of Service" attacks. This fact reminds us that cyber security is not merely a technical concern and that there are other issues at play. Further research should focus on another one of these issues, i.e. the decision-making processes that determine security measures. Simon (1997) suggests that instead of following rigid rules for optimal decision-making, individuals inside and outside of organizational frameworks use heuristics, i.e. they make decisions based on the complexity of the situation at hand and on their inability to process and calculate the

expected utility of alternative decisions. They also encounter biases (such as over-confidence, conformation bias, and availability bias) that impede their decision-making. Within an organizational framework, heuristics and biases must be examined to understand whether they undermine the quality of decisions on cyber security. Future research should examine decisions that are all-encompassing, ranging from individual to organizational (and even national) decisions on cyber security. More specifically, it should analyze whether or not individuals and organizations are overly reliant on intuition rather than on objective knowledge when it comes to combatting threats, especially since current literature falls short of providing metrics to analyze threat responses (Julisch 2103¬). Taking into consideration the cyber domain's complexity, the inability to determine the scale of threats, and existing measures' respective levels of effectiveness, researchers should also focus on 1) whether perfectly rational decision-making is feasible for cyber security, as it is assumed in rational theory, or 2) whether a cyber agent would suffice for making cyber security decisions, since rationality is also bounded in the cyber domain, according to Simon (1997). Such research, in sum, will ultimately enhance cyber security, since decision-makers will be aware of factors impeding decision-making process and possible gaps and weaknesses in their thought processes.

Finally, this present research focused on cyber security in times of peace; however, cyber issues are increasingly becoming a source of conflict. Therefore, future research should evaluate cyber governance in the context of war. More specifically, it should examine the possibility of mobilizing civilian assets during war and the extent to which governments' wartime cyber security measures impede populations' democratic rights. With this knowledge in hand,

governments will be better equipped to react to cyber wars while keeping democratic rights intact.

Limitations

The proposed research has some limitations, the most significant being its cross-sectional design, which necessitates caution upon interpreting observed phenomena. Due to the study's cross-sectional design, it is not possible to discern causal relationships with any degree of certainty. Since existing literature mainly focuses on the developed world, where individualist approaches are strong and voluntary measures are preferred, using it as a benchmark for developed countries, where hierarchical approaches are dominant and regulation is seen as compulsory for stimulating changes in security tendencies, is problematic (Quigley and Roy 2011). When considered from a cultural perspective, organizations' cyber security tendencies may change across countries, which complicates the research's cross- sectional design. This limitation arising from the study's cross-sectional nature can be overcome through future studies' use of both longitudinal and experimental design, used to establish causality among study variables.

Another limitation is related to the survey's sample size. Although accessing participants through CSA was the best available option for the researcher, there are still limited possibilities for making generalizations based on such a small sample size (Singleton 2009; Trochim and Donnelly, 2008). However, scholarship acknowledges the possibility of a low response rate when information gathered through online surveys is of a sensitive nature, such as information on organizations' security practices (Kotulic and Clark 2004). Some participants could have

figured that such data are strictly confidential and internal to their own organizations. This concern was especially relevant for participants from public agencies, where sharing institutional information is highly restricted and official procedures for sharing such information are generally exhaustive, requiring authorization from higher executives. As such, these considerations could have negatively impacted the survey's total response rate (Abu Musa 2010).

Finally, although not intentionally, this study might have excluded micro and small sized organizations, since it targeted IT experts, CIOs, and executives responsible for IT departments (i.e. personnel who are generally indicative of larger organizations). Therefore, micro and small organizations (especially in the private sector) lacking budgetary and human resources to establish IT departments and manage similar governance concerns might not have been sufficiently captured.

Conclusion

This study focused on national cyber security preparation efforts through the lens of governance theory. According to its findings, governments, embracing a "whole of nation" approach, must mobilize all their national assets to maintain security in the cyber domain. This way, the more sophisticated that threats in the cyber domain become, the more prepared that governments are to combat them. States' intensified efforts to integrate cyber security into broader frameworks for national security and defense and to prepare for online threats is increasingly becoming less of a technological concern and more of a governance issue. The first dimension of this governance problem is for states to create dynamic cyber security capacities across all spectra of the government by orchestrating efforts among numerous state authorities.

The second dimension is for public organizations to establish mechanisms allowing them to cooperate with the private sector in matters of security (Kramer et al. 2009). To achieve such a goal, government agencies need to adjust their institutional mindsets and embrace a coherent security strategy centered on sharing power with other domestic actors, mainly private sector organizations that own and operate a great bulk of critical infrastructure. The third dimension of cyber security governance is for states to establish a balance between democracy and security, especially since the former is at great risk of being compromised in favor of the latter.

In short, national cyber security preparation depends on the extent to which a government organizes its interdepartmental model based on the needs of public and private entities and mobilizes private actors to help defend against common threats. All governance efforts must attribute value to those democratic gains that the Internet and communication technologies have unprecedentedly promoted for the last thirty years.

APPENDIX A

IRB APPROVAL FORM

THE UNIVERSITY OF TEXAS AT DALLAS
Office of Research Compliance
800 W Campbell Road AD15 Richardson Texas 75080-3021
972-883-4558 Fax 972-883-2310

Date: 11 December 2013

To: Gokhan Ikitemur
Douglas K. Lowell, Ph.D.
Economic, Political and Policy Sciences

From: Sanaz Okhovat
Senior Director, Office of Research Compliance
Office of Research

Re: **MR 13-467**
Enhancing the Effectiveness of Cybersecurity Governance in Turkey through Public-Private Cooperation

This letter is notification of Minimal Review Approval of research project listed above. This submission meets the criteria for exemption #2 of Chapter 45 Code of Federal Regulations Part 46.101(b). IRB approval of this research begins as of **11 December 2013** and ends on **10 December 2014.**

The IRB requires all those who have access to research data be trained in research ethics and practices concerned with the protection of the welfare and rights of research participants. These ethical principles are outlined in the Belmont Report.

Investigators and key personnel involved with this protocol must have documented training with this office. The training can be found at http://www.utdallas.edu/research/orc/irb/required_training/

If you have any questions related to this approval, you may contact me by phone at 972-883-4579 or by email at sanaz.okhovat@utdallas.edu.

APPENDIX B

SCALES FOR STUDY VARIABLES

Variables	**Scales**	**Cronbach's Alfa**
National cybersecurity Preparedness	Q12_7, Q31_2, Q31_3, Q31_6, Q31_7 Q31_8, Q31_9, Q31_10, Q38, Q40_9, Q40_10, Q40_11,	0.80
Public private cooperation	Q12_1, Q12_3, Q12_4, Q12_5, Q12_6, Q12_8, Q12_9, Q35, Q36, Q37, Q40_8	0.73
Organizational preparedness	Q40_1, Q40_2, Q40_3, Q40_4, Q40_5, Q40_6, Q55, Q56, Q57, Q58	0.89
Institutional effectiveness	Q32_1, Q32_2, Q32_3, Q32_4, Q32_5, Q32_6, Q32_7, Q32_8, Q32_9, Q32_10, Q32_11, Q32_12	0.8
Democratic values	Q62, Q63, Q64, Q65, Q66, Q67	0.65

APPENDIX C

QUESTIONNAIRE

Cybersecurity Governance Survey

Section 1
Cooperation

1. How would you classify your organization?
    - Public agency
    - Private business

2. If you are a government agency (if not please skip to Q4) – do you have any formal cooperation concerning cyber-security practices with private businesses?
    - Yes
    - No
    - Don't know

3. If you responded yes to the previous question (If "No" please go to Q12), what is the nature of this cooperation? Mark all that apply.
    - Financial contract
    - Information sharing
    - Sharing of best practices
    - Training
    - Resource sharing
    - Cyber-security research
    - Ad Hoc alliances against imminent cyber threats
    - Forensic
    - Technological assistance (please skip to Q8)

4. If you are a private company, how often do you communicate with government agencies concerning cyber-security issues?
    - Daily
    - Weekly
    - Monthly
    - Bi-annually
    - Annually

- We don't communicate

5. Do you cooperate with government agencies concerning cyber security threats?
   - Yes
   - No
   - Don't know

6. If you responded yes (if not please skip to Q12) to the previous question, what is the nature of this cooperation? Mark all that apply.
   - Financial contract
   - Information sharing
   - Sharing of best practices
   - Training
   - Resource sharing
   - Cyber-security research
   - Ad Hoc alliances against imminent cyber threats
   - Forensic
   - Technological assistance

7. What events or circumstances motivate your organization to have a cyber-security cooperation with public organizations. Mark all that apply.
   - Previous cyber attack
   - Regulatory compliance
   - Security incentives provided by public sector
   - Previous security cooperation for threats other than cyber attacks
   - The growing scale of attacks in your sector
   - Privacy concerns regarding consumers/citizens information
   - Potential liability concerns in the event sensitive information is compromised
   - Other (please specify-----)

8. If your agency/company involves in public-private cyber-security cooperation- who drives or sets the agenda and strategy?
   - Government agency
   - Private/Business
   - Shared

9. Does this cooperation have defined roles or responsibilities for parties?
   - Yes
   - No
   - Don't know

10. Does the public-private sector collaborative effort or partnership have specific performance measures to determine the success or progress?
    - Yes
    - No
    - Don't know

11. Please detail the nature and extent of your cooperation with government agencies/private business concerning cyber-security.

12. How influential do the following factors that might be encountered in the process of engaging the private sector in collaborative cyber security activities aiming to enhance overall national cyber security preparedness.

	1. not at all influential	2. somewhat influential	3. Neutral	4. influential	5. very influential
Trust					
Liability concerns					
Regulations/Laws					
Budget concerns					
Differing Sectorial Goals (i.e profit seeking in the private sector)					
Public sector cannot assume leadership role					
Undefined roles and responsibilities					
Differences in organizational decision making structures					
Parties do not attach adequate importance to cyber threats					
Lack of communication to lay the groundwork for cooperation					
Other factors					

Cybersecurity Preparedness

Directions: Please use a scale of 1 to 5, where 1 is "not likely at all" and 5 is "very likely" for the following questions (13-14).

13. How likely do the following cyber-security concerns pose a threat to your agency/company?

	1. Not likely at all	2. Somewhat likely	3. Neutral	4. Likely	5. Very likely
Computer virus, worm, or Trojan horse					
Denial of service					
Electronic vandalism or sabotage					
Fraud/ Embezzlement					
Theft of intellectual property (copyrights, patents, trade secrets, trademarks)					
Theft of personal or financial information such as names and dates of birth					
Other computer security incidents such as hacking, spoofing, phishing					
Misuse of computers by employees (Internet, e-mail, etc.)					
Breaches resulting from information obtained from stolen laptops					
Other please specify:----					

14. How likely do the following potential sources of cyber-security threats cause for a security concern to your agency/company?

	1. Not likely at all	2. Somewhat likely	3. Neutral	4. Likely	5. Very likely
Current employee					
Former employee, contractor, vendor, temporary worker, etc.					
Domestic competitor					
Foreign competitor					
Lone wolf hackers					
Activist/ Activist Organizations/ Hactivists					
Organized crime					
Foreign Nation States (please specify -----)					
Other (please specify: --)					

15. Has your department/agency/company suffered from a cyber-attack in the past 12 months? (If "no", please skip to Q20)
    - Never
    - 1 time
    - 2 times
    - 3 times
    - 4 times
    - More than five times

16. To which of the following organizations were these incidents reported? Mark all that apply.
    - The Centre for Response to National Cyber Threats (USOM)
    - Sectorial Cyber Incident Response Teams (SOME)
    - Ministry of Transportation, Maritime Affairs and Communications
    - The Information and Communication Technologies Authority (BTK)
    - The Scientific and Technical Research Council of Turkey (TÜBİTAK)
    - Under secretariat of Public Order and Security
    - The National Intelligence Organization
    - Ministry of National Defense
    - Ministry of Interior
    - The Presidency of Telecommunication and Communication
    - The Cyber-security Board

- Law Enforcement Agencies
- Military
- Other (please specify---)

17. How many of these incidents were reported to the organizations specified in Q16?
    - Never
    - 1 time
    - 2 times
    - 3 times
    - 4 times
    - More than five times
    - All incidents were reported

18. If any incidents were not reported to the organizations specified in Q16, what were the reasons?
    - Handled internally
    - Reported to third party contractor providing cyber security services
    - Reported to another organization (please specify---)
    - Negative publicity
    - Lower customer/client/investor confidence
    - Lower citizen confidence
    - Competitor advantage
    - Did not want data/hardware seized as evidence
    - Did not know who to contact
    - Incident outside jurisdiction of law enforcement
    - Did not think to report
    - Nothing to be gained/nothing worth pursuing
    - Other (please specify---)

19. What was the relationship between the suspected offender and this company at the time of the incidents indicated in Q15? Mark all that apply.
    - Current employee
    - Former employee, contractor, vendor, temporary worker, etc.
    - Domestic competitor
    - Foreign competitor
    - Lone wolf hackers
    - Activist/ Activist Organizations/ Hactivists
    - Organized crime
    - Foreign Nation States (please specify---)
    - Other (please specify---)
    - I don't know

20. Has your department/agency/company successfully stopped a significant cyber-attack in the past 12 months?
    - Yes
    - No
    - Don't know

21. Has your agency/organization ever cooperated with any public organization to stop these attacks?
    - Yes (please specify organization ---)
    - No
    - Don't know

22. How influential do you think this collaborative incident response was effective to stop cyber-attacks?
    - Not at all influential
    - Somewhat influential
    - Neutral
    - Influential
    - Very influential

23. Do you participate in annual national cyber security drills carried out by public organizations.
    - Yes
    - No
    - Don't know

24. Does your organization participate in any Sectorial Cyber Incident Response Teams' (SOME) activities, if available in your industry sector?
    - Yes
    - No
    - Don't know

25. Think for a moment about the financial costs associated with a cyber-attack against your company's computer system. How would you rate the potential cost of the average attack?
    - Not expensive at all ≤ 50.000₺
    - Not very expensive 250.000₺- 50.000₺
    - Somewhat expensive 500.000₺- 250.000₺
    - Expensive 1000.000₺- 500.000₺
    - Very expensive ≥1.000.000₺

26. What do you think is the main reason for the increased number of cyber-attacks over the past year? (Please select which one applies to you).

- Defenses aren't strong enough
- There are more hackers/ organized criminal groups than in the past
- Nation states sponsor cyber attacks
- The number hasn't risen; it's just that there is more media hype surrounding them
- Don't know

27. Thinking about the issue of cyber security overall, how would you describe the threat governments and businesses face, on a scale of 1 to 5, with 1 representing not threat at all and 5 representing a profound, ongoing threat that grows worse with the passage of time?

	1- No threat	2- Low threat	3- Neutral	4- Threat	5- Profound threat
Government					
Businesses					

Directions: Please use a scale of 1 to 5, where 1 is "not vulnerable at all" and 5 is "very vulnerable" for the following questions. (14-15)

28. How would you rate government's/ Business sector's vulnerability to major cyber-attacks?

	1- Not vulnerable at all	2- Somewhat vulnerable	3- Neutral	4- Vulnerable	5- very vulnerable
Government IT systems					
Business IT systems					

29. If there were a coordinated and targeted cyber-attack in your country, which sector do you believe is most vulnerable?

	1. Not vulnerable at all	2. Somewhat vulnerable	3. Neutral	4. Vulnerable	5. Very vulnerable
Financial services					
Communications					
Utilities					
Media					
Telecommunication					

Transportation (air, rail and/or highway)					
Education					
IT(Hardware/Software)					
Manufacturing					
National Defense					
Local government services					
Essential government services(e-state)					
Other (please specify---)					

30. How vulnerable are business/government IT systems because of a shortage of qualified IT security professionals?

	1. Extremely vulnerable	2. Vulnerable	3. Somewhat vulnerable	4. Moderately vulnerable	5. Not vulnerable
Government IT systems					
Business IT systems					

Directions: Please use a scale of 1 to 5, where 1 is "not at all influential" and 5 is "very influential" for the following questions. (31-32)

31. How influential do you think each of the following items on improving the state of cyber security?

	1. not at all influential	2. somewhat influential	3. Neutral	4. influential	5. very influential
Individual employees					
Companies implementing best practices and better security policies					
IT security industry through better technology					
Public Awareness about evolving cyber threats					

Public private cooperation					
Public private partnership					
Information sharing between public and private sectors					
Government regulations					
Low enforcement					
National cyber-security drills					
Enhancing national capacity to producing hardware and software					

32. How influential do the following government institutions to improve your agency/ company's overall cyber-security strategy?

	1. Not at all influential	2. Somewhat influential	3. Neutral	4. Influential	5. Very influential
The Centre for Response to National Cyber Threats (USOM)					
Sectorial Cyber Incident Response Teams (SOME)					
Ministry of Transportation, Maritime Affairs and Communications					
The Information and Communication Technologies Authority (BTK)					
The Scientific and Technical Research Council of Turkey (TÜBİTAK)					
Under secretariat of Public Order and Security					
The National Intelligence Organization					
Ministry of National Defense					
Ministry of Interior					
The Presidency of					

Telecommunication and Communication					
The Cybersecurity Board					
Law Enforcement Agencies					
Military					

33. If you were to find it necessary to seek government assistance with cybercrime or a cyber-security-related event, which organization(s) would you contact immediately?

- The Centre for Response to National Cyber Threats (USOM)
- Sectorial Cyber Incident Response Teams (SOME)
- Ministry of Transportation, Maritime Affairs and Communications
- The Information and Communication Technologies Authority (BTK)
- The Scientific and Technical Research Council of Turkey (TÜBİTAK)
- Under secretariat of Public Order and Security
- The National Intelligence Organization
- Ministry of National Defense
- Ministry of Interior
- The Presidency of Telecommunication and Communication
- The Cyber security Board
- Law Enforcement Agencies
- Military
- Other (please specify ---)
- None of these organizations

34. Which of the following institutions seek your input or opinion on policy or operational decisions regarding national cyber security policy.
    - The Centre for Response to National Cyber Threats (USOM)
    - Sectorial Cyber Incident Response Teams (SOME)
    - Ministry of Transportation, Maritime Affairs and Communications
    - The Information and Communication Technologies Authority (BTK)
    - The Scientific and Technical Research Council of Turkey (TÜBİTAK)
    - Under secretariat of Public Order and Security
    - The National Intelligence Organization
    - Ministry of National Defense
    - Ministry of Interior
    - The Presidency of Telecommunication and Communication
    - The Cyber security Board
    - Law Enforcement Agencies
    - Military
    - Other (please specify ---)

Directions: Please use a scale of 1 to 5, where 1 is “not satisfied at all” and 5 is “very satisfied” for following questions.

	1. Not satisfied at all	2. Somewhat satisfied	3. Neutral	4. Satisfied	5. Very satisfied
35. How satisfied are you that business and government’s information security initiatives aligned with each other?					
36. How satisfied are you that current national cyber security governance is appropriately structured to enable public private cooperation at national level?					
37. How are you satisfied that relevant government agencies actively engage both business stakeholders and technology decision makers in identifying requirements for the Nation’s cyber security strategy?					
38. How satisfied are you that governments and businesses have					

appropriate information sharing on cyber threats and how to combat them.					
39. How satisfied are you that current law in country is adequate against to deal with cyber threats?					

40. How much of a barrier is each of the following to improvement of the overall strategic effectiveness of your agency/company's information security function?

Directions: Please use a scale of 1 to 5, where 1 is "not a barrier at all" and 5 is "Extreme barrier" for each.

	1. Not a barrier at all	2. Somewhat of a barrier	3. Neutral	4. Barrier	5. Extreme barrier
Leadership: CEO, president, board, or equivalent					
Lack of an effective information security strategy at organizational level					
Lack of an actionable vision or understanding of how future business needs impact information security					
Insufficient capital expenditures					
Absence or shortage of in-house technical expertise					
Competing priorities, other initiatives					
Lack of effective laws/regulations					
Lack of public private cooperation					
Lack of public private partnership					

Insufficient government guidance					
Complexity of the external environment (government's cyber security structure)					

41. What is your view regarding overall cyber security governance in Turkey?

Section 2

Information Technology Governance

Organizational Cyber Security Governance Self- Assessment

	Yes	No	Not applicable
42. Does your organization have an information security strategy?			
43. Does your agency have a documented and approved governance for information security (i.e. defined responsibilities, policies and procedures)?			
44. Is there a business continuity/disaster recovery plan in place?			
45. Is this plan include measures in terms of how to deal with information security incidents/emergencies?			
46. Does your agency/company have a social media strategy (defines who is responsible to make announcements on social media regarding your organization, and who is responsible to secure the usage of your institutional account etc.)?			
47. Is business continuity/disaster recovery plan tested regularly?			
48. Do CIO/high executives in your agency/company understand the linkage between IT (cyber securıty) risks and enterprise risk management?			
49. Is there a Chief Information Officer with sufficient authority and resources specifically charged with managing information security in the organization?			
50. Is Chief Information Officer/ IT officer required to provide a report on cyber-security status, or posture of			

the enterprise, to the CIO/ high executives?			
51. Do you have a methodology that helps you determine the effectiveness of your organization's IT security policies and procedures based on clear measures?			
52. Does your agency/organization outsource any of the information security functions?			
53. Does your organization have a formalized plan for responding to insider IT security events committed against your organization?			
54. Are there appropriate training and awareness programs to ensure that personnel are aware of their (cyber) security responsibilities?			

Directions: Please use a scale of 1 to 5, where 1 is "not aligned at all" and 5 is "very aligned" for the following questions (55-56).

	1. Not aligned at all	2. Somewhat aligned	3. Neutral	4. Aligned	5. Very aligned
55. In your opinion how well are your agency/company's (IT) security policies aligned with your company's business objectives?					
56. In your opinion, how well is your agency/company's IT security spending aligned with your agency/company's business objectives?					

57. How confident are you that your company/agency's entire system (including all divisions/branches if there is any) is protected from cyber threats?
    - Not confident at all
    - Somewhat confident
    - Neutral

- Confident
- Very confident

58. How confident are you that your organization has instilled effective information security behaviors into the organizational culture?
    - Not confident at all
    - Somewhat confident
    - Neutral
    - Confident
    - Very confident

59. How frequently is information security governance included on your organization's leadership agenda?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Always

60. What percentage of this agency/company's total budget did this company/agency spend on the information security technology safeguards in 2013? Estimates are acceptable. Please round to nearest whole percent.
    - % 0
    - %1- %2
    - %3- %4
    - %5- %6
    - %7- %8
    - %9- %10
    - More than %10

61. With an eye on FY 2014, do you anticipate that cyber-security spending will increase, decrease or stay the same at your agency/company?
    - Increase more than 5%
    - Increase 1% to 5%
    - Stay the same
    - Decrease 1% to 5%
    - Decrease more than 5%
    - Don't know/decline to say

Section 3

Democratic Values

On a scale of 1 to 5, to what extent is you agree or disagree with the following questions. On a scale of 1 to 5, please rate your level of agreement with each factor, with 1 = very disagreed and 5 = very agreed.

	1. Not agreed at all	2. Somewhat agreed	3. Neutral	4. Agreed	5. Very agreed
62. Despite growing cyber threats, access to the Internet should be a fundamental right for all people.					
63. It is ok for people to express their ideas on the Internet, even if they are extreme.					
64. People should be able to express their opinion anonymously on the Internet.					
65. Governments should monitor content on the Internet.					
66. Governments should censor Internet content in order to protect children.					
67. Online security for both individual users and private companies depends on government regulation of the Internet.					
68. Legislations should enable government agencies and private companies to exchange information, including personal internet content and e-mails, to prevent potential cyber-attacks.					

Demographic Questions

69. In what sector your agency/company operate?
    - Finance/banking/insurance
    - Public accounting
    - Transportation/aerospace
    - Retail/wholesale/distribution

- Media
- Military
- Law enforcement
- Central government
- Provincial government
- Local government
- Technology services/consulting
- Manufacturing/engineering
- Telecommunications/communications
- Mining/construction/petroleum/agriculture
- Utilities
- Legal/law/real estate
- Healthcare/medical/pharmaceutical
- Advertising/marketing/media
- Education/nonprofit
- Other (please specify: ---)

70. Which of the following is closest to your job level?
    - President/CEO
    - Professor
    - Deputy governor/District governor
    - Vice president
    - Law enforcement officer
    - Practitioner/Professional
    - Military officer
    - Supervisor
    - Manager
    - Director
    - Chief Information Officer
    - IT Expert
    - External consultant
    - Other (please specify: ---)

71. Which of the following best describes your primary involvement with IT security and/or cyber-security at your agency? Select all that apply.
    - Define mission or technology requirements
    - Manage implementation of security technology
    - Manage relationships with vendors or service providers
    - Make the final decision for products or service providers
    - Make the final decision for IT security decisions
    - Investigate or evaluate products or service providers
    - Make the tasks given by the CIO

- Other

72. How is your company/agency's cyber security model structured?
    - Centralized and IT security responsibility is assumed by central IT department
    - Centralized for common e-services but each division/branch is responsible for their computer security
    - Decentralized and each division/branch is responsible for their IT security
    - Decentralized but general IT security principles are determined by central IT department
    - My company/agency has no division/branch
    - Don't know/not applicable

73. In 2013, what types of computer networks (including Internet) or equipment did this company/agency use?
    - Local area network (LAN)
    - Wide area network (WAN)
    - Process control network (PCN)
    - Virtual private network (VPN)
    - Wireless network (e.g.,802.11)
    - Electronic data interchange (EDI)
    - Internet
    - Intranet
    - Extranet
    - Stand-alone PCs (not on LAN)
    - Company-owned laptops
    - Laptops not owned by company
    - Other (Please specify: ---)

74. In 2013, what types of network access did this company/agency support? Mark all that apply.
    - Hard-wired telecommunications lines
    - Remote dial-in access via telecommunications lines
    - Access to company networks or e-mail through Internet
    - Wireless access to e-mail
    - Wireless access to Internet
    - Wireless access to this company's data or other networks
    - Other (Please specify: ---)

75. In 2013, which of the following Internet services, if any, did this agency/company provide to other companies/agencies or individuals as its PRIMARY line of business? Mark all that apply.-

- Internet Service Provider (ISP)
- Web Search Portal
- Publicly accessible website WITHOUT e-commerce/ e-state capabilities
- Publicly accessible website WITH e-commerce/ e-state capabilities
- Other Internet service Specify:
- None of the above

76. Does your company/agency have an institutional account on social medial websites (Facebook, Twitter etc.) to directly access customers/citizens?
    - Yes
    - No
    - Don't know

77. In which geographic location is your company/agency located?
    - Marmara Region
    - Central Anatolia Region
    - Aegean Region
    - Mediteriranian Region
    - Black Sea Region
    - South Anatolia Region
    - East Anatolia Region

78. How many people are employed in your enterprise, including all branches, divisions and subsidiaries?
    - under 100
    - 100 - 499
    - 500 – 999
    - 1,000 - 2,499
    - 2,500 - 4,999
    - 5,000 - 7,499
    - 7,500 - 9,999
    - 10,000 - 19,999
    - 20,000 - 29,999
    - 30,000 - 49,999
    - 50,000 - 99,999
    - 100,000 or more
    - Don't know

REFERENCES

Abdulhamid, Shafii M., Sulaiman Ahmad, Victor O. Waziri, and Fatima N. Jibril. 2014. Privacy and national security issues in social networks: The challenges. *International Journal of the Computer, the Internet and Management* 19. no.3: 14 -20

Abu-Musa, Ahmad. 2010. Information security governance in Saudi organizations: An empirical study. *Information Management & Computer Security* 18, no. 4: 226-276.

Acemoglu, Daron, Azarakhsh Malekian, and Asuman Ozdaglar. 2013. *Network Security and Contagion*.

Alikilic, Ozlem, and Umit Atabek. 2012. Social media adoption among Turkish public relations professionals: A survey of practitioners. *Public Relations Review* 38, no. 1: 56-63.

Allen, Julia H. and Jody R. Westby. 2007. Characteristics of effective security governance 1. *EDPAC: The EDP Audit, Control, and Security Newsletter* 35, no. 5: 1-17.

Ammori, Marvin and Keira Poellet. 2010. " Security versus freedom" on the internet: Cybersecurity and net neutrality. *SAIS Review* 30, no. 2: 51-65.

Anderson, Ross and Tyler Moore. 2006. The economics of information security. *Science* 314, no. 5799: 610-613.

Andreasson, Kim. 2012. *Cybersecurity: Public sector threats and responses*. Boca Raton, FL: Taylor &Francis Group

Andress, Amanda. 2003. *Surviving Security: How to Integrate People, Process and Technology.* London: CRC Press.

Aquilina, Kevin. 2010. Public security versus privacy in technology law: A balancing act? *Computer Law & Security Review* 26, no. 2: 130-143.

Arat, Tugrul, Izak Atiyas, Erdem Basci, and Turgut Tan. 2001. The Legal Framework for Private Sector Activities in Turkey. In *Turkey and Central and Eastern European Countries in Transition*, ed. S. Togan and V.N. Balasubramanyan, 222-243. New York NY: Palgrave

Arquilla, John and David Ronfeldt. 1993. Cyberwar is coming! *Comparative Strategy* 12, no. 2: 141-165.

Bardach, Eugene. 1998. *Getting agencies to work together: The practice and theory of managerial craftsmanship*. Washington, DC: Brookings Institution Press

Baskerville, Richard, Paolo Spagnoletti, and Jongwoo Kim. 2014. Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management* 51, no. 1: 138-151.

Bauer, Johannes M. and Michel J. G. van Eeten. 2009. Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy* 33, no. 10–11: 706-719.

Beasley, Mark S. and Mark L. Frigo. 2007. Strategic risk management: Creating and protecting value. *Strategic Finance* 88, no. 11:24-33

Belk, Robert and Matthew Noyes. 2012. On the use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy. http://live.belfercenter.org/files/cybersecurity-pae-belk-noyes.pdf (accessed September 10, 2013)

Bessant, Judith. 2012. Human rights, the law, cyber-security and democracy: After the European convention. *Australian Journal of Human Rights* 18, no. 1: 1-26.

Betz, David and Stevens, Tim. 2011. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. New York: Routledge.

Bonabeau, Eric. 2007. Understanding and managing complexity risk. *MIT Sloan Management Review* 48, no. 4: 62-68, http://search.ebscohost.com/login.aspx?direct=true&db=bft&AN=510663623&site=ehost-live.

Bremmer, Ian. 2010. Democracy in cyberspace-what information technology can and cannot do. *Foreign Affairs* 89, no. 6: 86–92

Brito, Jerry and Tate Watkins. 2012. Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. *Harvard National Security Journal* 3, no. 1: 39-84

Busch, Nathan E. and Austen D. Givens. 2012. Public-private partnerships in homeland security: Opportunities and challenges. *Homeland Security Affairs* 8, no. 1: 1-24

CAN Cyber preparedness workshop: Bridging the gap between emergency management and cybersecurity summary report. http://www.cna.org/sites/default/files/research/CyberWorkshopSummaryReport.pdf. (accessed August 28, 2013).

Caruson, Kiki, Susan A. MacManus, and Brian D. McPhee. 2012. Cybersecurity policy-making at the local government level: An analysis of threats, preparedness, and bureaucratic roadblocks to success. *Homeland Security & Emergency Management* 9, no 2: 1–22

Cavusoglu, H., B. Mishra, and S. Raghunathan. 2004. A Model for IT security Investments. *Communications of ACM* 47, no. 7: 87-92

Chabinsky, R., Steven. 2010. Cybersecurity strategy: A primer for policy makers and those on the front line. *Journal of National Security L.aw & Policy* 4: 27-39

Chawki, Mohamed. 2010. Anonymity in cyberspace: Finding the balance between privacy and security. *International Journal of Technology Transfer and Commercialisation* 9, no. 3: 183-199.

Chesterman, Simon. 2008. We can't spy… if we can't buy!': The privatization of intelligence and the limits of outsourcing 'Inherently governmental functions. *European Journal of International Law* 19, no. 5: 1055-1074.

Chong, Josephine LL, Prof Tan, and B. Felix. 2012. IT governance in collaborative networks: A socio-technical perspective. *Pacific Asia Journal of the Association for Information Systems* 4, no. 2: 3.

Choo, Kim-Kwang Raymond. 2011a. Cyber threat landscape faced by financial and insurance industry. *Trends and Issues in Crime and Criminal Justice* no. 408: 1.

Choo, Kim-Kwang Raymond. 2011b. The cyber threat landscape: Challenges and future research directions. *Computers & Security* 30, no. 8: 719-731.

Citron, Danielle Keats. 2009. Cyber civil rights. *Boston University Law Review.* 89, no. 61: 62-125

Clarke, Roger. 2009. Privacy impact assessment: Its origins and development. *Computer Law & Security Review* 25, no. 2: 123-135.

Clarke, Richard A. and Knake, Robert K. 2010. *Cyberwar: The Next Threat to National Security and What to Do about It.* New York: Harper/Collins.

Clinton, Larry. 2011. A relationship on the rocks: Industry-government partnership for cyber defense. *Journal of Strategic Security* 4, no. 2. 97-112.

Colarik, Andrew and Lech Janczewski. 2012. Establishing cyber warfare doctrine. *Journal of Strategic Security* 5, no. 1: 31-48.

Coldebella, Gus P. and Brian M. White. 2010. Foundational questions regarding the federal role in cybersecurity. *Journal of National Security Law & Policy* 4, : 233-243

Comscore. 2009. Turkey has seventh largest online audience in Europe. www.comscore.com/Press Events/Press Releases/2009/5/Turkey has Seventh LargestOnline Audience in Europe/(language)/eng-US (accessed May 2, 2014)

Connell, Anne, Tim Palko, and Hasan Yasar. 2013. Cerebro: A platform for collaborative incident response and investigation. Paper presented at the IEEE International Conference, Waltham, MA. November 12-14

Cornish, Paul. 2009. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks, Directorate General External Policies of the Union, European Parliament, http://www.isis-europe.org/pdf/2009_artrel_247_09-02-epstudy-cyberterrorism.pdf (accessed at September 15 2013).

Cornish, Paul, Rex Hughes, and David Livingstone. 2009. *Cyberspace and the national security of the united kingdom: Threats and Responses*. Chatham House, London.

The Cost of Data Breach Study: United States. 2011. Ponemon Research Institute & Symantec Corp. 2012. http://www.symantec.com/about/news/release/article.jsp?prid=20120320_02. (accessed August 21, 2013).

Council of Europe Convention on Cybercrime – Budapest, 23.XI.2001 (ETS No. 185) (2002),http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG (accessed May 23, 2013).

Council of Europe Convention on Cybercrime Explanatory Report, Nov. 8, 2001,http://conventions.coe.int/Treaty/en/Reports/Html/185.htm. (accessed May 24, 2013).

Coyne, Christopher J. and Peter T. Leeson. 2008. Who's to protect cyberspace. *Journal of Law Economy and Policy* 1, : 473-478

Creswell, John W. and Vicki L. Plano Clark. 2007. *Designing and conducting mixed methods research*. Thousand Oaks, CA: Sage Publications

Croteau, A-M., and François Bergeron. 2009. Interorganizational governance of information technology. In Proceedings of 42nd Hawaii international conference on systems sciences, 1-8. Washington, DC: IEEE Computer Society Press

Dahlgren, Peter. 2005. The internet, public spheres, and political communication: Dispersion and deliberation. *Political Communication* 22, no. 2: 147-162.

De Haes, StevenVan Grembergen, Wim. 2009. An exploratory study into IT governance implementations and its impact on Business/IT alignment. *Information Systems Management* 26, no. 2: 123-137,

Deibert, Ronald and Rafal Rohozinski. 2010. Liberation vs. control: The future of cyberspace. *Journal of Democracy* 21, no. 4: 43-57.

Deibert, Ronald J., and Rafal Rohozinski. 2010. Risking security: policies and paradoxes of cyberspace security. *International Political Sociology* 4, no. 1: 15-32.

The Deloitte-NASCIO Cybersecurity Survey. 2010. http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2010.PDF (accessed September 27, 2013)

DeVos, Stephanie A. 2011. Google-NSA alliance: Developing cybersecurity policy at internet speed. *Fordham Intell.Prop.Media & Ent.LJ* 21, : 173.

Diamond, Larry and Marc F. Plattner. 2012. *Liberation technology: Social media and the struggle for democracy*. Washington D.C.: The Johns Hopkins University Press

Dixon, Jeffrey C. 2008. A clash of civilizations? examining liberal-democratic values in turkey and the european Union1. *The British Journal of Sociology* 59, no. 4: 681-708.

Doğan, Nejat. 2006. Human rights and Turkey's bid for EU membership: Will "Fundamental rights of the union" bring fundamental changes to the Turkish constitution and Turkish politics? *Turkish Studies* 7, no. 2: 243-259.

Donahue, J.D., and R.J. Zeckhauser. 2006. Public private collaboration for infrastructure security. In *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, 1st ed. Auerswald, Philip, E., Lewis Branscomb, Todd La Porte and Erwann Michel-Kerjan, 429-456. New York: Cambridge University Press

Douglas, Warfield. 2012. Critical infrastructures: IT security and threats from private sector ownership. *Information Security Journal: A Global Perspective* 21, no. 3: 127-136,

Dourada, Eli. 2012. Is There a Cybersecurity Market Failure? George Mason Univ. Mercatus Ctr., Working Paper No. 12-05. http://mercatus.org/publication/there-cybersecurity-market-failure-0

Dunn-Dunn-Cavelty, Myriam Dunn. 2008. *Cyber-security and threat politics: US efforts to secure the information age*. New York: Routledge.

Dunn-Dunn-Cavelty, Myriam and Manuel Suter. 2009. Public–Private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection* 2, no. 4: 179-187.

Dutton, William H. and Malcolm Peltu. 2007. The emerging internet governance mosaic: Connecting the pieces. Information Polity 12, no. 1: 63-81.

Dynes, Scout, Eric Goetz, and Michael Freeman. 2007. Cyber security: Are economic incentives adequate? In *Critical infrastructure protection, ed.* Goetz, Eric and Sujeet Shenoi, 15-27. New York, NY: Springer

The EastWest Institute Cybersecurity Survey. 2010. http://www.ewi.info/cyber-survey (accessed May 25, 2013)

Elkin-Koren, Niva, and Eli M. Salzberger. 1999. Law and economics in cyberspace. *International Review of Law and Economics* 19. No. 4: 553-581.

Etzioni, Amitai. 2011. Cybersecurity in the private sector. *Issues in Science and Technology* 28, no. 1: 58-62.

Executive Office of the President. 2009 Cyberspace Policy Review: Assuring and Trusted and Resilient Information and Communication Infrastructure. http://www.whitehouse.gov.libproxy.utdallas.edu/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed May 16, 2013).

The Federal Cybersecurity Survey. 2012. http://reports.informationweek.com/abstract/104/8769/government/research-federal-government-cybersecurity-survey.html (accessed September 21, 2013)

Feng, Nan, Harry Jiannan Wang, and Minqiang Li. 2014. A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information Sciences* 256, no. 0: 57-73.

Fleming, H. Matthew and Eric Goldstein. 2014. Evaluating the impact of cybersecurity information sharing on cyber incidents and their consequences. *Social Sciences Research Network*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418357 (accessed May 5, 2014)

Friedman, Thomas L. 2002. *Longitudes and attitudes: Exploring the world after September 11*. New York: Farrar, Strauss and Giroux

Friedman, Allan A. 2013. Cybersecurity and Trade: National Policies, Global and Local Consequences.

http://www.brookings.edu/~/media/research/files/papers/2013/09/19%20cybersecurity%20and%20trade%20global%20local%20friedman/brookingscybersecuritynew.pdf, (accessed at September 10 2013).

Gal-Or, Esther and Anindya Ghose. 2005. The economic incentives for sharing security information. *Information Systems Research* 16, no. 2: 186-208.

Garvey, Paul R., Richard A. Moynihan, and Les Servi. 2013. A macro method for measuring economic-benefit returns on cybersecurity investments: The table top approach. *Systems Engineering* 16, no. 3: 313–328.

Ghernouti-Hélie, Solange. 2010. A national strategy for an effective cybersecurity approach and culture. Paper presented at the ARES International Conference on Availability, Reliability and Security, Krakow. February 15-18

Ghose, Anindya and Uday Rajan. 2006. The economic impact of regulatory information disclosure on information security investments, competition, and social welfare. Paper presented at the Fifth Annual Workshop on Economics and Information Security (WEIS06), Cambridge, UK. June 26-28

Givens, Austen D. and Nathan E. Busch. 2013. Information sharing and public-private partnerships: The impact on homeland security. *Homeland Security Review* 7, no. 2.

Givens, Austen D. and Nathan E. Busch. 2013. Realizing the promise of public-private partnerships in US critical infrastructure protection. *International Journal of Critical Infrastructure Protection* 6, no. 1: 39-50.

Givens, Austen D. and Nathan E. Busch. 2013. Integrating federal approaches to post-cyber incident mitigation. *Journal of Homeland Security and Emergency Management* 10, no. 1: 1–28

Goldsmith, Stephen and William D. Eggers. 2004. *Governing by network: The new shape of the public sector*. Washington, DC: Brookings Institution

Goodyear, Marilu, Holly T. Goerdel, Shannon Portillo, and Linda Williams. 2010. Cybersecurity management in the states: The emerging role of chief information security officers. Washington, D.C: IBM Center for the Business of Government

Gordon, Lawrence A., Martin P. Loeb, and William Lucyshyn. 2003. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* 22, no. 6: 461-485.

Gordon, A. Lawrence and Martin, P. Loeb. 2006. *Managing Cybersecurity Resources: A Cost Benefit Analysis.* New York NY: McGrow Hill

Graubart, Richard, Deborah J. Bodeau, and Jennifer Fabius-Greene. 2010. Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels. Paper presented at the second IEEE International Conference, Minneapolis, MN. August 20-22

Gray, Barbara. 1989. *Collaborating: Finding common ground for multiparty problems*. San Francisco: Jossey-Bass

Grigoriadis, Ioannis N. 2014. The constitutional system of Turkey: 1876 to present. *Southeast European and Black Sea Studies* 14, no. 1: 132-134.

Guitton, Clement. 2013. Cyber insecurity as a national threat: Overreaction from Germany, France and the UK? *European Security* 22, no. 1: 21-35.

Gurkaynak, Gonenc, Ilay Yilmaz, and Nazli Pinar Taskiran. 2013. Governmental efforts and strategies to reinforce security in cyberspace. *International Law Research* 2, no. 1: p185.

Gürkaynak, Gönenç, Ilay Yilmaz, and Nazli Pinar Taskiran. 2014. Protecting the communication: Data protection and security measures under telecommunications regulations in the digital age. *Computer Law & Security Review* 30, no. 2: 179-189.

Hansen, Lene and Helen Nissenbaum. 2009. Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly* 53, no. 4: 1155-1175.

Hardy, Gary. 2006. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report* 11, no. 1: 55-61.

Hare, Forrest B. 2009. Private sector contributions to national cyber security: A preliminary analysis. *Journal of Homeland Security and Emergency Management* 6, no. 1.

Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. 2010. Leaving deterrence behind: War-fighting and national cybersecurity. *Journal of Homeland Security and Emergency Management* 7, no. 1: 1-24

Harknett, Richard J. and James A. Stever. 2011. The new policy world of cybersecurity. *Public Administration Review* 71, no. 3: 455-460.

Harknett, Richard J. and James A. Stever. 2009. The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. *Journal of Homeland Security and Emergency Management* 6, no. 1: 1-14.

Hathaway, Melissa E. and Alexander Klimburg. 2012. Preliminary Considerations: On National Cyber Security. In *National Cyber Security Framework Manual*, ed. Alexander Klimburg, 1-43. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence

Hill, Jonah Force. 2012. *Internet fragmentation: Highlighting the major technical, governance and diplomatic challenges for US policy makers*. Harvard Belfer Center for Science and International Affairs.

Hiller, Janine S. and Roberta S. Russell. 2013. The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review* 29, no. 3: 236-245.

Hocevar, S., Thomas, G. F., and Jansen, E. 2006. Building Collaborative Capacity: An Innovative Strategy for Homeland Security Preparedness. In *Innovation Through Collaboration,* ed. M. M. Beyerlein, D. A. Johnson, and S. T. Beyerlein, 255–274. New York: Elsevier.

Huntington, Samuel P. 2012. *The third wave: Democratization in the late 20th century*. University of Oklahoma Press.

INSA. 2009. Addressing cyber security through public-private partnership: An analises of existing model. http://issuu.com/insalliance/docs/addressing_cyber_security_through_public___private/1(accessed July 25, 2013)

The International Telecommunications Union. 2014. "Definition of Cybersecurity." http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx. (accessed April 1, 2014).

Internet World Stats. 2011. Internet usage in Europe. Internet user statistics & population for 53 European countries and regions. http://www.internetworldstats.com/stats4.htm#europe Accessed 01.02.11.

Irion, Kristina. 2013. The governance of network and information security in the European Union: The European public-private partnership for resilience (EP3R) In *The secure information society: Ethical, legal and political challenges*, ed. Krüger, Jörg, Bertram Nickolay, and Sandro Gaycken, 83-116. London: Springer.

ISACA. 2006. *Information security governance: Guidance for boards of directors and executive management* (2nd ed.). Illinois, IL: IT Governance Institute

James Langevin, Micheal McCaul, Scott Charney, and Harry Raduege, 2008. Securing Cyberspace for the 44th Presidency. *Center for Strategic & International Studies*. http://Csis.org/media/pubs081208_securingcyberspace_44.pdf (accessed January 1, 2014).

Jirasek, Vladimir. 2012. Practical application of information security models. *Information Security Technical Report* 17, no. 1–2: 1-8.

Johnston, C. Allen, and Ron Hale. 2009. Improved security through information security governance. *Communications of the ACM* 52, no. 1: 126-129,

Julisch, Klaus. 2013. Understanding and overcoming cyber security anti-patterns. *Computer Networks* 57, no. 10: 2206-2211.

Kelly, Brian B. 2012. Investing in a centralized cybersecurity infrastructure: Why" hacktivism" can and should influence cybersecurity reform. *Boston University Law Review* 92, no. 5: 1663-1712.

Kemp, Roger L.. 2010. *Homeland security: Best practices for local government*. 2nd ed. Washington, DC: ICMA Press

Kernaghan, Kenneth. 2000. The post-bureaucratic organization and public service values. *International Review of Administrative Sciences* 66, no. 1: 91-104.

Kesan, Jay P. and Carol M. Hayes. 2011. Mitigative counterstriking: Self-defense and deterrence in cyberspace. *Harvard Journal of Law & Technology* 25, no. 2: 417-527

Khansa, Lara and Divakiran Liginlal. 2009. Quantifying the benefits of investing in information security. *Communications of the ACM* 52, no. 11: 113-117,

Khoo, Benjamin, Peter Harris, and Stephen Hartman. 2010. Information security governance of enterprise information systems: An approach to legislative compliant. *International Journal of Management & Information Systems* 14, no. 3.49-55

Klimburg, Alexander. 2011. Mobilising cyber power. *Survival* 53, no. 1: 41-60.

Klimburg, Alexander. 2011. The Whole of Nation in Cyberpower. *Georgetown Journal of International Affairs*, Special Edition http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien /News/The_Whole_of_Nation_in_Cyberpower_AK.pdf (accesed at November 12, 2013)

Klimburg, Alexander. 2012. *National cyber security framework manual. Tallinn:* NATO Cooperative Cyber Defense Center of Excellence

Klimburg, Alexander and Philipp Mirti. 2012. Cyberspace and Governance—A primer. *Oiip Policy Paper*: 9-14.

Koski, Chris. 2013. Does a partnership need partners? assessing partnerships for critical infrastructure protection. *The American Review of Public Administration*: 0275074013494754.

Koski, Chris. 2011. Committed to protection? partnerships in critical infrastructure protection. *Journal of Homeland Security and Emergency Management* 8, no. 1.

Kostyuk, Nadiya. 2013. International and Domestic Challenges to Comprehensive National Cybersecurity: A Case Study of the Czech Republic. *Journal of Strategic Security* 7, no. 1: 68-82.

Kouwenhoven, Vincent. 1993. The rise of the public private partnership: A model for the management of public-private cooperation. In *Modern Governance: New Government.Society Interactions*, ed. Jan Kooiman, 119-130. London: Sage publications

Krahmann, Elke. 2003. Conceptualizing security governance. *Cooperation and Conflict* 38, no. 1: 5-26.

Kramer, Franklin D. Larry, K. Wentz, and Stuart H. Starr. 2009. *Cyberpower and national security*. Washington, DC: Potomac Books, Inc.

Lake, Celinda and Jennifer Sosin. 2002. Public Opinion Polls and Democracy. In *How American Governments Work: A Handbook of City, County, Regional, State, and Federal Operations*, ed. Kemp, L. Roger, 411-429. North Carolina: McFarland Company, Inc.

Levin, Avner, Paul Goodrick, and Daria Ilkina. 2012. Securing cyberspace: A comparative review of strategies worldwide. *The Privacy and Cyber Crime Institute*, http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf (accessed March 22, 2013).

Lewis, James Andrew. 2005. Aux armes, citoyens: Cyber security and regulation in the united states. *Telecommunications Policy* 29, no. 11: 821-830.

Lewis, A. James and Katrina Timlin, 2009. *Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization*, Geneva: UNIDIR

Lewis, James Andrew and Katrina Timlin. 2011. *Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization, Geneva:* UNIDIR.

Lewis, James A. 2009. Sovereignty and the role of government in cyberspace. *Journal of World Affairs* 16, no 2: 55

Lewis, James A.. 2011.Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. *Center for International & Strategic Studies*. http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf (accessed March 28, 2013)

Lewis, W. Arthur. 1965. Beyond African dictatorship, the crisis of the one-party state. In *Democracy online: The prospects for political renewal through the internet*, ed. Shane, M. Peter. New York: Routledge.

Lijphart, Arend. 2012. *Patterns of democracy: Government forms and performance in thirty-six countries.* New York: Yale University Press.

Lord, Kristin M. and Sharp, Travis 2011. *America's Cyber Future: Security and Prosperity in the Information Age*, Volume I, Washington DC: Center for a New American Security.

Luiijf, Ham, Kim Besseling, Maartje Spoelstra, and Patrick de Graaf. 2013. Ten National Cyber Security Strategies: A Comparison. In *Critical Information Infrastructure Security,* ed. Sandro Bologna, Bernhard Hämmerli, Dimitris Gritzalis, and Stephen Wolthusen, 1-17. Berlin: Springer

Luiijf, Eric, Kim Besseling, and Patrick De Graaf. 2013. Nineteen national cyber security strategies. *International Journal of Critical Infrastructures* 9, no. 1: 3-31.

Luthy, David and Karen Forcht. 2006. Laws and regulations affecting information management and frameworks for assessing compliance. *Information Management & Computer Security* 14, no. 2: 155-166.

MacKinnon, Rebecca. 2011. China's" networked authoritarianism". *Journal of Democracy* 22, no. 2: 32-46.

Macmanus, Susan A., Kiki Caruson, and Brian D. McPhee. 2012. Cybersecurity at the local government level: Balancing demands for transparency and privacy rights. *Journal of Urban Affairs* 35, no 4: 451–470.

Madnick, Stuart, Nazli Choucri, and Jeremy Ferwerda. 2014. Institutions for cyber security: International responses and global imperatives. *Information Technology for Development* 20, no. 2: 96-121

Mankin, Don, Susan Cohen, and Stephen P. Fitzgerald. 2004. Developing complex collaboration: Basic principles to guide, design, and implementation. In *Complex*

collaborative: Building the capabilities for working across boundaries, ed. M.M. Beyerlein, D.A. Johnson, and S.T. Beyerlein, 1-26. New York: Elsevier.

Marshall, Gary S. 2007. *A brief tour of public organization theory in the United States. In Democracy and public administration*, .ed. Richard C. Box, New York: M.E. Shape, Inc.

Mattesich, P., M. Murray-Close, and B. Monsey. 2001. *Collaboration: What makes it work–a review of the research literature on factors influencing successful collaboration*. Saint Paul, MN: Amherst H.Wilder Foundation.

May, Peter J. and Chris Koski. 2013. Addressing public risks: Extreme events and critical infrastructures. *Review of Policy Research* 30, no. 2: 139-159.

Mayer-Schoenberger, Viktor and David Lazer. 2007. *Introduction to Governance and information technology: from electronic government to information government*. Cambridge, MA: MIT Press.

McCormick, Gordon H. 2003. Terrorist decision making. *Annual Review of Political Science* 6, no. 1: 473-507.

Mehravari, Nader. 2013. Resilience management through use of CERT-RMM & associated success stories. Paper presented at the IEEE International Conference, Nov 12-14, in Waltham, MA 119 – 125)

Mikkonen, Tomi. 2014. Perceptions of controllers on EU data protection reform: A finnish perspective. *Computer Law & Security Review* 30, no. 2: 190-195.

Mitropoulos, Sarandis, Dimitrios Patsos, and Christos Douligeris. 2006. On incident handling and response: A state-of-the-art approach. *Computers & Security* 25, no. 5: 351-370.

Moore, Mark Harrison. 1995. *Creating public value: Strategic management in government* Cambridge, MA: Harvard University Press.

Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. 2013. Internet security and networked governance in international relations. *International Studies Review* 15, no. 1: 86-104.

Mueller, Milton, John Mathiason, and Hans Klein. 2007. The internet and global governance: Principles and norms for a new regime. *Global Governance: A Review of Multilateralism and International Organizations* 13, no. 2: 237-254.

Muhlberger, Peter. 2004. Access, skill, and motivation in online interaction versus ordinary discussion. In *Democracy online: The prospects for political renewal through the internet*, ed. Shane, M. Peter, 225-239. New York: Routledge.

Murray, Andrew. 2007. *The regulation of cyberspace: Control in the online environment*. New York: Routledge.

Naim, Moises. 2013. *The End of Power: From Boardrooms to Battlefields and Churches to States, Why Being In Charge Isn't What It Used to Be*. New York, NY: Basic Books

Narasimhan, Harikrishna, Venkatanathan Varadarajan, and Pandu Rangan Chandrasekaran. 2010. Towards a cooperative defense model against network security attacks. Paper presented at the annual Workshop on the Economics of Information Security, Cambridge, MA., June 7-8

National Bureau of Economic Research. 2013. *Network security and contagion,* by Acemoglu, Daron, Azarakhsh Malekian, and Asuman Ozdaglar. No. w19174. http://www.nber.org/papers/w19174 (accessed April 5, 2014).

The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust, and Security Online. http://www3.weforum.org/docs/WEF_GITR_TheNewInternet World_Report_2011.pdf (accessed May 25, 2013)

National Computer Security Survey (NCSS). http://www.rand.org/pubs/technical_ reports/TR544.html (accessed September 27, 2013)

National Cyber Incident Response Plan. 2010. http://www.federalnewsradio.com/pdfs/NCIRP_ Interim_Version_September_2010.pdf (accessed September 21, 2013).

National Preparedness Report. 2013. http://www.fema.gov/media-library-data/20130726-1916-25045-0015/npr2013_final.pdf. (accessed September 21, 2013)

Nickolov, Eugene. 2006. Critical information infrastructure protection: Analysis, evaluation and expectations. *Information and Security* 17, : 105.

Nielsen, Suzanne C. 2012. Pursuing security in cyberspace: Strategic and organizational challenges. *Orbis* 56, no. 3: 336-356.

Nissenbaum, Helen. 2004. Privacy as contextual integrity. *Washington Law Review*. 79, : 119.

Nojeim, Gregory T. 2010. Cybersecurity and freedom on the internet. *Journal of National Security Law & Policy* 4, : 119-137

Nye, Joseph S. 2011. *The future of power.* New York, NY: PublicAffairs.

Nye, S. Joseph. 2010. *Cyber Power*. Harvard Kennedy School Belfer Center for Science and International Affairs.

OECD. 2012. *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*. *OECD Digital Economy Papers*, No. 211, OECD Publishing. http://dx.doi.org/10.1787/5k8zq92vdgtl-en (accessed May 26, 2013)

O'Loughlin, John. 2004. Democratic values in a globalizing world: A multilevel analysis of geographic contexts. *Geojournal* 60, no. 1: 3-17.

Ögüt, Hulisi, Srinivasan Raghunathan, and Nirup Menon. 2011. Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis: An International Journal* 31, no. 3: 497-512.

Ozbudun, Ergun. 2011. *The Constitutional System of Turkey: 1876 to Present*. New York: Palgrave Macmillan

Ozer, Nicole. 2012. Putting online privacy above the fold: Building a social movement and creating corporate change. *New York University Review of Law & Social Change* 36, .

Pawlak, Patryk and Cécile Wendling. 2013. Trends in cyberspace: Can governments keep up? *Environment Systems and Decisions* 33, no. 4: 536-543.

Perspective on Preparedness: Taking Stock Since 9/11 Report to Congress of the Local, State, Tribal, and Federal Preparedness Task Force September 2010 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.185.583&rep=rep1&type=pdf. (accessed August 21, 2013).

Posthumus, Shaun and Rossouw Von Solms. 2004. A framework for the governance of information security. *Computers & Security* 23, no. 8: 638-646.

Powell, Benjamin. 2005. Is cyberspace a public good-evidence from the financial services industry. *JL Econ.& Pol'y* 1, : 497.

Prieto, Daniel B. and Steven Bucci. 2010. *Meeting the Cybersecurity Challenge: Empowering Stakeholders and Ensuring Coordination.* New York, NY: The Center for The Business of Government

The PwC Global State of Information Security Survey. 2013. http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf (accessed September 27, 2013)

The PwC State of Cybercrime Survey. 2013. http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/us-state-of-cybercrime.pdf (accessed May 27, 2013)

Quey-Jen, Yeh, and Arthur Jung-Ting Chang. 2007. Threats and countermeasures for information system security: A cross-industry study. *Information & Management* 44, no. 5: 480-491.

Quigley, Kevin and Jeffrey Roy. 2012. Cyber-security and risk management in an interoperable world an examination of governmental action in North America. *Social Science Computer Review* 30, no. 1: 83-94.

Quigley, Kevin. Calvin Burns, and Kristen Stallard. 2013. Communicating effectively about cyber-security risks: Probabilities, peer networks and a longer term education program http://cip.management.dal.ca/wp-content/uploads/2013/04/Quigley-Burns-Stallard-Cyber-Security-Paper-Final-1.pdf, (accessed at November 5)

Rainey, Hal G. and Barry Bozeman. 2000. Comparing public and private organizations: Empirical research and the power of the A priori. *Journal of Public Administration Research & Theory* 10, no. 2: 447-470

Ransbotham, Sam and Sabyasachi Mitra. 2009. Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research* 20, no. 1: 121-139.

Reputation Impact of a Data Breach: U.S. Study of Executives & Managers, Ponemon Research Institute & Experian Corp., Nov. 2011, http://www.experian.com/blogs/data-breach/2012/01/17/how-data-breachesharm-reputations/.(accessed August 11, 2013).

Rhodes, Roderick Arthur William. 1996. The new governance: Governing without government1. *Political Studies* 44, no. 4: 652-667.

Robinson, Neil, Luke Gribbon, Veronika Horvath, Kate Robertson. 2013. *Cyber-security threat characterization: A rapid comparative analysis*. Santa Monica, CA: Rand Corparation

Robles, Rosslin John, Na-Yun Kim, and TH Kim. 2008. IT security governance for e-business. International Journal of Software Engineering and its Applications 2, : 99-106.

Rogers, Everett M. 2003. *Diffusion of innovations*. 5th ed. New York, NY: Free Press

Rosenzweig, Paul. 2010. The organization of the united states government and private sector for achieving cyber deterrence. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council. 245-279. Washington, DC: The National Academies Press

Rowe, Brent R. and Michael P. Gallaher. 2006. Private sector cyber security investment strategies: An empirical analysis. Paper presented at the Fifth Workshop on the Economics of Information Security, Cambridge, UK. June 26-28.

Sales, Nathan, Alexander. 2013. Regulating Cyber-Security. *Northwestern University Law Review* 107, no. 4: 1503-1568

Sayre, W. 1997.Premises of public administration: Past and emerging. In J. M. Shafritz and A. C. Hyde (eds.), *Classics of Public Administration*. Oak Park, Ill.: Moore.

Schmitt, Michael N. 1999. Computer network attack and the use of force in international law: Thoughts on a normative framework. *Columbia Journal of Transnational Law* 37, : 1998-1999.

Scully, Tim. 2014. The cyber security threat stops in the boardroom. *Journal of Business Continuity & Emergency Planning* 7, no. 2: 138-148.

Seckinelgin, Hakan. 2004. Contractions of Sociocultural Reflex: Civil Society in Turkey. In *Exploring Civil Society: Political and Cultural Contexts*, ed. Marlies Glasius, David Lewis, and Hakan Seckinelgin, 173-180. New York NY: Routledge

Selvi, Kiymet. 2006. Developing a teacher trainees democratic values scale: Validity and reliability analyses. *Social Behavior and Personality: An International Journal* 34, no. 9: 1171-1178.

Shackelford, Scott J. 2012. In search of cyber peace: A response to the cybersecurity act of 2012. *Stanford Law Review Online* 64, : 106.

Shackelford J. Scott and Amanda N. Craig. 2014. Beyond the new "digital divide": Analyzing the evolving role of national governments in internet governance and enhancing cybersecurity. *Stanford Journal of International Law* 50, no. 1: 119-184,

Shane, Peter M. 2004. *Democracy online: The prospects for political renewal through the internet*. New York: Routledge.

Shore, Malcolm, Yi Du, and Sherali Zeadally. 2011. A Public-Private partnership model for national cybersecurity. *Policy & Internet* 3, no. 2: 1-23.

Singleton, Royce A., and Bruce C. Straits .2010. *Approaches to Social Research*. 4th Ed. New York: Oxford University Press.

Skelcher, Chris and Jacob Torfing. 2010. Improving democratic governance through institutional design: Civic participation and democratic ownership in Europe. *Regulation & Governance* 4, no. 1: 71-91.

Skopik, Florian, Zhendong Ma, Paul Smith, and Thomas Bleier. 2012. Designing a cyber attack information system for national situational awareness. In *Future security*, Nils Aschenbruck, Peter Martini, Michael Meier, and Jens Tölle, 277-288. Berlin Heidelberg: Springer

Smedinghoff, Thomas J. 2003. The developing US legal standard for cybersecurity. *Sedona Conference Journal* 4. 109-120

Smith, Bruce P. 2005. Hacking, poaching, and counterattacking: Digital counterstrikes and the contours of self-help. *JL Econ.& Pol'y* 1, : 171.

Smith, Stephen, Donald Winchester, Deborah Bunker, and Rodger Jamieson. 2010. Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Quarterly* 34, no. 3: 463-486.

Solove, Daniel J. 2006. *The digital person: Technology and privacy in the information age*. New York: NYU Press

Sommer, Peter and Ian Brown. 2011. Reducing systemic cybersecurity risk. *Organisation for Economic Cooperation and Development Working Paper no.IFP/WKP/FGS (2011)* 3, .

Sozen, Süleyman and Ian Shaw. 2003. Turkey and the european union: Modernizing a traditional state? *Social Policy & Administration* 37, no. 2: 108-120.

Sørensen E, Torfing J. 2007. *Theories of Democratic Network Governance*. Basingstoke: Palgrave Macmillan

Stavridis, James and Evelyn N. Farkas. 2012. The 21st century force multiplier: Public–Private collaboration. *The Washington Quarterly* 35, no. 2: 7-20.

Stivers, Camilla. 2000. Resisting the ascendancy of public management: Normative theory and public administration. *Administrative Theory and Praxis* 22, no. 1: 10-23

Straub, W. Detmar, Hsu, Carol, and Jae-Nam Lee. 2012. Institutional influences on information systems security innovations. *Information Systems Research* 23, no. 3-part-2: 918-939.

Straub, W. Detmar, Seymour Goodman, and Richard L. Baskerville. 2008. Framing the information security process in modern society. In *Information Security: Policy, Processes and Practices*, ed. Detmar W. Straub, Seymour E. Goodman, Richard Baskerville, 5–12. New York, NY: M. E. Sharpe

Tanaka, Hideyuki, Kanta Matsuura, and Osamu Sudoh. 2005. Vulnerability and information security investment: An empirical analysis of e-local government in japan. *Journal of Accounting and Public Policy* 24, no. 1: 37-59.

Thierer, Adam. 2013. Privacy, security, and human dignity in the digital age: The pursuit of privacy in a world where information control is failing. *Harvard Journal of Law & Public Policy* 36, no. 2: 410-454.

Thomas, Gail F., Susan P. Hocevar, and Erik Jansen. 2006. *A Diagnostic Approach to Building Collaborative Capacity in an Interagency Context*.

Thomas, N. Rachel. 2013. Securing Cyberspace through public-private partnerships: A Comparative Analysis of Partnership Models, *Center for Strategic and International Studies*.http://csis.org/publication/securing-cyberspace-through-public-private-partnerships (accessed at February 12, 2014)

Thompson, K. Karson. 2011. Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate. *Texas Law Review* 90, no. 2: 465-495

Trim, Peter and David Upton. 2013. *Cyber security culture: Counteracting cyber threats through organizational learning and training.* Brookfield, VT: Gower Publishing Co.

UK fights cybercrime. 2012. *Computer Fraud & Security* 2012, no. 2: 1-3.

United States Government, Accountability Office and Accountability Office United States Government. 2013. *Cybersecurity : National strategy, roles, and responsibilities need to be better defined and more effectively implemented : Report to congressional addressees*.

Uroš, Svete. 2012. European e-readiness? cyber dimension of national security policies. *Journal of Comparative Politics* 5, no. 1: 38-59

U.S. Chamber of Commerce. 2011. *Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper*, https://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf (accessed May 25, 2013)

U.S. Department of Homeland Security. 2010. Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland 2010. Prepared by Department of Homeland Security. Washington, DC: Government Printing Office

U.S. Department of Homeland Security. 2011. Blueprint for a Secure Cyber Future: Cybersecurity Strategy for the Homeland Security Enterprise 2011. Prepared by Department of Homeland Security. Washington, DC: Government Printing Office

U.S. Government Accountability Office. Critical infrastructure protection: Key private and public cyber expectations need to be consistently addressed, by Cathleen A. Berrick. GAO-10-628. 2010. http://www.gao.gov/new.items/d10628.pdf (accessed May 1, 2013).

U.S. Government Accountability Office. Cybersecurity: Challenges in Securing the Electricity Grid, GAO-12-926T, 2012, http://www.gao.gov/assets/600/592508.pdf (accessed May 20, 2013).

U.S. Department of Homeland Security. 2006. National Infrastructure Protection Plan. Washingon, DC: U.S. Government Printing Office

U.S. Government Accountability Office. 2009. *Key Improvements Are Needed to Strengthen the Nation's Posture*, by David Powner. GAO-09-432T. 2009. http://www.gao.gov/new.items/d09432t.pdf (accessed May 15, 2013).

U.S. Government Accountability Office. 2010. *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative,* GAO-10-338. http://www.gao.gov/assets/310/301459.pdf (accessed March 1, 2014).

U.S. Government Accountability Office. 2010. *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed,* GAO-11-24. http://www.gao.gov/assets/320/310967.pdf (accessed April 1, 2013).

Von Solms, Basie. 2006. Information security–the fourth wave. *Computers & Security* 25, no. 3: 165-168.

Von Solms, Basie. 2005. Information security governance: COBIT or ISO 17799 or both? *Computers & Security* 24, no. 2: 99-104.

Von Solms, Basie and Rossouw Von Solms. 2004. The 10 deadly sins of information security management. *Computers & Security* 23, no. 5: 371-376.

Von Solms, Rossouw and Johan van Niekerk. 2013. From information security to cyber security. *Computers & Security* 38, no. 0: 97-102.

Warner, Danielle. 2012. From bombs and bullets to botnets and bytes: Cyber war and the need for a federal cybersecurity agency. *S.Cal.L.Rev.* 85, : 1A-1643.

Weill, Peter and Jeanne W. Ross. 2004. *IT governance: How top performers manage IT decision rights for superior results*. Boston, MA: Harvard Business School Press.

Weill, Peter and Jeanne Ross. 2005. A matrixed approach to designing IT governance. *MIT Sloan Management Review* 46, no. 2: 26-34.

Werlinger, Rodrigo, Kasia Muldner, Kirstie Hawkey, and Konstantin Beznosov. 2010. Preparation, detection, and analysis: The diagnostic work of IT security incident response. *Information Management & Computer Security* 18, no. 1: 26-42.

White House. 2010. *National Security Strategy.* Washington, DC: U.S. Government Printing Office

White House. 2011. *Presidential Policy Directive 8 on National Preparedness*. Washington, DC: U.S. Government Printing Office

White House. 2008. *Presidential Policy Directive 54 on Cybersecurity Policy.* Washington, DC: U.S. Government Printing Office

White House 2011. *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*. Washingon, DC: U.S. Government Printing Office

Wilson, James Q. 2000. *Bureaucracy: What government agencies do and why they do it*. New York: Basic Books, Inc.

Yavuz, Devrim Adam. 2012. Capital, the state and democratization: The case of Turkish industry. *Sociology* 46, no. 3: 507-522.

Zarvić, Novica, Carl Stolze, Matthias Boehm, and Oliver Thomas. 2012. Dependency-based IT governance practices in inter-organisational collaborations: A graph-driven elaboration. *International Journal of Information Management* 32, no. 6: 541-549.

VITA

Gokhan Ikitemur was born in Istanbul, Turkey in 1979. After graduating from Ankara University Faculty of Political Sciences with a Bachelor of Arts degree 2001, he entered the Turkish Ministry of Interior as candidate district governor in the same year. In 2004, he entered Exeter University, United Kingdom, and graduated in 2005 with a Master of International Relations degree. From 2003 to 2011, he worked for the Turkish Ministry of Interior as district governor and deputy provincial governor in different parts of Turkey.