



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

Master's Thesis

**Restructuring the National  
Cybersecurity Governance System  
in South Korea**  
**- Critical Information Infrastructure -**

우리나라 국가 사이버안보 거버넌스  
체계의 재구조화 방안에 관한 연구

**August 2019**

**Graduate School of International Studies  
Seoul National University  
International Commerce Major**

**Do Kyung KIM**

# **Restructuring the National Cybersecurity Governance System in South Korea**

**- Critical Information Infrastructure -**

**Sheen Seoung Ho**

**Submitting a master's thesis of International  
Studies**

**August 2019**

**Graduate School of International Studies  
Seoul National University  
International Commerce Major**

**Confirming the master's thesis written by**

**Do Kyung KIM**

**August 2019**

Chair Sheen Seoung Ho (Seal)

Vice Chair Han Jung Hoon (Seal)

Examiner Kim Tae Kyoon (Seal)

## **Abstract**

*Korea's national cybersecurity governance system is characterized by high levels of fragmentation and instability, unable to form coherent national-level response to increasingly sophisticated and devastating cyber attacks, with the public, private and military sector each struggling to provide for its own cybersecurity. The purpose of this paper is to analyze the contemporary situation and underlying problems of South Korea's national cybersecurity in the area of critical information infrastructure from the governance perspective, then suggest relevant policy measures to bolster cybersecurity of critical information infrastructure. In order to fulfill the objective, this paper first examines the theories pertinent to the concept and emergence of the governance perspective in the disciplines of social science. Then, the components of governance and the requirements for successful governance are explored in order to establish the dimensions of analysis. Subsequently, the paper undertakes a case-study of the U.S. cybersecurity governance system to draw relevant policy implications. The following chapter examines the contemporary situation and underlying problems of South Korea's cybersecurity governance, in accordance with the five dimensions of the governance system. This paper concludes with policy suggestions to consolidate stable and sustainable cybersecurity governance system in Korea.*

**KEYWORDS:** cybersecurity, governance, critical information infrastructure, cyber attack, South Korea

**Student Number:** 2017-29595

# Contents

## List of Figures and Tables`

## Abbreviations

## CHAPTER I. Introduction

1.1 Research Background .....	1
1.2 Research Purpose and Research Questions.....	5

## CHAPTER II. Theoretical Underpinning and Research Design

2.1 Theoretical Underpinning.....	8
1) Cybersecurity.....	8
2) Critical Infrastructure or Critical National Infrastructure.....	9
3) Critical Information Infrastructure.....	11
4) Emergence of Governance Perspective.....	12
5) Conceptualizing Governance.....	14
6) Governance Capacity and Good Governance.....	17
7) Conditions for Governance Formation.....	18
8) Requirements for Successful Governance.....	19
2.2. Literature Review.....	22
1) Literatures on Regional and Global Cybersecurity Governance.....	22
2) Literatures on Cybersecurity Governance in South Korea.....	24

3) Common Limitations of Precedent Studies.....	27
2.3 Research Method: Document Research and Case Study.....	28
2.4 Rationale for U.S. Cybersecurity Governance as Case Study.....	32
2.5 Dimensions of Analysis.....	33

**CHAPTER III. The Cybersecurity Governance System of the United States**

3.1 An Overview of Cybersecurity Legislation and Policies in the U.S.....	35
3.2 Legal and Institutional Systems: Roles and Responsibilities.....	43
3.3 Federal Cybersecurity Budget.....	45
3.4 Public-Private Partnership: Critical Infrastructure Sector Partnership..	47
3.5 Federal Cybersecurity Monitoring and Evaluation Systems.....	51

**CHAPTER IV.**

**An Analysis of South Korea’s National Cybersecurity Governance System on Critical Information Infrastructure**

4.1 An Overview of South Korea’s National Cybersecurity Challenges.....	53
4.2 An Analysis of the Cybersecurity Governance System of South Korea..	57
1) Legal and Institutional Systems.....	57
2) Administrative System for Critical Information Infrastructure.....	67
3) Finance and Budget Systems.....	76
4) Public-Private Partnership.....	79
5) Monitoring and Evaluation Systems.....	81

**CHAPTER V.**

**Policy Measures to Consolidate the National Cybersecurity Governance**

**System in South Korea**

5.1 Policy Suggestions to Consolidate the Cybersecurity Governance System

- 1) Legal and Institutional Systems..... 84
- 2) Administrative System..... 86
- 3) Finance and Budget Systems..... 90
- 4) Public-Private Partnership..... 92
- 5) Monitoring and Evaluation Systems..... 95

5.2 Engineering Cyber Resilient Governance..... 101

**CHAPTER VI. Conclusion**

6.1 Conclusion and Implications ..... 105

6.2. Future Avenues of Research..... 109

Bibliography..... 110

# List of Figures and Tables

## Figures

**Figure 2-1** Critical Information Infrastructure and Critical Infrastructure

**Figure 2-2** Dimensions of Governance

**Figure 3-1** Sequential Interaction Between Key Agencies

**Figure 3-2** Federal IT Spending and Cybersecurity Spending FY 2011-2020

**Figure 3-3** U.S. Public-Private Partnership Management Structure in the DHS

**Figure 4-1** Laws on Cybersecurity in Korea

**Figure 4-2** Relevant Agencies Responsible for National Cybersecurity in Korea

**Figure 4-3** Management System of the Critical Information Infrastructure Protection

## Tables

**Table 2-1** Dimensions of Analysis

**Table 3-1** Sixteen Critical Infrastructure Sectors in the United States

**Table 4-1** List of North Korea's Major Cyber Attacks Against South Korea

**Table 4-2** Nine Critical Infrastructure Sectors in South Korea

**Table 4-3** Specific Items of Information Protection Budget 2018

**Table 4-4** Information Protection Budget of Korea (2015-2019)

**Table 5-1** Comparison of Cybersecurity and Cyber Resilience

## Abbreviations

CAA	Central Administrative Agency
CDA	Critical Digital Assets
CERT	Cyber Emergency Response Team
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CISA	Cybersecurity Information Sharing Act
CISA	Cybersecurity and Infrastructure Security Agency
CNCI	Comprehensive National Cybersecurity Initiative
CRR	Cyber Resilience Review
DHS	Department of Homeland Security
DOD	Department of Defense
EFTA	Electronic Financial Transaction Act
FBI	Federal Bureau of Investigation
FSC	Financial Services Commission
FISMA	Federal Information Security Modernization Act

GCC	Government Coordinating Councils
GSA	General Services Administration
ICT	Information and Telecommunication Technologies
ISAO	Information Sharing and Analysis Organization
KHNO	Korea Hydro and Nuclear Power
KIICA	Korean IT International Cooperation Agency
KISA	Korea Information Security Agency
KINAC	Korea Institute for Non-proliferation and Control
KrCERT/CC	Korea Computer Emergency Response Team Coordination Center
MA	Management Agency
MSIP	Ministry of Science, Information and Communications Technology and Future Planning
NCI	National Critical Infrastructures
NCS	National Cyber Strategy
NCSC	National Cyber Security Centre
NIDA	National Internet Development Agency
NIPP	National Infrastructure Protection Plan
NIS	National Intelligence Service
NIST	National Institute of Standards and Technology

NSA	National Security Agency
NSRI	National Security Research Institute
NRMC	National Risk Management Center
OMB	Office of Management and Budget
PDD	Presidential Decision Directive
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SSA	Sector-Specific Agencies

# CHAPTER I

## Introduction

### 1.1 Research Background

#### *Contemporary Cyber Threat Landscape*

National security can no longer be isolated from cybersecurity, with almost all modern services heavily dependent on digitalized modes. In terms of the range and scope of potential ramifications, cyber attacks currently outstrip the risk of physical attacks.<sup>1</sup> Cyber attacks affect both the economic and political stability of a state, as the range of cyber crimes have multiplied from cyber espionage, targeting of major critical infrastructures and services such as the electric-grid and banking services, to destructive military grade weapon, such as Stuxnet, a malicious computer worm which destroyed the development of Iranian nuclear facilities in 2010.<sup>2</sup> They also pose a significant threat to the future trajectory of democracies, as experienced during the 2016 U.S. presidential elections. The frequency of cyber attacks has also been on the rise, as resorting to cyber weapons, unlike traditional forms of military weapons, possess low barrier to entry, low risk of potential retaliation, and advantage of relative anonymity of the attacker.<sup>3</sup>

---

<sup>1</sup> Anthony Craig and Brandon Valeriano, "Conceptualising Cyber Arms Races," *International Conference on Cyber Conflict* 8, no. 5 (2016):141-158.

<sup>2</sup> James Farrell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War." *Survival* 53, no. 1 (2011): 23-40.

<sup>3</sup> Valeriano, Brandon, and Ryan Maness, *Cyber war versus cyber realities: Cyber conflict in the international system* (London: Oxford University Press, 2015).

Critical Infrastructures (CI) are specific infrastructures which possess significant national importance, as they underpin the wellbeing a country's population and economy. Deliberate or inadvertent disturbance to CI can wreak havoc on national economy, and potentially provoke national security ramifications. In the recent decades, increased utilization of Information and Telecommunication Technologies (ICT) to monitor and manage CI has contributed to operational efficiencies; however, rising dependency on ICT has heightened vulnerability to cyber attacks.

In the context of South Korea, heavy reliance on ICT in the wide range of CI sectors, renders it particularly prone to potential disturbances to continuous CI functioning. Considering the recent atmosphere of abating diplomatic tensions between South and North Korea, North Korea is unlikely to launch physical attacks on the South by sea, air or land. Nonetheless, regardless of the reconciliatory geopolitical climate, North Korea's attacks in cyberspace continues to expand.<sup>4</sup> Previously, North Korea's intention of launching cyber attacks sought to extract military information from Korea. Recently, amidst international sanctions on North Korea to deter further nuclear development, it has shifted its focus of cyber attacks on targeting financial service sectors to seek alternative sources of funding for its nuclear development. The estimated financial losses from North Korea's cyber attacks on crypto-currency exchange between 2015-2018 is 100 billion won, yet Korea has been unable to undertake effective countermeasures against North Korea's

---

<sup>4</sup> Timothy Martin, "North Korea While Professing Peace Escalated Cyber attacks on South," *Wall Street Journal*, May 25 2018, accessed February 10 2019, <https://www.wsj.com/articles/north-korea-while-professing-peace-escalated-cyberattacks-on-south-1527239057>.

increasing frequency of cyber attacks.<sup>5</sup> There exist significant barriers to active response to North Korea's cyber attacks. Korea possesses asymmetric weakness compared to North Korea in the realm of cyber space, as Korea's dependence on cyber infrastructure is much greater than that of North Korea's, rendering it more vulnerable to cyber attacks. Furthermore, Korea currently lacks information infrastructure to launch effective retaliatory cyber attacks on North Korea, and should such means be acquired, there is a possibility of such retaliatory action escalating into a physical war.

### ***International Legal Vacuum in Tackling Cyber Breaches***

Cyber threats are destabilizing forces in international security, yet the speed of technological advances continuously outpaces the international legal and policy developments. Currently, there is an absence of an overarching international legal framework to provide effective legal remedies for cyber breaches occurring at an international level. This is largely due to challenges in accurately identifying the perpetrator. Under the existing international legal framework, for a state to be held responsible for a particular act, the act must be attributable to the state concerned. Regarding cyber attacks however, states covertly operate through non-state actors, and frequently employ proxies, rendering it challenging to establish legal attribution required to hold states responsible for cyber breaches.<sup>6</sup> Furthermore, should legal

---

<sup>5</sup> Won Byung Chul, "The Reality of Cybersecurity in Korea by Four Cybersecurity Experts," *Boan News*, November 12 2018, accessed February 10, 2019, <https://www.boannews.com/media/view>

<sup>6</sup> Hathaway, Oona, Rebecca Crootof, Philip Levitz, and Haley Nix, "The law of cyber-attack," *California Law Review* 100 (2012): 817.

attribution be successfully established, the international law currently lacks mechanisms to allow effective response to a cyber attack, as the state's use of force is limited to self-defense in response to an armed attack, which concerns the gravest use of physical force.<sup>7</sup> In the same vein, countermeasures under specific circumstances may be a viable option under the international law, yet, the lengthy procedural requirements are deemed impractical in expedient response to impending cyber attacks.

### ***Need for a Coherent Cybersecurity Governance***

In coping with such reality, well coordinated national cybersecurity governance is critical, and the increasing government expenditures allocated specifically towards cybersecurity across major Western powers is evidence of their current efforts.<sup>8</sup> Currently, Korea's cybersecurity governance remains highly fragmented, unable to form coherent national-level response to increasingly sophisticated and devastating cyber attacks, with the public, private and military entities each struggling to provide for its own cybersecurity. It is imperative to note that the provision of national-level cybersecurity depends on forming strong partnerships between the public and private entities overall, as the private entities possess greater expertise on cybersecurity.

---

<sup>7</sup> Michael Schmitt, *Tallinn manual on the international law applicable to cyber warfare*, (London: Cambridge University Press, 2013): 45.

<sup>8</sup> Steve Morgan, "Worldwide cybersecurity spending increasing to \$170 billion by 2020," *Forbes* March 3 2016, accessed February 12, 2019, <https://www.forbes.com/sites/stevemorgan/2016/03/09/>

## **1.2 Research Purpose and Research Questions**

Against this backdrop, the purpose of this paper is to analyze the contemporary situation and underlying problems of South Korea's national cybersecurity in the area of critical information infrastructure from the governance perspective, then suggest relevant policy measures to tackle the possible cyber attacks upon critical information infrastructure. In the process of analysis, the case study on the cybersecurity governance system of the United States is undertaken as an instrument of benchmarking to attain some policy implications from the experiences of advanced countries. To this end, the paper first examines the theories relating to the concept and emergence of the governance perspective in the disciplines of social science. Then, the components of governance and the requirements for successful governance are explored in order to establish the dimensions of analysis. The following chapters undertake a case study on the cybersecurity governance system of the U.S., which is generally regarded as a leading country in responding to serious cyber attacks, and conduct empirical investigations into the contemporary situation and underlying problems in South Korea's cybersecurity governance. This paper finalizes the chapters by suggesting some policy measures to consolidate a stable and sustainable cybersecurity governance system for critical information infrastructures.

With regard to the more detailed structure of the paper, the following chapter on theoretical underpinnings and research design introduces key concepts referred to throughout the paper, expounds upon the adoption of qualitative document analysis for research methodology, outlines the dimensions of analysis, and conducts literature review. The literature review is divided into two specific themes: the first theme

intends to grasp how existing literatures understand the cybersecurity governance in regional and global context, whereas the second theme reviews the researches on more specific national cybersecurity governance in South Korea. The next chapter conducts a case-study into the cybersecurity governance in the U.S., to draw policy implications in the context of Korea. The consecutive chapter, delves into the contemporary situation and underlying problems in Korea's cybersecurity governance. Subsequently, the paper suggests constructive and specific policy recommendations to bolster national cybersecurity governance in Korea in accordance with the elements of good governance. The final chapter acknowledges some limitations of this paper, and suggests avenues for further research, then, concludes by summing up the research findings and implications.

To accomplish the above-mentioned research plans, this paper strives to answer the following research questions:

- Why is the adoption of the governance perspective appropriate in analysing the cybersecurity governance system of critical information infrastructure?
- What are the specific components of the governance system and which requirements should be satisfied to be considered a good and successful governance?
- How does the cybersecurity governance system of the United States, including its institutions, policies, and public-private partnerships, operate in practice and what policy implications can be drawn from the case study of the United States?

- What are the contemporary situation and underlying problems of South Korea's national cybersecurity governance system regarding critical information infrastructure, in terms of the components of and requirements for the successful governance system?
- What policy measures should be pursued to consolidate the national cybersecurity governance system in South Korea?

# CHAPTER II

## Theoretical Underpinning and Research Design

### 2.1 Theoretical Underpinning

This section seeks to provide a definitional account of key terms or concepts that will be utilized throughout the paper: cybersecurity, national critical infrastructure, critical information infrastructure, governance, and good governance.

#### 1) Cybersecurity

In defining cyber security, the Oxford Dictionaries defines cybersecurity as “the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.”<sup>9</sup> The NIST refers to cybersecurity as “the ability to protect or defend the use of cyberspace from cyber attacks”, and the cyber space is more specifically defined as “a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”<sup>10</sup> On the other hand, the International Telecommunications Union (ITU) prescribes the following as cybersecurity, “the

---

<sup>9</sup> Stevenson, Angus, and Maurice Waite, eds. *Concise Oxford English Dictionary: Book & CD-ROM Set* (London: Oxford University Press, 2011).

<sup>10</sup> Richard Kissel, “Glossary of Key Information Security Terms,” *National Institute of Standard and Technology*, 2013 DoC. USA. <http://nvlpubs.nist.gov/nistpubs/ir2013/NIST.IR.7298R2.pdf>

collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be utilized to protect the cyber environment and organization and user's assets.”<sup>11</sup> However, since cybersecurity for the purpose of this paper seeks to incorporate the governance aspect, the definition offered by Schutz et, al. as “the governance, development, management and use of information security, OT security, and IT security tools and techniques for achieving regulatory compliance, defending assets and compromising the assets of adversaries” is deemed more relevant.<sup>12</sup>

## **2) Critical Infrastructure or Critical National Infrastructure**

Reference to the term “critical infrastructure” initially began during 1990s, and since 1996, the U.S. has adopted comprehensive infrastructure protection program. Nonetheless, it was not until the beginning of the 2000, until the term and the concept garnered more widespread attention, when Y2K or millennium Bug posed threat to computer systems across the globe, along with 9/11 Terrorist Attack in 2001 in the U.S. In 2002, the U.S. Department of Homeland Security was established, and signified American government's dedication to incorporate threats to essential infrastructures to comprehensively promote national security.<sup>13</sup>

---

<sup>11</sup> Overview of cybersecurity, ITU-T X.1205

<sup>12</sup> Daniel Schatz, Rabih Bashroush, and Julie Wall, "Towards a More Representative Definition of Cyber Security," *Journal of Digital Forensics, Security and Law* 12, No. 2, Article 8 (2017).

<sup>13</sup> Randvanosky and McDougall, *Critical infrastructure: Homeland security and emergency preparedness*, 4<sup>th</sup> ed, (Florida: CRC Press, 2016):74-77.

Critical Infrastructure or Critical National Infrastructure refers to physical, nonphysical and cyber resources or assets and systems which are deemed imperative to the maintenance of governmental, social and economic functions of a country. According to section 1016(e) of the USA Patriot Act of 2001, Critical Infrastructure is defined as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”<sup>14</sup>

Of the various types of infrastructures designated as “critical national infrastructures”, the 2013 National Infrastructure Protection Plan (NIPP) of DHS distinguishes between commercial infrastructures and public infrastructures. The former includes telecommunication infrastructure and systems, healthcare systems, water supply and treatment management, energy production and electricity generation, food and agriculture, information technology and financial services, and the latter includes security services from the police and military, transportation infrastructures including roads and ports, utility infrastructures such as the electric power grid and telecommunications lines, and government facilities.<sup>15</sup>

---

<sup>14</sup> 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).

<sup>15</sup> Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*, (Washington, DC: Department of Homeland Security, 2013).

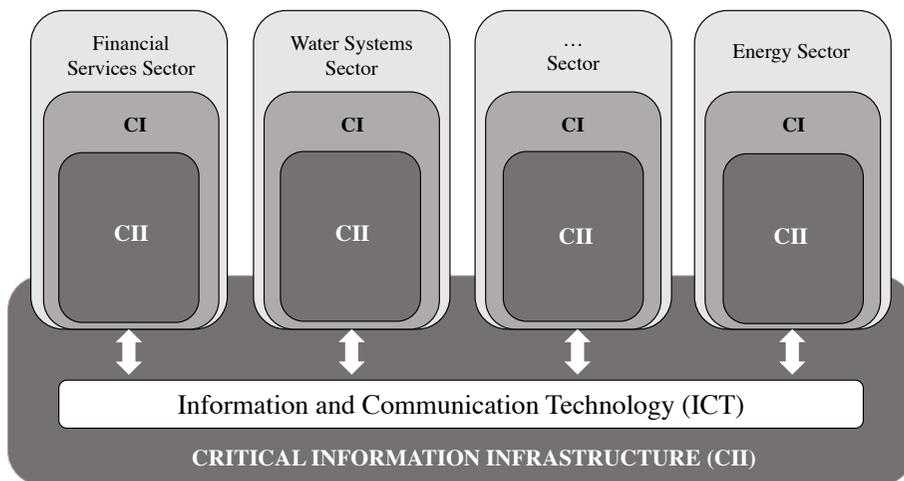
### **3) Critical Information Infrastructure**

Critical Infrastructures ought to be distinguished from Critical Information Infrastructures (CII), albeit the two concepts are interrelated. DHS defines CII as “any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice or video that is: (1) vital to the functioning of critical infrastructure; (2) So vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, national economic security, or national public health or safety; or (3) Owned or operated by or on behalf of a State, local, tribal, or territorial government entity.”<sup>16</sup> More generally, CII is interconnected information system and networks which support key assets and services within critical national infrastructures. Therefore, critical Infrastructure is a broader concept which encompasses all CII, whereas CII does not refer to all critical infrastructures (see Figure 2-1). Although critical infrastructure could fail due to various reasons such as natural catastrophe,

---

<sup>16</sup> Adapted from Cyber Legislative Proposal: Blueprint for a secure cyber future, (DHS, Nov 2011), Accessed <https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf>.

CII fails are primarily caused by cyber-related threats, thereby focusing more on technology.



Source: European Union Agency for Network and Information Security

**Figure 2-1** Critical Information Infrastructure and Critical Infrastructure

#### 4) Emergence of Governance Perspective

Governance is a means to achieve efficiency and democracy simultaneously by engaging various actors in the process of public service delivery through a horizontal network, breaking away from existing single, government-centered operation in solving public problems. Governance has emerged under the need to establish a new relationship between the government, market, and civil society to overcome ungovernability crisis, and replaces the concept of government, which seeks to separate the public and private sectors and approaches problem-solving in a

hierarchical manner. Therefore, governance is utilized when interdependent actors such as governments, markets and civil society, operate in a horizontal and autonomous network, based on partnerships.<sup>17</sup>

More specifically, in the process of state-power division, which gave rise to de-nationalization, the relationship and partnership among various actors of the state, market and civil society were emphasized. In particular, the governance perspective was activated as a solution to aggregate emerging civil society's desire to participate in public decision-making. Furthermore, the progression of political democratization has rendered it challenging for the government to impose unilateral adjustment of interests. Accordingly, the desire for civil society to freely resolve conflicts and reach social consensus, necessitated participatory governing system. On top of this, the spread of neoliberalist society and globalization rolled back the state's traditional roles, reinforced the role of markets and civil society, and promoted globalization networks through the emergence of international civil society. The advances in information services, expansion of networks facilitated participation through information services, and emerging discussion of government reforms, such as the New Public Management theory discarded the hierarchical system, placing emphasis on competition, autonomy, and responsibility. In addition, the necessity of expertise in the private sector due to increased sophistication of government work, the need to adapt to the private sector, and the need to utilize private resources activated

---

<sup>17</sup> Klijn Erik-Hans. "New public management and governance: a comparison." *Oxford handbook of governance* (2012): 201-214.

governance perspective that incorporates the following elements of openness, communication, distribution and cooperation.

### **5) Conceptualizing Governance**

In conceptualizing governance, Rhodes defines it as a “network of public sector, private sector and volunteer organizations in policy making and delivery of service.”<sup>18</sup> Governance calls for a change in the role of traditional dominant state to a minimum state. It is a form of new public management which involves introducing market efficiency to the public sector, and setting a normative standard of government role. Further, it is a comprehensive activity that includes activities of informal organizations, non-governmental organizations as well as governments. Based on horizontal linkage between actors, and self-organizing networks, governance seeks to forge public-private partnerships to attain common goals. Jessop conceptualizes it similarly as “the rise of horizontal and cooperative organization among interdependent actors, such as the market, society and civil society, in response to market and government failures.”<sup>19</sup> Kooiman refers to governance as shifting away from one-sided and vertical relationships to horizontal interactions between government-civilian relations, highlighting dynamism, complexity, and diversity as key characteristics of governance.<sup>20</sup> On the other hand, Stoker perceives governance

---

<sup>18</sup> Rod Rhodes, “Understanding governance: policy networks, governance, reflexivity and accountability,” *Public Policy and Management*, Philadelphia, US. Open University, (1996): 252-254.

<sup>19</sup> Bob Jessop, “Liberalism, Neo-Liberalism and Urban Governance: A State Theoretical Perspective,” *Antipode* 34, no.3 (2002): 452-472. <https://doi.org/10.1111.1467-8330.00250>.

<sup>20</sup> Jan Kooiman, *Governing as Governance*, (New York: Sage Publications, 2003):114.

as a self-organizing network, featuring interdependence, resource exchange, rules of game and autonomy from the state, underscoring the interrelationship between the government and non-governmental organizations.<sup>21</sup> Lee refers to governance as “a voluntary network in which various stakeholders or actors participate and interact to solve problems in national society”<sup>22</sup>, whereas Ahn refers to it as “divided and multidisciplinary networks that focus on communication between social sub-systems, avoiding direct government intervention.”<sup>23</sup>

The governance concept of consultation refers to an autonomous adjustment form which exists within the civil society domain, distinct from national and market instruments. Governance is conceived as a form of institutions and coordination in which various actors cooperate on the basis of autonomous interdependencies in the absence of formal authority. In broader context, governance is new collaborative modus operandi, emerging in response to the blurring boundary between the public and private organizations, seeking a new form of cooperation based on partnerships among countries, civil society and markets.

Taken together, governance can be conceived as the voluntary participation and interaction of various groups or public and private organizations, incorporating governments, markets and civil society in the policy process and service delivery process to tackle problems by forming a horizontal and cooperative network, as

---

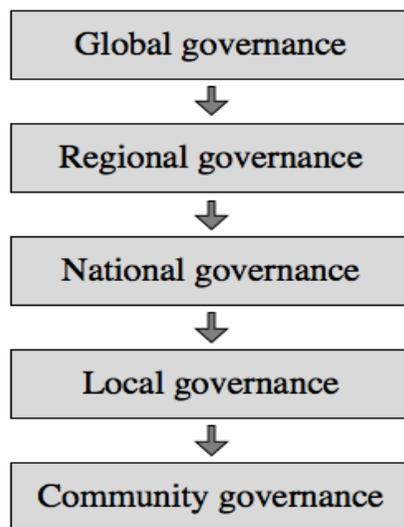
<sup>21</sup> Gerry Stoker, "Governance as Theory: Five Propositions." *International Social Science Journal* 50, No. 155 (1998): 17-28.

<sup>22</sup> Myung-seok Lee, "Conceptualizing Governance: Governance as a Social Coordination." *Korean Public Administration Review* 36, No.4 (2002): 331-333.

<sup>23</sup> Byung Young Ahn, "The Changing Role of the State in the 21<sup>st</sup> Century and Governance," *Idea and Ideology the Quarterly* 44, No.3 (2000): 13-15.

opposed to hierarchical orders and coordination. Inherent in conceptualizing governance is horizontal cooperation between different stakeholders, which clarifies and coordinates each of their respective roles and responsibilities, and reinforces the connectivity integration. Fulfilling such objective requires continuous and stable interaction, communication, voluntary participation and cooperation, trust, responsibility, understanding, etc. Traditional bureaucratic perspective on the other hand assumes government as the exclusive legal enforcer and supplier of hierarchical system.

There are five dimensions of governance: global governance, regional governance, national governance, local governance, and community governance (see Figure 2-2). This paper will focus primarily on the national governance level to analyze the national cybersecurity governance.



**Figure 2-2** Dimensions of Governance

## 6) Governance Capacity and Good Governance

Governance capacity refers to the ability of governance to solve problems. More specifically, it can be determined as the ability of actors within governance to organize and operate autonomous cooperation. Determinants of governance capabilities include stakeholder autonomy, conflict resolution, mutual trust through information and authority sharing, collaborative leadership through respect for different opinions, open communication, equitable benefit and burden, stakeholder protection, and incentives. As desirable elements of governance, the United Nations Development Programme (UNDP) identifies the following: participation, governance by law, transparency (the free-flow and access to information, provision of information), responsiveness, consensus-oriented, accountability, strategic vision, resource conservation, equity, empowerment, partnership, efficiency, community foundation, etc.<sup>24</sup>

Different organizations prescribe slightly varying accounts of what good governance consists of. Good governance according to the World Bank incorporates the following elements: voice and accountability, political stability and absence of violence, government effectiveness, regulatory quality, rule of law, control of corruption.<sup>25</sup> The International Monetary Fund incorporates the establishment of rule by law, enhancement of efficiency and responsibility in the public sector and an active

---

<sup>24</sup> Qudrat-I Elahi, Khandakar, "UNDP on good governance," *International Journal of Social Economics* 36, no. 12 (2009): 1167-1180.

<sup>25</sup> Pena, Jorge, Luis Guasch, and Alvaro Escribano, "Reforming public institutions and strengthening governance: a World Bank strategy," (The World Bank, 2000): 78.

response to corruption as components of good governance<sup>26</sup>, whereas the United Nations prescribe good governance as consensus-oriented, participatory, abiding by the rule of law, effective and efficient, accountable, transparent, responsive, equitable and inclusive.<sup>27</sup>

## **7) Conditions for Governance Formation**

There exist several key conditions for the formation of governance. First, there ought to be resource dependency among the actors. Participation in governance incurs costs, therefore, there must be sufficient benefits for actors to participate at the cost of such expense. Simply put, actors participate in governance when there is a possibility of obtaining resources in which they do not possess, from the other party.

Second, network formation and collaborative interaction between actors is necessary. Actors form governance based on resource dependency, and interaction takes place in an autonomous and network, which involves flexibility, autonomy, interdependence, etc. However, this does not imply that the role and the weight of the actor is equivalent. Rather the greater the resources, the more central the actor's status.

Third, trust, autonomy and reciprocity among actors are required, since governance is sustained through voluntary participation and cooperation, not through centralized orders and directives. Relationships between actors are horizontal, and

---

<sup>26</sup> Nanda Ved, "The good governance concept revisited." *The ANNALS of the American academy of political and social science* 603, No. 1 (2006): 269-283.

<sup>27</sup> Thomas, Weiss. "Governance, good governance and global governance: conceptual and actual challenges." *Third world quarterly* 21, no. 5 (2000): 795-814.

actors within governance must form reciprocal relationships. Reciprocity is where all actors form win-win relationship by participating in governance, which depends on the generation of continuous benefits.

Fourth, the sharing of goals and beliefs among actors, particularly their beliefs in democracy, devotion to the promotion of common understanding, faith in and respect for the members.

Fifth, setting the rules of the game is critical to maintain governance, the rules must be complied, and failure to comply would lead to sanctions against the violators.

Sixth, sharing information and authority must be maintained through horizontal power-relations, along with sharing the means to achieve the common goal.

Last but not least, setting the scope of participants is relevant in building and maintaining governance, as it seeks to engage and not exclude any actors.

### **8) Requirements for Successful Governance**

As there were preconditions for the formation of governance, there also exist requirements for successful governance. First, trust, autonomy and community spirit ought to be promoted. The role and leadership of the public sector is important in the process of accumulating trust through societal-wide formation of social capital, creation of reciprocal benefits, agreement and concessions, compliance with agreements and rules. Although the nature of governance is voluntary, it operates on certain set of rules and trust. Therefore, for successful sustenance of governance, a diagnostic leadership is required to create of an atmosphere of dialogue and compromise, establish decision-making and communication channels, participate and

respect for minority opinions. Community spirit refers to the attachment of actors towards the community and their active participation in problem solving.

Second, continuous participation and interaction should be encouraged, whereby the public sector should act as the facilitator to encourage active participation. The facilitator ought to monitor the operation of governance, to ensure effective communication, as continuous benefit creation critically depends on fostering participation and interaction of the relevant actors.

Third, fostering a conducive social environment by identifying major private sectors in the relevant policy areas, disclosing information and encouraging active participation is necessary. Efforts should be geared towards integrating the private sector into the public management process through continuous identification of demands and via community surveys and complaints and satisfaction surveys for public services.

Fourth, roles and responsibilities of the actors should be clearly outlined. The public sector plays a complex role as regulators, rule-setters, facilitators or applicators, whereas the private sector serves as a decision-maker and service-provider within governance. On the other hand, civic groups act as advocates, monitors, and often perform the roles of intermediaries.

Fifth, enhancing the network between actors and services is required. Gilbert and Terrell (2013) identifies fragmentation, discontinuity, accountability and inaccessibility as problems in the service delivery system.<sup>28</sup> Among these factors, the issue of fragmentation and discontinuity are largely due to the lack of integration and

---

<sup>28</sup> Gilbert and Terrell, *Dimensions of Social Welfare Policy*, (New York: Pearson, 2013).

connectivity. Linkage is an active interaction which emphasizes cooperation between the participating actors to attain a common objective.

Sixth, the establishment of governance leadership is important. Although leadership is also voluntary, sharing vision and reaching common understanding through communication and exchange of information depends on a participatory and supportive leadership.

Seventh, coordination and communication system should be established. Coordination is the orderly arrangement of various activities. There are various methods of coordination, such as installing controls and clarifying roles and responsibilities for accountability. Effective coordination requires proper communication channels, efficient information sharing, and provision of incentives. Communication is essential to governance maintenance, and it can be facilitated through the formation of horizontal communication channels, establishment of cyberspace for collecting and disseminating information, and the dissemination of periodic reports.

Eighth, rule-setting and power-sharing should be established. The relevant actors' actions must be reasonable and predictable, which requires the provision of rules and observance to the rules. Furthermore, empowerment is crucial, as the actors are to share authority and responsibility in the process of working collaboratively towards the common goal.

Last but not least, information sharing system ought to be established. Since governance operates in a networked manner, it depends on the medium which connects these networks and efficiently distributes the relevant information.

## 2.2 Literature Review

### 1) Literatures on Regional and Global Cybersecurity Governance

Previous literatures on national cyber security have primarily focused on the development and evolution of cyber offense and defense capabilities, along with predicting the future of cyber warfare and cyber security dilemma. These literatures have also put forth constructive policy recommendations, and cyber security strategies to pursue on organizational, national, regional, and supranational level.

Christou explores regional cybersecurity governance in the European Union, and contributes a conceptual framework to better grasp E.U efforts to enhance cybersecurity governance. This concept acknowledges the sophisticated and multi-layered quality of the cybersecurity ecosystem, that deviates away from the existing approach of security as control. The author identifies six preconditions, which form the foundation of assessing EU's evolution in cyberspace governance to attain effective security in cyberspace: the ability to adapt to new structures and operating assumptions, acceptance of complexity in governance logics, formation of trust-based partnerships between the main stake-holders, consolidation of common understandings of key concepts pertinent to cybersecurity governance, acceptance of a culture of cybersecurity among all relevant actors, and establishment of coherency and consistency across all levels and actors. When taken together, the aforementioned conditions form the foundation of assessing EU's cybersecurity governance.<sup>29</sup>

---

<sup>29</sup> George Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, (London: Palgrave Macmillan, 2017): 29.

From a global governance perspective on cybersecurity, Bae highlights the need for an international norm on cybersecurity.<sup>30</sup> There have been ongoing international efforts to establish an international norm, ranging from United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), International Telecommunications Union (ITU), Shanghai Cooperation Organization (SCO), Internet Corporation for Assigned Names and Numbers (ICANN), etc., with global-level discussions held at the regional, individual national levels in Europe, Asia, and other countries, as well as by governments, supranational companies, NGOs, and other international organizations. In particular, two major achievements in the UN GGE are worth highlighting: delineation of the global cybersecurity agenda, and introducing the application of international law to the cyberspace. Currently, discussions on cybersecurity international norms are at odds between the West, which seeks to extend the existing international legal framework to incorporate cybersecurity realm, and Russia and China on the opposite side of the spectrum, which pursues introduction of a new international cybersecurity legislation in recognition of national sovereignty. Despite the lack of consensus on establishing international cybersecurity law, acknowledging and understanding the different values held by different countries itself can be perceived as a significant achievement so far, as continuous cooperation can seek to mitigate those differences.

---

<sup>30</sup> Bae Young Ja, *National Cybersecurity*, (2016): 97-129.

## 2) Literatures on Cybersecurity Governance in South Korea

Park and Kim examines the existing cybersecurity propulsion system of Korea and identifies the inherent problems in distributed cybersecurity management system during normal situations. The authors suggest that the propellant system for cybersecurity ought to be integrated, with significant improvement in the legal system in order to overcome the inefficient management method. In order to do so, it is critical to raise awareness on cybersecurity, with the National Assembly actively encouraging interest articulation and pursuing interest aggregation on this matter to draw up specific measures for readjustment of the legal system and seek revision or introduction of relevant legislation.<sup>31</sup>

Similarly, D. Kim delves into the more recent legal-institutional aspect of cybersecurity governance in South Korea, and introduces the legal development in support of national cyber security. In doing so, Kim identifies fragmented cybersecurity laws in Korea as great impediment to effective response to adverse cyber incidents. The author recommends establishing cyber threat information sharing system for public and private entities, legislating a comprehensive cybersecurity law by first tackling the legal risks involved in the process of providing cyber threat information to the government, and enhancing personal information protection system. To fulfil the objectives of strengthening the comprehensive legal

---

<sup>31</sup> Sang Don Park and Injung Kim, "A Study on Tasks for the Legal Improvement for the Governance System in Cybersecurity," *KSH Transactions on Internet and Information Systems* Vol.12, No.2 (2015): 843-859.

basis for national cybersecurity, the government ought to assume a proactive leadership role.<sup>32</sup>

Cho and Kwon compares the cybersecurity governance of South Korea and the U.S. from the perspective of cyber threat securitization theory.<sup>33</sup> The securitization theory is utilized to explicate why cybersecurity governance overall has been more coherent and successful in the U.S., then in South Korea, where it is characterized by high levels of incoherent fragmented policies. Despite the both countries undergoing significant levels of losses from incessant cyber attacks, the differing outcome of cybersecurity governance is the result of the country's capacity to form securitization discourse around the issue. Delving deeper, the authors identify that the success in U.S capacity to securitize cybersecurity was facilitated by the Obama administration's recognition of cyber threats as key issue of national security agenda by utilizing executive orders to bypass congressional opposition. As series of cyber terrors took place during this process, passing relevant bills became smoother as the perception of the political community as a whole shifted from the protection of privacy to inevitably accepting the public-private information sharing system. On the other hand, the legacy of conflictual state-society relations in Korea has led to fragmented cyber threat securitization, leading to successful politicization of privacy

---

<sup>32</sup> Do Seung Kim, "A Study on Law and Organization for Strengthening Cybersecurity," *Study on the American Constitution* 28, no.2 (2017): 99-130.

<sup>33</sup> Cho Hwha Soon and Kwon Oung, "Comparing Korea and U.S. Cybersecurity Governance: from the Perspective of Cyber Threat Securitization Theory," *Information Society & Media* 18, No. 2 (2017): 97-120.

and human rights over establishing a comprehensive legal basis for public-private information sharing system.

In discussing South Korea's cybersecurity strategy and diplomacy, Kim also identifies similar problems of fragmented nature of Korea's cybersecurity governance as did the previous authors.<sup>34</sup> The author strategizes the next step for Korea to strengthen its national cybersecurity, and recommends weaving intricate network shield against potential cyber attacks. Building such sophisticated shield against cyber attacks require budgetary and institutional support for technical capability development. More specifically, the construction of network shield is based on increasing the following capacities: prevention, detection and resilience. Reinforcing such defense technology capacity critically depends on the availability of relevant human resources, in particular, highly trained cybersecurity professionals who can comprehensively deal with hardware, software, network, information protection, digital forensics, etc., in the event of an adverse cyber incident. In pursuing national cybersecurity strategies, the author highlights avoiding the following hyper security discourse of excessive securitization, militarization, politicization and realism, as falling into these could easily overlook the complex nature of cybersecurity and hinder effective formation of national cybersecurity governance.

---

<sup>34</sup> Sangbae Kim, *National Cybersecurity Strategy*, (Seoul: Critical Perspectives on Society Academy, 2017).

### **3) Common Limitations of Precedent Studies**

Overall, literatures which tie both the cybersecurity realm and international security from politics and governance perspective are at nascent stages due to the complexity of approaching the cyber discipline with abstruse cyber lexicon from a political-science discipline. Literatures on South Korea's national cybersecurity governance have sought to prescribe constructive recommendations to strengthen the country's cybersecurity. However, the recommendations proposed by the existing literatures tend to be somewhat broad, and tend to limit the scope of recommendation to a single-focus area. Strengthening the cybersecurity governance requires both holistic and deep understanding of South Korea's unique pre-existing institutions' relationships, and recommendations ought to be sufficiently sophisticated and comprehensive to fulfil the aforementioned objective.

Furthermore, existing literatures suggest "what" the country must pursue to reinforce national cybersecurity governance, but fails to incorporate "how" such policies or recommendations are to be realistically pursued. More specifically, existing literatures indicate the fragmented nature of Korea's cybersecurity governance and broadly calls for streamlined approach to bolster cybersecurity, yet fails to more specifically indicate how policymakers can achieve such integrated cybersecurity governance. Therefore, sorely required is a research delving deeper into the procedural aspect of how integrative cybersecurity governance can be achieved in Korea, based on the comprehensive model of good governance.

### **2.3 Research Method: Document Research and Case Study**

This research is a prescriptive research which seeks to bolster cybersecurity governance system in South Korea drawing upon U.S. as a case study, by analyzing the reality and underlying problems of cybersecurity governance system in South Korea and develop policy means to prescribe practical policies. Therefore, although this research is primarily dependent on qualitative research methodology, it seeks to enhance accuracy by utilizing diverse research methodologies.

Above all, this article conducts theoretical debates, establishment of the dimensions of analysis, analysis of contemporary situation and underlying problems, and foreign case-study through document research. In addition, as part of the document research, content analysis will be conducted on government released publications, internal documents of relevant institutions, etc. Furthermore, case-study will be conducted to obtain policy implications through foreign cases. The details of each research methodology will be further elaborated below.

In the document research, document is divided into primary, secondary and tertiary document data. The primary documents are directly gathered and prepared by the researchers, and the secondary documents are indirectly gathered by the researchers. The tertiary documents include abstracts, indices, etc.<sup>35</sup> Among these three categories, this paper will primarily refer to primary and secondary documents, and diverse texts and journals will be utilized to investigate theoretical discussions,

---

<sup>35</sup> Flick, Uwe, Ernst Von Kardorff, and Ines Steinke, "What is qualitative research? An introduction to the field." *A companion to qualitative research* (2004): 3-11.

conduct literature review, establish dimensions of analysis, and examine a foreign case-study.

For this purpose, this paper makes use of major domestic libraries and data searching websites, as well as United States' Libraries, U.S Government websites, and relevant search engines will be actively utilized with regard to examining foreign case study. With regard to collecting empirical data and materials, this article collects primary and secondary documents to analyze relevant institutions and contemporary situations. Collected data and materials will be appropriately processed to meet the uses in required parts. In terms of gathering data, various documents including official intergovernmental data such as statistics data, white papers and legislative documents from the U.S Congress, Department of Homeland Security, Office of Management and Budget as well as business reports and publications from related agencies will be included. Publications by local governments and related organizations will also be analyzed. This research will also actively utilize credible newspaper articles and analyze some pending issues as well.

In order to supplement and confirm the document research, content analysis will be conducted. Content analysis is a research method that deduces conclusion by classifying and interpreting unstructured materials according to a type of system, and seeks to classify large amount of information into smaller manageable numbers and identify trends based on coding rules. Content analysis sets specific symbols, propositions, and people that are expressed as messages as analytical units, and analyses them according to pre-set classified items and coding rules, such as calculating the frequency of their appearance and measuring the space of their

appearance. Classified items correspond to research variables, and treat how to classify data and materials in accordance with intended criteria. A unit of analysis is the smallest unit of research contents, which researchers aggregate to investigate frequency, is classified by criteria and items. Content analysis can be utilized in both qualitative and quantitative studies. Content analysis is conducted in the following order: setting research questions, selecting the unit of analysis, choosing preliminary item of analysis, adjusting analysis items or targets, planning coding procedures and coder training, calculating reliability and analyzing the results of coding.<sup>36</sup>

This article includes the case study on an advanced country. A case study provides detailed analyses of one or more cases, whereby an in-depth technical and analytical research is pursued based on sufficient information of specific individual, group, organization, and event. For the purpose of conducting a case-study, diverse sources of information are utilized including observations, interviews, audio visual materials, documents and reports. Case studies can be either single case or multiple case studies. The former conducts intensive study on one example, and is primarily adopted for analyzing typical cases, rare and unique cases, and longitudinal comparison. Although there are limits to generalization in a single case study, this is not necessarily true for all cases. The latter incorporates two or more cases, and strives to overcome the limits of generalization in a single-case study, through the logic of repeated experiment.<sup>37</sup> Multi-case studies are useful for comparative analysis in accordance to the context.

---

<sup>36</sup> Krippendorff Klaus, *Content Analysis: An Introduction to its Methodology*, (London: Sage publications, 2018): 132-139

<sup>37</sup> Yin and Robert K, *Case Study Research and Applications: Design and methods*, (London: Sage publications, 2017).

Case studies are conducted in the following stages: research design, preparation of data sets (case study protocol and development), data gathering (interview, observation, literature review, etc.), data analysis (detailed description and technical analysis, interpretation, argument, understanding context of the case, etc.), drawing implication (analysis outcome explanation, mentioning the relationship between research purpose and research outcomes, etc.). The advantage of conducting case-study is the simultaneous adoption of diverse research methods, often in combination with interviews, observations, and literature reviews.<sup>38</sup> This research seeks to analyze the case of the U.S. national cybersecurity governance to draw benchmarking implications, and conducts a single-case study to reveal proactive efforts through comprehensive establishment of relevant legislative and administrative systems to strengthen its cybersecurity governance system. The following section will provide rationale behind the selection of the U.S. as case study for national cybersecurity governance, and the specific lists of analysis will be established to systematically analyze the case based on the dimensions of analysis provided below.

---

<sup>38</sup> Thomas Gary, *How to do your case study*, (New York: Sage Publications, 2015).

## 2.4 Rationale for U.S. Cybersecurity Governance as Case Study

The United States was specifically chosen amongst other major Western powers as it has been a leading country in actively promoting national cybersecurity governance. The U.S. has acknowledged the importance of national cybersecurity as it became the target of cyber attacks from North Korea, China and Iran in the 2000s. Furthermore, the country also recognized its exceptional vulnerability to cyber attacks, with increasingly greater proportion of national critical infrastructures dependent on IT. It is also important to note that the large percentage of critical infrastructures in the U.S are privately owned, thereby rendering public-private partnerships and information-sharing critical to efficient response and defence against cyber attacks. Since then, the U.S. has actively sought to form a multi-stakeholder form of cybersecurity governance, which emphasizes the collaboration between the public and the private sector, by drawing relevant stakeholders together to participate in dialogue, decision-making and implementation of decisions.<sup>39</sup>

In addition to the consolidation of an effective national cybersecurity governance, the U.S. leads in cybersecurity technology, analysis and gathering cyber intelligence and cyber warfare. According to the Global Cybersecurity Index (GCI)<sup>40</sup> established by ABI Research and ITU to determine a country's level of cybersecurity

---

<sup>39</sup> Kuehn A, *Extending Cybersecurity, Securing Private Internet Infrastructure: the US Einstein Program and its Implications for Internet Governance*, In: Radu R., Chenou JM., Weber R. (eds) *The Evolution of Global Internet Governance*. (London: Springer Publications, 2018).

<sup>40</sup> The Global Cybersecurity Index (GCI) takes into account the following five pillars to measure a country's level of cybersecurity against cyber attacks at a global level: (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Building, and (v) Cooperation which are then aggregated into an overall score.

threat preparedness, the U.S. is ranked as number one in terms of best prepared against cyber attacks. Accordingly, this paper selects the cybersecurity governance system of the U.S., among other countries as a target of case study to draw benchmarking implications from the experiences of advanced countries.

## **2.5 Dimensions of Analysis**

The governance system is a type of comprehensive entity, which consists of some sub-components. In order to establish and operate the governance system, various components such as legal institutions, budget, and staff and organizations should be well equipped and operated within the government, whereas the cooperation with and support from the private sector should be secured from external sources. In particular, a firm and healthy partnership between public and private sectors is one of the necessary requirements to establish the governance system, since the governance system is based on the constructive interdependence between the public and private sectors. While the traditional government perspective emphasized the boundary distinction between public and private sectors, the governance perspective underlines the blurred boundary between them. The public and private sectors intimately cooperate in treating public matters; therefore, the private sector substantially participate in the process of government policy-making as well as policy implementation. By considering these characteristics of the governance system, this paper selects the following five components as the variables to examine the contemporary situations and underlying problems of the cybersecurity governance system of Korea (refer to Table 2-1).

**Table 2-1** Dimensions of Analysis

Dimensions	Contents
Legal and Institutional Systems	The provision of effective legal and institutional frameworks, their specificity and feasibility
Administrative System	Cybersecurity organizational structure, linkage institutions and personal procurement
Finance and Budget Systems	The sufficiency of financial resources, the financing and distribution of resources
Public-Private Partnerships	The availability of private sector support or cooperation in the process of implementation, and the communication channel between the government and the private sector
Monitoring and Evaluation Systems	The management and evaluation systems, incentive system

# CHAPTER III

## The Cybersecurity Governance System of the United States

### 3.1 An Overview of Cybersecurity Legislation and Policies in the United States

Since the mid 1980s, there have been various enactment of laws pertinent to cybercrime such as the Computer Fraud and Abuse Act in 1986. The Clinton Administration strived to develop an effective cybersecurity strategy on a federal level to strengthen the U.S. critical infrastructure protection against evolving threats by suggesting how cybersecurity was fundamental to the confidence of economic security. In 1996, the Clinger-Cohen Act, also referred to as the Information Technology Management Reform Act, sought to reform the federal government IT management by granting agencies to acquire IT resources independently. The Act also sought to institute competent IT leadership in each agency by mandating the appointment of Chief Information Officers with their roles and responsibilities clearly outlined.<sup>41</sup> In 1998, Presidential Decision Directive (PDD)-63 *Critical Infrastructure Protection* provided the first comprehensive cybersecurity governance for critical national infrastructures.<sup>42</sup> According to the Direction, a Senior Directorate for Infrastructure Protection on the National Security Council staff was to be established to minimize physical and cyber attack vulnerability to critical infrastructures. In

---

<sup>41</sup>Clinger-Cohen Act, available: <https://business.defense.gov/Portals/57/Documents/Federal>

<sup>42</sup> Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators, *Federal Register* 63, Issue 150 (1998).

addition, the Office of National Coordinator for Security, and Infrastructure Protection and Counter-Terrorism, in charge of overseeing the Critical Infrastructure Coordination Group were established to strengthen critical Infrastructure protection. Overall, the PDD-63 emphasized forming partnerships with the private-sector to coordinate more effective cybersecurity governance.<sup>43</sup>

Following the Clinton Administration, the Bush Administration acknowledged the possibility of cyber terror of being a critical national security threat after the 9/11 Terror in 2001, and further bolstered critical infrastructure security policies through executive order and legislations. Central to the Administration's efforts to strengthen cybersecurity governance is the enactment of Homeland Security Act in 2002, and the establishment of Department of Homeland Security (DHS) based on the Act. The DHS integrated the fragmented relevant information agencies and was tasked with overseeing the U.S. cybersecurity and homeland security. In December 2002, the Federal Information Security Management Act (FISMA) was enacted, to serve as the basis for other cyber-related laws, and it delineates specific roles and responsibilities for federal cybersecurity and mandates agencies to protect their respective information systems. Among the major federal cybersecurity initiatives, the January 2008 Comprehensive National Cybersecurity Initiative (CNCI) is worth noting, as it forms the foundation for future federal cybersecurity initiatives in enhancing federal government's protection of sensitive information.<sup>44</sup>

---

<sup>43</sup> James Boys, "The Clinton administration's development and implementation of cybersecurity strategy (1993–2001)," *Intelligence and National Security* 33, No.5 (2013): 755-770.

<sup>44</sup> National Presidential Security Directive 54: January 2008 Comprehensive National Cybersecurity Initiative (CNCI).

During the Obama Administration since 2009, the issue of addressing cybersecurity was further highlighted and witnessed dramatic improvements to the US cyber laws. The Cyberspace Policy Review published in May 2009 suggested future direction for national cybersecurity, and appointed a separate Cybersecurity Policy Official to oversee and control cybersecurity policy and possess direct leadership over this matter. The Cybersecurity Policy Official provides streamlined policy guidance, and clarifies the roles and responsibility of each institutions in federal government to deter, prevent, detect and defend against cyber attacks. Subsequently, the administration established cybersecurity center, and appointed Cybersecurity Coordinator as the special advisor to the President. Alongside, the National Cyber Incident Response Plan was established, and provided cybersecurity training called Cyber storm under the Department of Defense and DHS, which intended to strengthen central government's capacity to respond to adverse cyber incidents. During this time, the Obama administration sought policies to balance the issue of privacy and state security, which greatly contributed to overcoming political deadlocks in the Congress in enacting future cybersecurity legislations.

As cyber attacks on U.S. critical Infrastructure continued in 2013, the Obama administration re-visited the existing cybersecurity strategy, and stepped up the cybersecurity governance system. The Executive Order (EO) 13636 and PDD-21 are evidence of the aforementioned effort. The EO 13636- *Improving Critical Infrastructure Cybersecurity* sought to establish cyber threat information-sharing system and laid the groundwork for cybersecurity framework to reduce cyber

vulnerabilities to critical infrastructures.<sup>45</sup> The PDD- 21 *Critical Infrastructure Security and Resilience* sought to refine and clarify functional relationships across the Federal Government to streamline critical infrastructure security and resilience. The Directive also illuminates upon effective information exchange and implementation of integrated analysis, planning and decisions pertinent to critical infrastructure.<sup>46</sup>

In 2014, the Cybersecurity Enhancement Act was enacted to provide a voluntary public-private partnership to enhance cybersecurity and reinforce cybersecurity R&D, develop and educate workforce, and raise public awareness and preparedness. Furthermore, the National Cybersecurity Protection Act of 2014, formalized the NCCIC in DHS to share information on cybersecurity matters across the federal and non-federal sectors. In order to secure information and data on federal cybersecurity, the Federal Information Security Modernization Act (FISMA 2014) amended the the pre-existing FISMA 2002 law, revising the roles and responsibilities of DHS and OMB pertinent to federal agency information security. Partially due to FISMA requirements, the federal government yields plethora of federal cybersecurity data, and OMB's FISMA report is deemed the most all-inclusive source, which encompasses federal performance on cybersecurity incidents, cybersecurity initiative implementation, and advancements to information security objectives.

---

<sup>45</sup> Executive Order-13636: *Improving Critical Infrastructure Cybersecurity* (2013).

<sup>46</sup> Presidential Decision Directive- 21: *Critical Infrastructure Security and Resilience* (2013).

In February 2015, the publication of EO-13691 *Promoting Private Sector Cybersecurity Information Sharing*, provided institutional basis for cyber threat information-sharing with the private sector. More specifically, the Order fostered the establishment of Information Sharing and Analysis Organizations (ISAOs) to serve as the center for sharing cybersecurity related information among the private and federal entities, by extending the existing Information Sharing and Analysis Centers (ISACs) activities from information sharing centered around private entities to public-private information sharing. On top of this, the Order also established a public-private entities' information-sharing channel through an agreement between National Cybersecurity and Communications Integration Center of the DHS and ISAO. In the same year, Cybersecurity Information Sharing Act (CISA) of 2015 featuring similar content had been passed in the Senate, consolidating the foundations for a stable cyber threat information-sharing system in cybersecurity governance.<sup>47</sup> In April 2015, The National Cybersecurity Protection Advancement Act, amending the Homeland Security Act of 2002, sought to expand the composition of DHS NCCIC to include tribal governments, information-sharing, and analysis centers, and private entities among its non-federal representatives.<sup>48</sup>

Under the auspices of EO-13636, PDD-21, and EO-13691, cyber threat information-sharing with the private sector had been repeatedly emphasized, and the accumulation of such efforts have resulted in the enactment of Cybersecurity Act of

---

<sup>47</sup> CISA grants the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies.

<sup>48</sup> National Cybersecurity Protection Advancement Act of 2015, (sec 2).

2015. The Cybersecurity Act of 2015, identified as one of the most significant piece of cyber-related legislation, provides a stable legal framework for establishing information-sharing system among the private sector and federal government entities. The Act safe harbors private sectors which share cybersecurity information from liability, and grants other entities external to the federal government to monitor information systems and pursue defensive cybersecurity measures. Furthermore, the Act contains provisions for a cybersecurity propulsion system to regulate and identify federal authority and responsibilities pertinent to cybersecurity. It also mandates all civilian agencies to adopt EINSTEIN<sup>49</sup>, in order to detect and deter threats to federal networks.<sup>50</sup> In the following year, the Cybersecurity National Action Plan (CNAP) was introduced to establish practical action plan for Federal Government, and facilitate conditions necessary for long-run strategies to fortify national cybersecurity across the Federal Government, private-sector and individuals. The Plan established the Commission on Enhancing National Cybersecurity, consisting of top strategic, business and technical members outside the government, to give practical advice on bolstering long-term cybersecurity.

Following the Obama Administration, the incumbent Trump Administration has continued the momentum accumulated from previous administrations to enhance the cybersecurity governance system of the country. In May 2017, President Trump

---

<sup>49</sup> EINSTEIN is a DHS program which serves two major functions in federal government cybersecurity. First, it detects and blocks cyber attacks from compromising federal agencies, and second, it provides DHS with the situational awareness to use threat information detected in one agency to protect the rest of the government and to help the private sector protect itself.

<sup>50</sup> Paul Rosenzweig. "The Cybersecurity Act of 2015." *Lawfare* (2015). Accessed: <https://www.Lawfareblog.com/cybersecurity-act>.

issued Executive Order-13800 *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. The Order seeks to modernize Federal information technology infrastructure by forming strong partnership across the Federal Government with state and local government and private entities to safeguard critical Information infrastructures against the backdrop of escalating cybersecurity threats. Furthermore, the Administration enacted National Institute of Standards and Technology (NIST) Small Business Cybersecurity Act in 2018 for the purpose of providing cost-effective cybersecurity strategies for small- and medium-sized businesses (SMB) which are more susceptible to growing cyber threats. The Act mandates the NIST to take into account the nature and size of small businesses when formulating voluntary, consensus-based, industry-led guidelines to reduce cyber vulnerabilities of critical infrastructure. The Administration also renewed the National Cyber Strategy (NCS) in the same year, revealing the most comprehensive and proactive NCS to date. The strategy directs periodical review of defense against cyber attacks, and continues the ongoing efforts to build collaboration across various stake-holders to enhance common defense against cyber attacks.

More controversially, the Trump Administration rescinded PDD-20 of the Obama-era, which limits the use of offensive cyber weapons, and alleviated certain restrictions governing the approval process for the use of offensive cyber weapons.<sup>51</sup> This signifies that the Administration intends to respond not only defensively but also

---

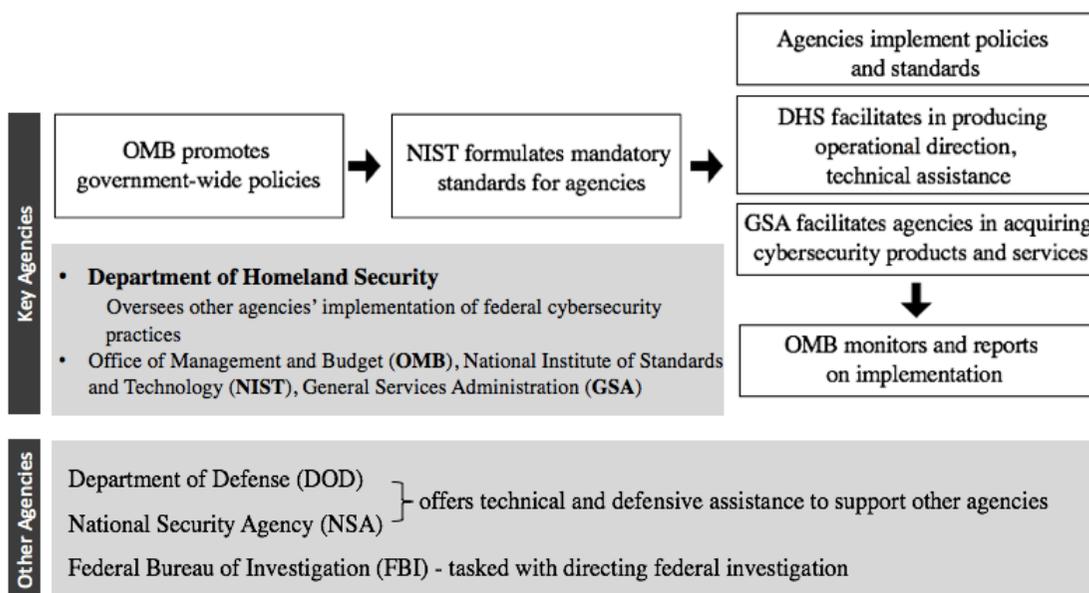
<sup>51</sup> Dustin Volz, "Trump, Seeking to Relax Rules on U.S. Cyber attacks, Reverses Obama Directive," *Wall Street Journal*, August 15 2018, accessed April 12, 2019, <https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721>

offensively should it be deemed necessary, and endorses the best defense is good offense logic, by deterring adversaries through effective cyber offense. The change delegates greater authority to the commander of U.S. Cyber Command, essentially granting the U.S. military to utilize cyber offensives against U.S. adversaries with significantly less oversight from the State Department, Commerce Department, and intelligence agencies. Although the rescinding of PDD-20 has received mixed views, as more frequent cyber offensives towards U.S. adversaries could provoke greater retaliation, the intention serves to streamline the process of responding to imminent cyber attacks in certain circumstances, and reduces the time-consuming process of coordinating with various agencies.

Overall, there have been great continuities over the past Administrations in formulating and consolidating stable cybersecurity governance system in the U.S., and the country has been successful in forging a common-defense line against cyber threats through the combination of Executive Orders, Presidential Decision Directives, and provision of solid legal basis for information-sharing between the public and private entities. Currently, the U.S. is at the crossroads of reinforcing a unified, holistic, and proactive cybersecurity strategy based on strong public-private partnerships.

### 3.2 Administrative System: Roles and Responsibilities

The Federal Information Security Modernization Act of 2014 mandates every federal agency to be responsible for its own cybersecurity. Nonetheless, some agencies including the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the General Services Administration (GSA) serve inter-dependent functions in facilitating and monitoring other agencies' cybersecurity measures. Among the aforementioned agencies, the DHS oversees the other agencies in implementing federal cybersecurity practices. Overall, these agencies each with its prescribed roles and responsibilities interact in a sophisticated manner to reinforce federal cybersecurity. The (Figure 3-1) below outlines the sequential interaction between the key agencies involved in Federal cybersecurity.



**Figure 3-1** Sequential Interaction Between Key Agencies

To further elaborate on each of the aforementioned agencies' roles, the OMB is charged with formulating and overseeing the entire implementation of policies, standards, and guidelines on federal information security.<sup>52</sup> The NIST is tasked with formulating mandatory standards and guidelines for non-national security federal information systems.<sup>53</sup> Yet, the NIST does not possess the authority to verse or demand compliance. The DHS performs the leading operational role in facilitating cybersecurity risk management through the protection of federal networks. In broadly outlining its functions, the DHS strives to offer consistent set of security to all agencies, serve as an information-sharing center, promotes comprehensive implementation of NIST guidance, and lends assistance to other agencies in responding to adverse cyber incidents. The GSA identifies and delivers the necessary cybersecurity products and services for federal agencies.

In addition to the OMB, DHS, NIST, and GSA, other agencies such as the Department of Defense (DOD), Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) also perform vital roles to enhance federal cybersecurity. The intelligence community offers crucial pieces of information in aiding civilian aspects of federal government in identifying, deterring and responding to cyber incidents. Both the DOD and NSA offers technical and defensive assistance in support of other agencies, and the FBI is tasked with directing federal investigation

---

<sup>52</sup> Office of Management and Budget Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2016. [https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy\\_2016\\_fisma\\_report%20to](https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to).

<sup>53</sup> NIST, <https://www.nist.gov/cyberframework>.

should federal systems be compromised. Furthermore, the DOD and intelligence agencies are charged with the protection of national security systems, including sensitive classified networks.

### **3.3 Federal Cybersecurity Budget**

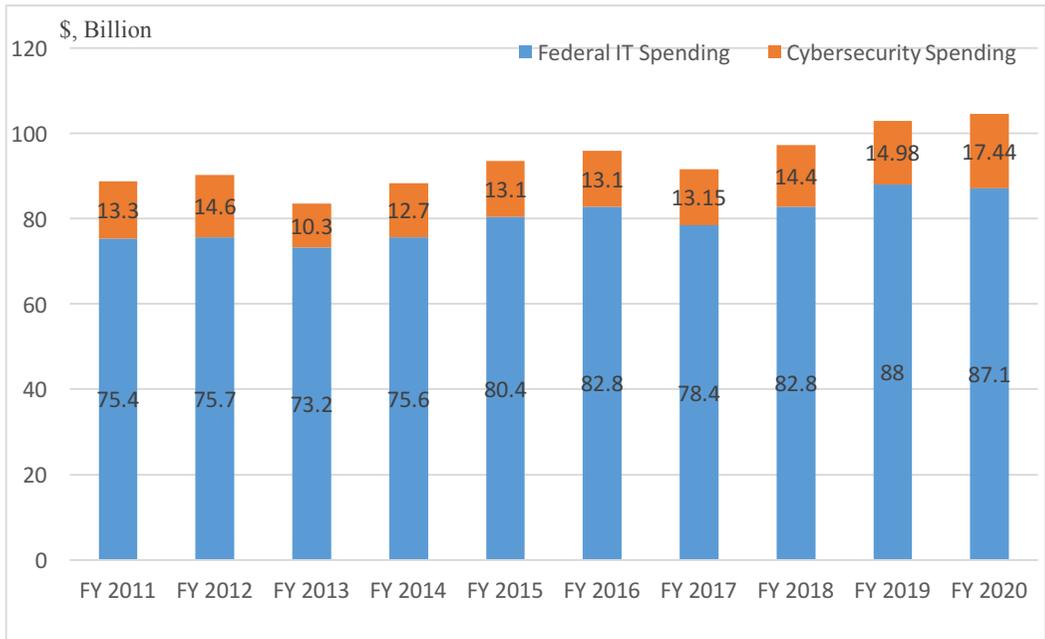
Although the federal government allocates increasingly greater proportion of the national budget in support of federal IT and cybersecurity, grasping the precise spending trends is challenging due to the variance in accounting methods across different sources. On top of this difficulty, there is no consensus on what the cybersecurity spending is exactly composed of. Notwithstanding these inherent challenges, this paper will refer to the Executive Office of the President OMB IT Dashboard, an official website of the U.S. Government which displays federal information technology online for federal agencies and public scrutiny. Government-wide IT spending is referred to as “the total budgetary resources based on Development, Modernization, and Enhancement (DME) and Operations and Maintenance (O&M) services.”<sup>54</sup>

The Cybersecurity spending is generally characterized by an upward trend, along with the Federal IT spending (refer to figure 3-2). In the more recent years however, from 2018-2020, the proportion of cybersecurity spending has seen even greater increase, which strongly correlates with the National Cyber Strategy plan in

---

<sup>54</sup> Office of Management and Budget, IT Dashboard <https://itdashboard.gov/> accessed 2019.

2018 to dedicate more resources towards strengthening national cybersecurity efforts.<sup>55</sup>



Source: Office of Management and Budget (2019)

**Figure 3-2** Federal IT Spending and Cybersecurity Spending FY 2011-2020

It is important to note that the graph is not an entirely comprehensive calculation of government-wide spending based on IT investments, as it omits sensitive classified IT spending and the IT Modernization fund.

<sup>55</sup> National Cyber Strategy of the United States of America 2018, available, <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

### **3.4 Public-Private Partnership: Critical Infrastructure Sector Partnership**

The U.S. has relentlessly emphasized public-private partnership as the backbone of cyber-security strategy.<sup>56</sup> The privatization of Critical Infrastructures in the 1990s, relying on private-sector efficiency and business practices awakened the need for a public-private partnership early on. Since a large proportion of national critical infrastructure is privately owned and operated, public-private sector partnership which facilitate integrated and cooperative engagement are critical to critical infrastructure security. Such partnerships are to foster an environment conducive to information-sharing on critical threat information, risk mitigation, and other crucial pieces of information.

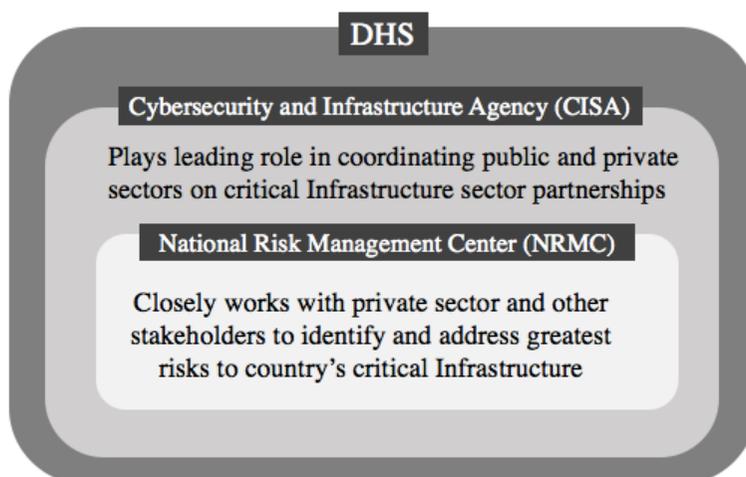
The DHS Cybersecurity and Infrastructure Security Agency (CISA) plays a leading role in coordinating the public and private sectors on critical infrastructure sector partnerships. CISA seeks to form national capacity to defend against cyber attacks in collaboration with the federal government. In order to protect government networks which underpin critical operations of partner departments and agencies, CISA provides cybersecurity tools, incident response services and assessment capabilities.

Housed within the CISA is the National Risk Management Center (NRMC) which undertakes planning, analysis, and collaboration center in order to identify and address the the greatest risks to the country's critical infrastructure. In doing so, the

---

<sup>56</sup> William J. Clinton, National Plan for Information Systems Protection Version 1.0: an invitation to a dialogue (Washington DC: The White House, 2000); George W. Bush, The National Strategy to Secure Cyberspace (Washington DC: The White House, 2003).

NRMC closely works with the private sector and other important stakeholders in the critical infrastructure sector to “identify, analyze, prioritize, and manage” risks and vulnerabilities to national critical infrastructures. Damage or disruption to the national critical infrastructure functions would have a severely crippling ramification on the country’s security, economic security, public health, etc. Refer to Figure 3-3 below for the U.S. Public-private partnership management structure in the DHS.



**Figure 3-3** U.S. Public-Private Partnership Management Structure in the DHS

With regards to Critical Infrastructure sector partnerships structure, the National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience lays out a systematic framework for a structured partnership between the public and the private sector for Critical Infrastructure protection. More specifically, the NIPP outlines mechanisms for private sector owners and operators and government agencies’ cooperation. It also

categorizes the country’s critical infrastructure into the following 16 sectors (refer to Table 4-1), with sector-specific agencies (SSAs) identified in accordance to each sectors. Furthermore, it outlines the partnership requirement between the federal government and private critical infrastructure owners.

---

**Table 3-1** Sixteen Critical Infrastructure Sectors in the United States

---

Chemical Sector  
Commercial Facilities Sector  
Communications Sector  
Critical Manufacturing Sector  
Dams Sector  
Defense Industrial Base Sector  
Emergency Services Sector  
Energy Sector  
Financial Services Sector  
Food and Agriculture Sector  
Government Facilities Sector  
Healthcare and Public Health Sector  
Information Technology Sector  
Nuclear Reactors, Materials, and Waste Sector  
Transportation Sector  
Water and Wastewater Systems Sector

---

Source: Department of Homeland Security U.S. (2019).

The Critical Infrastructure Partnership Advisory Council (CIPAC), which supports NIPP implementation, contributes operational framework for undertaking sector partnership structure. More specifically, the CIPAC fosters public-private cooperation, information-sharing across the entire Critical Infrastructure protection by coordinating the private owners of critical infrastructure, trade association

members of Sector Coordinating Councils (SCC) and members of Government Coordinating Councils' (GCC) engagement. The Sector Coordinating Councils are self-organized and governed councils which facilitates the interaction of critical infrastructure owners and other relevant stakeholders for deliberating on sector-specific strategies, policies, and activities. The Government Coordinating Councils, created as government version of each SCC is composed of diverse governmental levels, and facilitate in interagency and cross-jurisdictional collaboration. Furthermore, the Critical Infrastructure Cross-Sector Council seeks to assist in cross-sector issues for SCCs, whereas the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) seeks to integrate various levels of the government in the protection of national Critical Infrastructures.

The provision of a systematic framework for coordinating public-private partnership under the DHS CISA, together with the underpinning legal-institutional provision of the aforementioned Cyber Information Sharing Act of 2015, synergistically contributes to consolidating an effective trust-based public-private partnership in the U.S for Critical Infrastructure protection.

### **3.5 Federal Cybersecurity Monitoring and Evaluation Systems**

This section examines the operation of monitoring and evaluation systems of federal cybersecurity in the U.S.

The Office of Management and Budget is in charge of conducting the overall cybersecurity evaluation of federal agencies through the President's Management Council (PMC)<sup>57</sup> and Federal Information Security Management Act reporting. Furthermore, some federal agencies such as the Department of Defence or Department of Justice have formulated internal cybersecurity dashboards to track their progress.<sup>58</sup>

The OMB publishes the Federal Cybersecurity Risk Determination Report and Action Plan to the President of the United States, which encapsulates the OMB's evaluation of cybersecurity risk management capabilities across the Federal agencies, and identifies mission critical cybersecurity gaps which ought to be patched. In producing the Risk Report, the OMB in collaboration with the DHS conducted a detailed evaluation of Federal cybersecurity by assessing the cyber capabilities of 96 civilian agencies across 76 metrics to examine the agencies' ability to identify, detect, respond and recover from adverse cyber breaches.

---

<sup>57</sup> The PMC advises the President and the Office of Management and Budget (OMB) on government reform initiatives, provides performance and management leadership throughout the Executive Branch, and oversees implementation of government-wide management policies and programs. The PMC comprises the Chief Operating Officers of major Federal Government agencies, primarily Deputy Secretaries, Deputy Administrators, and agency heads from GSA and OPM.

<sup>58</sup> Kate Charlet, "Understanding Federal Cybersecurity," *Harvard Kennedy School Belfer Center for Science and International Affairs* (2018).

The OMB's Federal Cybersecurity Risk Determination refers to Key Performance Indicators (KPI) on cybersecurity across the U.S. government agencies, published on performance.gov, an official website of the U.S. government. Based on the performance summary derived from KPI, the OMB produces quarterly summary of progress and draws relevant action plans. The performance summary adheres to the following goal structure: enhance Federal IT and Digital Services, Reduce Cybersecurity Risks to Federal Mission, and Build a Modern IT Workforce.

The KPI is categorized into the following three areas: Management Asset Security (Hardware Asset Management, Software Asset Management, Authorization Management, Mobile Device Management), Limit Personal Access (Privileged Network Access Management, High Value Access Management, Automated Access Management), and Protect Networks and Data (Intrusion Detection and Prevention, Exfiltration and Enhanced Defenses, Data Protection). It closely tracks the progress of federal agencies' cybersecurity levels and provides comparisons between the agencies along with their respective performance from the previous fiscal year.

Although there exists room for further improvement in systematizing the monitoring and evaluation of federal cybersecurity posture in the U.S., such efforts are currently being pursued under the purview of the OMB. Furthermore, the Risk Report is intended to drive strategic investment into the cybersecurity areas which require greater budgetary allocation to ultimately lower the cybersecurity risk.

# CHAPTER IV

## **An Analysis of South Korea's National Cybersecurity Governance System on Critical Information Infrastructures**

### **4.1 An Overview of South Korea's National Cybersecurity Challenges**

Korea acknowledges the realm of cybersecurity as a critical part of national security in light of the major cyber attack experiences such as the January 25<sup>th</sup>, also referred to as "1.25" Internet Chaos in 2003, July 7<sup>th</sup> DDOS- Distributed Denial of Service Attack in 2009, June 25<sup>th</sup> cyber attacks in 2013, cyber attack on Korea Hydro and Nuclear Power (KHNO) plant in 2014, hacking incident of national defense data integration center which serves as the backbone of national defense network, etc.<sup>59</sup> In particular, the KHNO cyber incident sparked national interest, as North Korea stole critical information from KHNO through various channels, risking the safety and lives of South Korean citizens.

Despite possessing one of the world's fastest and most mobile IT infrastructures, and being one of the most cyber dependent countries, Korea has relatively insecure infrastructures vulnerable to cyber-attacks. Previously, hackers have compromised sensitive information and the welfare of government officials and

---

<sup>59</sup> Sangbae Kim, "Cyber Security and Middle Power Diplomacy: A Network Perspective." *The Korean Journal of International Studies* 12, No. 2 (2014): 323-352.

civilians by targeting government agencies, and the increasing frequency and gravity of cyber attacks have led the Korean government to reassess and re-strategize national cybersecurity.

North Korea's cyber attack capabilities have grown leaps and bounds with the establishment of the Reconnaissance General Bureau in February 2009, based in Pyongyang. The Bureau conducts hacking activities primarily in mainland China, crippling systems and forging key secrets of major agencies in South Korea. It is estimated that North Korea's cyber capabilities are only few steps behind those of the U.S. and China, and in comparison to that of South Korea's the gap is alarming. Personnel securement in undertaking cyber attacks in North Korea is also behemoth, with approximately 1200 personnel charged with hacking plans, 1800 personnel for technical support, and 3000 cyber agents from other supporting organizations.<sup>60</sup> During peacetime, North Korea's cyber attacks could result in stirring up social chaos; however, in the event of a war, it has the capacity to paralyze almost all information dependent infrastructures in South Korea, which could potentially determine the outcome of the physical war. Table 4-1 is a non-exhaustive list of major cyber attacks launched by North Korea on South Korea.

---

<sup>60</sup> Momoko Kidera and Ryotaro Sato, "North Korean hackers' evolution on display in US case," *Nikkei*, September 11, 2018, accessed March 13, 2019, <https://asia.nikkei.com/Spotlight/N-Korea-at-crossroads/North-Korean-hackers-evolution-on-display-in-US-case>.

**Table 4-1** List of North Korea’s Major Cyber Attacks Against South Korea

Incident	Year	Damage Content
7.7 DDos Attack	2009	Attack on the Blue House, National Intelligence Service, major medias, political parties, banks, portal sites.
3.4 DDos Attack	2011	Denial of service on 40 major domestic institutions
Nonghyup Bank Computer Network hacking	2011	Large scale data damage and service paralysis due to Nonghyunp bank computer network hacking.
3.20 Cyber Terror	2013	Major broadcasting stations (KBS, MBC, YTN), Financial Enterprise (Shinhan bank, Nonghyup, Jeju bank) computer network paralysis, simultaneous paralysis of 32000 computers.
6.25 Cyber Terror	2013	Tampering with Blue House and Office of Government Policy coordination homepage, DDos attacks against National Computing and Information service, 43 private enterprises including newspaper and broadcasting stations’ computer network paralysis and homepage modulation.
KHNO hacking	2014	Nuclear power plant blueprint, nuclear power plant control program, resident radiation dose assessment and program file, KHNO employees 10799 personal information leakage, and threatened the shutdown of nuclear power plant using leaked information as leverage.
Seoul Metro lines 1-4 server hacking	2015	2 servers in charge of Seoul Metro PCs hacked, unauthorized access to 213 company computers. 58 found to be infected with a malicious code, resulting in the leak of 12 documents.
Blue House, National Assembly, hacking	2015	Personal computers, e-mail accounts in the Blue House, National Assembly were hacked, although no data have been stolen.
Blue House malicious code distribution	2016	Blue House National Security Office, Office of Foreign Affairs and Security, Unification Policy Office, Office of Foreign Affairs Policy misrepresented e-mails sent.

Concerning the response to North Korea's increasing cyber attacks on South Korea, South Korea has maintained vigilant, yet somewhat unresponsive posture towards North Korea. Currently, there are many barriers to forming an active response to North Korea's cyber attacks on South Korea due to sensitive diplomatic and military issues involved. Accordingly, pre-emptive or retaliatory cyber attacks on North Korea to strengthen cyber defense capability is not a viable option due to South Korea's asymmetric weakness. Not only does South Korea lack information infrastructure to launch cyber attack on North Korea, but there exist some potential for cyberspace retaliation to escalate into physical war, in which case South Korea has more to lose from its developed information infrastructure.<sup>61</sup>

The National Cybersecurity Strategy 2019 of Moon Jae-in Government identifies six strategic tasks in its first national cybersecurity strategy paper, which is published by the National Security Office of Cheong Wa Dae (Office of the President). The Strategy includes the following: Increase the safety of national core Infrastructure; Enhance cyber attack response capabilities; Establish governance based trust and cooperation; Build foundations for cybersecurity industry growth; Foster cybersecurity culture; and Lead international cooperation in cybersecurity.

For the purpose of this paper, which delves into cyber governance efforts in critical information infrastructure sectors, the aforementioned first three strategies of increasing the safety of national core Infrastructure, enhancing cyber attack response capabilities, and establishing governance based trust and cooperation will be

---

<sup>61</sup> Sangbae Kim, *National Strategy of Cyber Security* (Seoul: Critical Perspectives on Society Academy, 2017).

primarily referred. In particular, the second strategic task of cyber attack response capabilities is deemed the most relevant as this task deals with formulating cyber attack deterrence strategies, strengthening readiness against massive cyber attacks, devising comprehensive and proactive countermeasures for cyber attacks, and enhancing cyber capabilities.

## **4.2 An Analysis of the Cybersecurity Governance System of South Korea**

### **1) Legal and Institutional Systems**

This section seeks to explore the current legal and institutional system in support of national cybersecurity governance in South Korea. In doing so, the governance system, relevant cyber security legislation together with previous efforts to enact integrative cyber security bill will be identified.

South Korea adopts distributed management method for cybersecurity propulsion system, dispersing roles and responsibilities across the following fields: private sector (spearheaded by the Ministry of Science, Information and Communications Technology and Future Planning), public sector (spearheaded by the National Intelligence Service), and Military (spearheaded by the Ministry of National Defense). In January 2015, the Korean government designated Special Secretary of Cyber Security in the Blue House, and Secretary of Cybersecurity was appointed to oversee cybersecurity policies and initiatives by Korean governmental authorities. However, as a result of inefficient response to various cyber attacks, the National Intelligence Service (hereinafter referred to as the “NIS”), Korea

Communications Commission, Ministry of Defense, Ministry of Public Administration and Security, Financial Services Commission, together with fifteen relevant ministries and institutions since 2011 participated to establish National Cybersecurity Master Plan for the purpose of establishing public, private and military joint response system with the NIS at the center of coordination.<sup>62</sup>

#### **a. An Overview of Cybersecurity Laws**

The Framework Act on Information Promotion in 1995 established the foundation of cybersecurity laws in Korea, containing broad issues relevant to cybersecurity. In order to consolidate cybersecurity at the national level, Act on the Protection of Information and Communications Infrastructure (2001), and the Act on the Promotion of Digitalization of Administrative Work for E-Government Realization (2001), which was later renamed as the Electronic Government Act in 2007, were enacted in the new millennium. The January 25<sup>th</sup> Internet Crisis, also referred to as 1.25 Internet Crisis in 2003, led to the strengthening of cybersecurity laws in a bid to safeguard national information and communication networks. Consequently, in the following year 2004, the Network Utilization and Information Protection, Etc. was further bolstered along with the issuance of the National Cyber Security Management Regulation in 2005 under Presidential Directive, and the enactment of Electronic Financial Transactions Act in 2006.

Currently, there exist no overarching legal framework to effectively regulate national cybersecurity in a coherent manner in Korea. The laws pertinent to the cyber

---

<sup>62</sup> The Korean Government, *National Cybersecurity Masterplan Establishment* (Korea Communications Commission report, 2011).

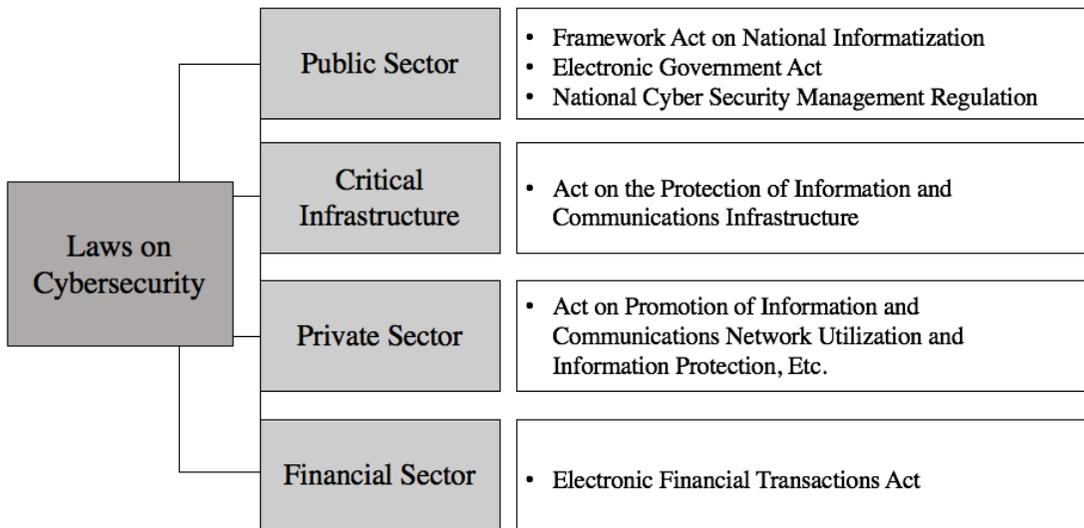
propulsion system are subject to separate statutes in accordance to specific sectors, thereby receiving different sector protection. For public sector cybersecurity, National Cybersecurity Management Regulation, Framework Act on National Informatization, and Electronic Government Act is applied. For the private sector, Act on the Promotion of Information and Communications Network Utilization and Information Protection, Etc. is applied. For the financial sector, Electronic Financial Transactions Act is applied. For critical information and communication infrastructure, the Act on the Protection of Information and Communications Infrastructure is applied, and provides protection for both the private and the public sector pertinent to critical information and communication infrastructure. Likewise, different statutes are applied in accordance to each specific sector, and is governed by separate propulsion systems each relevant to different ministries.<sup>63</sup>

---

<sup>63</sup> Min Sik Kim et. al, “Research on the Need for an Integrative Cyber Crisis Management System: Comparing U.S. and Korea’s Institution and Policies,” *Journal of Information Security* 9, no.1 (2009):56

## b. Key Cybersecurity Legislations in South Korea

Figure 4-1 more clearly illustrates the laws which underpin the following sectors: public sector, critical infrastructure, private sector, and the financial sector.



**Figure 4-1** Laws on Cybersecurity in Korea

## c. Bills for Nationwide Integrative Cybersecurity Responses

Bills pertinent to establishing an overarching national cybersecurity law have been continuously proposed since the 17<sup>th</sup> National Assembly. In December 2006, a bill relevant to cyber threat prevention and response had been proposed, yet, the bill's term was terminated without being examined, in the midst of discussing where the National Assembly Steering Committee ought to assign a sub-committee regarding cybersecurity. In a similar vein, another bill on National Cyber Crisis Management had been proposed during the 18<sup>th</sup> National Assembly, and placed on the intelligence

committee agenda in April 2009, but was also terminated without reaching the law-enforcement office. The 19<sup>th</sup> National Assembly marks the most active attempts to propose bills on cybersecurity, including Cyber Safety Management proposed in March 2013, Prevention of National Cyber Terror proposed in April 2013, Information-sharing on Cyber Threat proposed in May 2015. The bill on Cyber Terror Prevention and Response proposed in June 2015 had been examined through four stages, including the sub-committees drawing up alternatives and inviting experts for consultation on this matter, yet failed to reach final resolution. In February 2016, a sub-committee for agenda adjustment had been formulated, but also led to the denunciation of the bill without examination due to termination of the bill's term.<sup>64</sup> More recently, during the 20<sup>th</sup> National Assembly, a bill on Cybersecurity had been proposed by member of National Assembly representative initiative in May 2016, along with National Cybersecurity bill proposed by the government in January 2017 for examination in National Assembly Intelligence Committee. Despite the ongoing efforts to enact a new legislation on national cyber security, all of the initiatives to this date (February, 2019) had been denounced.

The most recent bill on National Cybersecurity proposed in May 2016, strived to establish more efficient response to national cyber threats. More specifically, since the public and private sectors' response to cyber attacks are separate and independent, an efficient response to a wide range of cyber threats on a

---

<sup>64</sup> Kwangho Kim, Sangdon Park, and Jongin Lim, "Changes of cybersecurity legal system in East Asia: focusing on comparison between Korea and Japan." In *International Workshop on Information Security Applications* (Springer, 2015): 348-356.

national level is challenging. In terms of the public sector, since appropriate response is based on the Presidential Order on National Cyber Safety Management Regulation, the private sector, institutional and judicial agencies other than administrative institutions, fall outside the scope of legal application. Concerning the private sector, the insufficiency of existing laws to prevent and respond to cyber attacks, significantly limits effective real-time detection and rapid response to cyber accidents. Therefore, the above-mentioned bill intended to foster legal environment conducive to government and private sector cooperation by establishing unified national-level response system to imminent cyber threats. In fulfilling the objective, the National Intelligence Service (chief intelligence agency of South Korea) was to serve as a control tower as it possesses top technology and knowledge in analysing and responding to cyber attacks in South Korea.

Notwithstanding the well-intended efforts, the NIS serving as the control tower sparked much controversy, as the bill would significantly expand the monitoring authority of NIS on the private sector. Under the proposed bill, mandatory information-sharing on cyber threats would extend the NIS authority to surveillance private information network, which could potentially lead to NIS abusing Personal Information Protection Act by invoking the exception clause under the pretext of cyber security, to carry out surveillance inspection on specific users. Furthermore, due to the lack of independent structure such as another cyber attack response institution within the government, National Assembly, or the court to place checks NIS activities, establishing Cyber Threat Information-sharing Centre within the NIS was deemed inappropriate. The historically deep-rooted public mistrust of NIS

activities is also another factor which renders the bill inappropriate for designating NIS to serve as a control tower for national-level cyber threats.

Taken together, although the NIS is best suited in terms of technological expertise and skills to play a chief role in coordinating effective public-private response to cyber attacks, excessive concentration of power in NIS, and its potential for excessive intervention in private sector has been identified as the greatest barrier to the passage of the bill.

#### **d. Critical Information Infrastructure Legislations**

The following section seeks to concisely introduce key elements of current legislations and regulations in support of separate, specific Critical Information Infrastructures: The National Cybersecurity Management Regulation, Act on the Protection of Information and Communications Infrastructure, Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters, Cyber Security Industry Enhancement Act, and Electronic Financial Transaction Act.

The National Cybersecurity Management Regulation was enacted under Presidential Direction in 2005, for the purpose of protecting national communication networks of central administrative agencies, local governments and public institutions, and to provide national-level response system against cyber attacks. According to the regulation, the Korean government authorities are to develop, establish and perform policies and initiatives pertinent to cybersecurity, in addition to outlining specific roles, duties and liabilities of government authorities. The regulation assigns the director of the NIS to control and coordinate policies and management pertinent to

national cybersecurity after consulting with the head of central administrative agency.<sup>65</sup> Furthermore, the regulation established the National Cyber Security Centre (hereinafter referred to as the “NCSC”) under the NIS in order to make more sophisticated and systematic response to cyber attacks which could pose grave threats to national security. The NCSC was ascribed the role of establishing national security policies, to assist in the operation of Strategy council and Counter plan council, collect, analyze and disseminate cyber threat information, ensure safety of national information and communication networks, outline and distribute national cyber security manual, investigate cyber accidents, support with restoration, and cooperate with foreign agency with regards to cyber threat information.<sup>66</sup> In the event of an adverse cyber incident, the head of central administrative agency, the head of local government and the head of public institutions are to immediately inform the Director of National Security Office and the Director of NIS. Pursuant to this, the Director of NIS is to take relevant necessary measures in response to the nature of the cyber incident. It is important to note that this regulation applies only to the public sector and does not govern the private sector.

The Act on Protection of Information and Communications Infrastructure has been enforced since 2002 to systematically and comprehensively respond to cyber attacks on Critical Information Infrastructure. The Act specifies a systematic structure in which protections are to take place, provisions on designation of information and communications infrastructure, evaluating vulnerabilities, establishing protection

---

<sup>65</sup> Cyber Security Management Regulation, Article 5

<sup>66</sup> Cyber Security Management Regulation, Article 8

plans, responding to cyber incidents and relevant penalties. Information and communications infrastructure, according to the Act on the Promotion of Information and Communications Network Utilization and Information Protection, refers to “infrastructures based on electronic systems to manage and control, and is relevant to national security, including defense, finance, communications, transportation, energy and information and communications network”.<sup>67</sup> The Act designates specific CII as be one of the following, i) critical transportation facilities, such as roads, railroads, subways, airports and harbors; ii) facilities for water resources and energy, including electricity, gas and oil; iii) relay broadcast facilities and the national command control communication network; iv) research facilities of government-funded research institutes related to nuclear energy, the national defense and science, or advanced defense industry.<sup>68</sup>

The Act outlines pro- and post-measures to ensure safe cyber-security environment in CII. For pro-protection measures, the Act stipulates creation of committee for CII protection under the Prime Minister, in order to provide effective nation-wide response system on CII. The committee is tasked with policy coordination on CII protection. Furthermore, the Act confers power to the heads of Central Administrative Agency (CAA) to designate information infrastructures as CIIs, which are operated by Management Agency (MA)s. Then, the MA is responsible for conducting regular assessment and evaluation of the CII it is in charge

---

<sup>67</sup> Act on Promotion of Information and Communications Network Utilization and Information Protection, Article 2 para.1-1

<sup>68</sup> CIIP Act, Article 7. para.2

of. Following the evaluation of the CII's vulnerabilities, the MA is to establish and implement necessary protection measures, and the NSCS, Ministry of Science, Information and Communications Technology and Future Planning (hereinafter referred to as "MSIP") and Ministry of National Defence possess the rights to review whether proper CII protection measures are implemented by MA. Separate reviews are conducted in accordance to the relevant sector. In conducting CII protection reviews, the NCSC is responsible for reviewing public sector MAs, the MSIP is in charge of reviewing private sector MAs, and the MND is tasked with reviewing military sector MAs.

In terms of post-protection measures, there exist three components: notification, resilience measures, technical assistance. For notification, the MA is to notify relevant administrative authorities and law enforcement authorities in the event of an adverse cyber incident. For resilience measures, the MA is to take necessary measures to ensure the resilience of the CII after the cyber intrusion. For technical assistance, the MAs may request technical assistance to the NSCS, MSIP or other specialized institutions as prescribed in the Presidential Decree. However, the NCSC cannot provide technical assistance to any information infrastructure which contains personal information.<sup>69</sup>

---

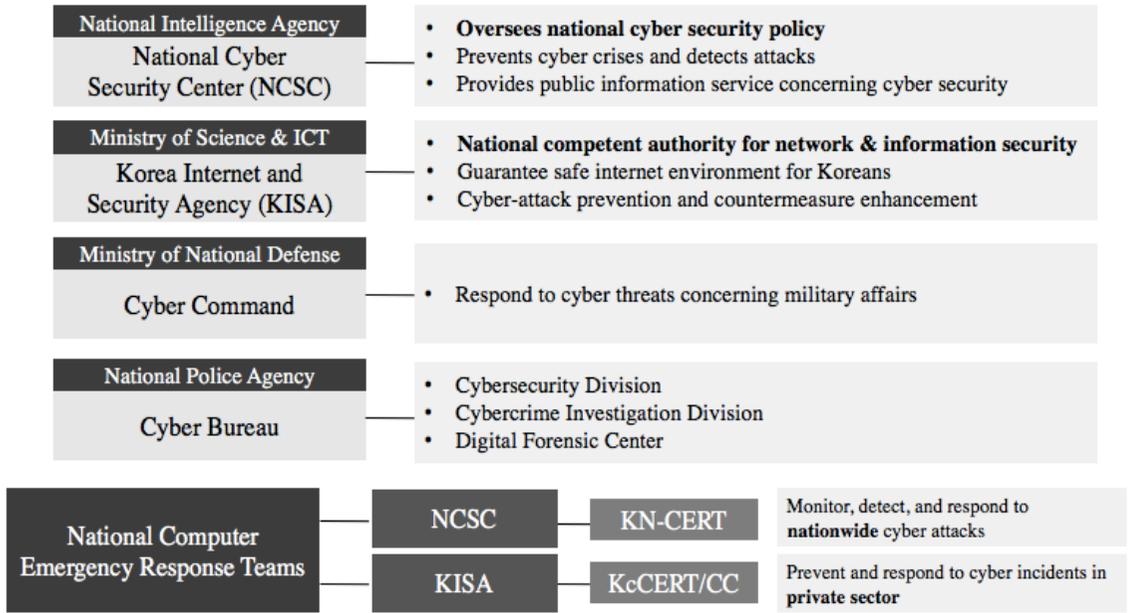
<sup>69</sup> CIIP Act, Article 12

## **2) Administrative System for Critical Information Infrastructure**

The National Security Research Institute (hereinafter referred to as “NSRI”) established in 2000 serves to research and enhance the national security system, national cyber safety technology, national security infrastructure technology, and to provide technical assistance for national security, technology policy establishment support, train manpower, commercialize technology, and implement necessary projects.

The Korea Internet and Security Agency (hereinafter referred to as “KISA”) was established in 2009 as a sub-organization of the Ministry of Science and ICT, by merging the following organizations: Korea Information Security Agency (KISA), National Internet Development Agency (NIDA) and the Korean IT International Cooperation Agency (KIICA). KISA seeks to promote safe internet environment, by offering various technical support for Internet cybersecurity, such as the Korea Computer Emergency Response Team Coordination Center (KrCERT/CC) for the private sector. On top of the internet cybersecurity, it offers personal information protection, internet and information security related policy research, electronic government service security improvement, cyber-attack prevention and countermeasure enhancement, and critical information communications infrastructure protection. For the protection of critical information communications infrastructure, KISA regularly performs analysis and evaluation of infrastructure weakness, facilitates in the provision of necessary technologies, and offers relevant

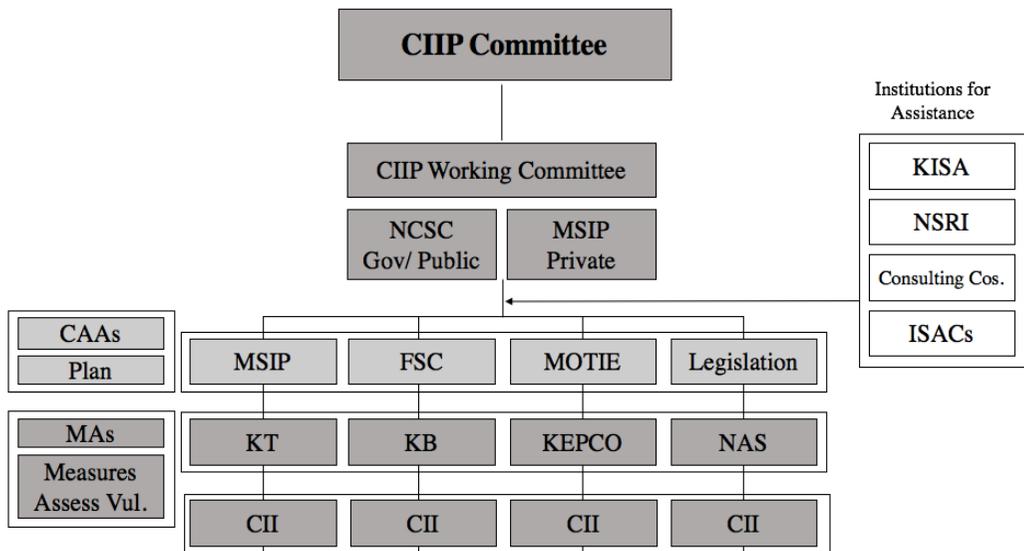
security measures.<sup>70</sup>



**Figure 4-2** Relevant Agencies Responsible for National Cybersecurity in Korea

<sup>70</sup> Korea Internet and Security Agency, <https://www.kisa.or.kr/eng/main.jsp>.

The Information Sharing and Analysis Center (hereinafter referred to as “ISAC”) was established under the Information and Communication Infrastructure Protection Act, and offers real-time response system in accordance to the relevant sector when critical information and communication infrastructure is breached due to cyber terrorism or other information breaches. In doing so, companies can form joint-response for information protection to mitigate the expense and workload, as opposed to when it is operated separately in specialized organizations. Currently, the Financial Supervisory Service operates the financial ISAC and telecommunication service providers operates the telecommunication ISAC.



Source: Korea Legislation Research Institute (2016)

**Figure 4-3** Management System of the Critical Information Infrastructure Protection

Currently, the Korea government identifies nine critical sectors which comprise its national critical infrastructure (see Table 4-2).

---

**Table 4-2** Nine Critical Infrastructure Sectors in South Korea

---

Energy Sector  
Telecommunications Sector  
Transportation Sector  
Financial Services Sector  
Healthcare and Medical Services Sector  
Nuclear Energy Sector  
Environment Sector  
Government Critical Facilities Sector  
Water Supply Sector

---

For the protection of critical infrastructures of nuclear energy sector, the Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters seeks to protect nuclear power plants from cyber attacks. Energy infrastructure protection from cyber attacks are enforced in accordance to the measures, plans and response processes as delineated in the Act. Two major Acts exist in support of nuclear power plants: Nuclear Safety Act and Nuclear Protection and Prevention Act. Whereas the former seeks to provide protection on issues relevant to safety managements in research, development, production, proper use of nuclear energy, in order to prevent radiation disaster and to ensure public safety, the latter seeks to bolster nuclear facilities' protection system against new threats such as cyber terror, and to establish effective radiation disaster management system based on legal and institutional frameworks.

The Korea Institute for Non-proliferation and Control (hereinafter referred to as “KINAC”) was established under the Nuclear Safety Act for the purpose of taking necessary steps to safeguard nuclear energy facilities and nuclear materials, and to control import and export of nuclear materials.<sup>71</sup> In addition, the KINAC has been entrusted by NSSC with conducting threat assessment, reviewing approval of physical protection facilities and installation, physical protection regulations and protection emergency plan, and inspections on physical protection. Following this, the KINAC has also formulated cybersecurity standards for nuclear power facilities.

In response to the North Korean cyber attacks against KHNP in 2014, protection of nuclear facilities systems from cyber attacks arose as key national agenda. Under the Nuclear Protection and Prevention Act, the KINAC established KINAC/RS-015, to establish efficient prevention, detection, and response system against adverse cyber incidents, and should cyber attacks occur, minimize the impacts and recover from the cyber attacks. More specifically, the main contents of KINAC/RS-015 are as follows. First, nuclear business operators are to form an independent and separate Cyber Security Team (CST). Second, nuclear business operators are to identify Critical Digital Assets (CDA)s, which refers to all digital assets whose systems and components perform Safety, Security, and Emergency Preparedness (SSEP) function. CDAs require protection against cyber attacks, and are connected either directly or indirectly with the critical system. Third, the operators

---

<sup>71</sup> Nuclear Safety Act, Article 6

are to establish a Defence-in-Depth (DiD) strategy<sup>72</sup>, to classify the degrees of cyber security to protect code digital assets. Fourth, the operators are to apply fundamental cybersecurity measures to CDA, consisting of technical, operational and management security measures. Lastly, the operators are to practice sustainable cybersecurity programs by continuously assessing and detecting vulnerabilities and reviewing the cybersecurity programs.

The following will examine legislations pertinent to promoting cybersecurity in financial transactions industry, securing electronic financial transaction and protecting personal Information.

The Electronic Financial Transaction Act (hereinafter referred to as “EFTA”) was enacted in 2006 in order to ensure safety and reliability of electronic financial transaction. The Act seeks to clarify legal relations and foster safe and convenient electronic financial industry for the people, and ultimately contribute to competitiveness of the national economy. The Act specifies electronic financial transaction as financial transaction such as banks, credits, securities, insurance, etc., through the means of electronic apparatus. It is critical for a financial company or an electronic financial business to selectively utilize means of access necessary for electronic financial transactions to accurately confirm the identity of a user.<sup>73</sup> A financial company or an electronic financial business possesses a duty to ensure

---

<sup>72</sup> Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack. This multi-layered approach with intentional redundancies increases the security of a system as a whole and addresses many different attack vectors.

<sup>73</sup> EFTA, Article 6. para.1

security to their users, and in doing so, they are required to comply with the standards related to the security and certification technologies determined by the Financial Services Commission (hereinafter referred to as “FSC”), and analyze and assess the vulnerability of electronic financial infrastructure and submit the results to the FSC. In doing so, a chief information security officer is to be designated to oversee vulnerability assessment of the information technology sector. In the event of an adverse cyber incident in the electronic financial infrastructure, the relevant financial company and electronic financial business are to swiftly report the details to FSC, which will prescribe necessary measures to minimize the effects of the incident.

The Cyber Security Industry Enhancement Act (hereinafter referred to as “CSIEA”) was enacted and enforced in 2015 for the purpose of creating robust information communication environment to contribute to the competitiveness of national economy, through the prescription of required matters in cybersecurity industry promotion.<sup>74</sup> In order to promote the cybersecurity industry, various government financial support is granted under the Act. The Minister of MSIP may offer long-term low interest loans to cybersecurity company, and the government may grant tax deduction in accordance to the Restriction of Special Taxation Act, the Restriction of Special Local Taxation Act and other relevant tax Acts.<sup>75</sup> Such financial support is expected to bolster the safety of cyber ecosystem through the

---

<sup>74</sup> CSIEA, Article 1

<sup>75</sup> CSIEA, Article 21. para. 2

creation of credible cybersecurity market, whilst also consolidating systematic cybersecurity industry promotion.

The Act on Promotion of Information and Communication Networks Utilization and Information Protection, Etc. seeks to foster the use of information and communication network, protect information and communication service users' personal information, and create safe cyber ecosystem for the network. The key contents of the Act covers prohibition against any unauthorized intrusions to the information and communication networks, requires the service providers of information and communications to take preventative protection measures against adverse cyber incidents, form information security pre-inspection system of vulnerabilities, and obliges security incident reporting along with systematic analysis of incident cause.<sup>76</sup>

Framework Act on Informatization enacted in 1995, later amended and renamed as the Framework Act on National Information in 2009, was enacted to form the foundation of information and communication industry along with fostering high-speed. The perspective since 1995 has shifted from fostering informatization of society to fostering the utilization of information. The national informatization is to provide support for both public and private sectors pertinent to information security. In addition, information security systems are to be evaluated and certified by specified standards recommended by the Minister of Science, ICT and Future Planning.

---

<sup>76</sup> Act on Promotion of Information and Communication Networks Utilization and Information Protection, Etc. available [https://elaw.klri.re.kr/eng\\_service/lawView.do?hseq=38422&lang=ENG](https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG).

For developing a digital government, the Act on Promotion of Digitalization of Administrative Work for E-government Realization was enacted in 2001, and later amended and renamed in 2010 as the Electronic Government Act. The previous Act sought to enhance public service efficiency and productivity through electronic processing of administrative work. The more recent Act broadened administrative information-sharing mechanisms, along with the provision of more strengthened protection of information resources for the e-government. The key contents of the Act emphasize safe and reliable information system as the foundation of e-government. Furthermore, the Act confers power to the Director of NIS to implement and oversee the security measures.

Insofar, this section has sought to promote comprehensive understanding of legal-institutional situation of cybersecurity in Korea. In doing so, it has identified that the greatest impediment to forming streamlined national-level response to cyber attacks is due to the absence of an integrative legal framework which seeks to coordinate the public, and the private sectors. Despite a myriad of attempts to enact such law, the controversy over where to designate the control tower for national cybersecurity has further complicated the process, as the control tower must not only possess superior technical capability and know-how to deal with complex cyber attacks, but also be sufficiently trust-worthy for the private sector to share critical and sensitive pieces of information.

### **3) Finance and Budget Systems**

This section on the finance and budget systems seeks to analyze the trends of national cybersecurity spending, and determine whether sufficient resources are allocated in support of national cybersecurity.

The cybersecurity budget for the defense sector is allocated under the national defense information service budget item. The national defense budget for information service consists of information and communication infrastructure, maintenance of information system development, information protection, information and communication operation support, telecommunication charge, telecommunication facilities, and defense broadband integration network.

The national defense budget for South Korea has had massive increase from the previous years at 46.7 trillion Won for the 2019 fiscal year. Among the national defense budget composition, Information security budget is allocated 502.7 billion Won, and among the information security budget, information protection budget is allocated 55.5 billion Won, reflecting 11.2% and 39% increase respectively, compared to the previous 2018 fiscal year. Among the entire national defense budget, the proportion of information protection budget which took up 0.09% in 2018 increased to 0.154%. in the 2019 fiscal year.

The information protection budget is particularly crucial to protect national information systems from evolving cyber threats, and to build the foundation for future cyber warfare. As an alternative to the current trend of troop reduction, investment in information protection has arose as a sine qua non. In 2015, the national defense information service budget stood at 550.1 billion Won, and in 2016, there

was a significant budget cut to 460.2 billion Won. Since then, it took three years for the national defense information service budget to recover to the 500 billion Won range as it used to be in 2015.

The budget for information protection is further distributed across the following areas: network protection, software protection, hardware protection, cyber response, protection management, and encryption equipment. In 2018, the following three areas took up the largest proportion of the information protection budget: management expenses (36.3%), cyber incident response (24.1%), encryption equipment (17.8%).

**Table 4-3** Specific Items of Information Protection Budget 2018

(Unit: billion Won)

Category of items	Budget	Ratio (%)
Network protection	5.29	13.3
Software protection	0.74	1.9
Hardware protection	2.67	6.7
Cyber responses	9.58	24.1
Management expenses	14.4	36.3
Encryption equipment	7.06	17.8
Total	39.7	100.0

Source: Ministry of Defense, *2019 White Paper* (2019).

Table 4-4 indicates specific spending trends for National Defense Budget, National Defense Informatization Budget, and Information Protection Budget between 2015 to 2019.

**Table 4-4** Information Protection Budget of Korea (2015-2019)

Year	National Defense Budget (trillion Won)	National Defense Informatization Budget (billion Won)	Information Protection Budget (billion Won)
2019	46.7	502.7	55.5
2018	43.2	451.8	39.9
2017	40.3	471.7	37.9
2016	38.8	460.2	41.9
2015	37.5	550.1	38.5

Source: Ministry of Defense, *2019 White Paper* (2019).

For the purpose of securing professional personnel who will be responsible for upgrading the defense cyber capabilities, including reorganization of the organization and functions, the cyber command sharply increased personnel budget for military personnel from 142.7 billion Won in 2018 to 226 billion Won for 2019.

Among the cyber security budget, a total of 12.1 billion Won has been set aside specifically to bolster cyber capabilities. The following are the specific cyber budget allocation for 2019: establishment of a cyber operation control system and surveillance reconnaissance operation system (1.4 billion Won), upgrading cyber

defense operation system (1.1 billion Won), establishment of security verification system to detect and prevent cyber attacks against weapons systems (8 billion Won), and establishment of a cyber warfare training center to develop cyber warfare professionals. The cyber warfare training center is to create practical training ground by formulating a training environment similar to that of the real cyber warfare environment, and this specific budget allocation reflects the Korean government and Defense Ministry's intention to strengthen cyber security in preparation for future cyber warfare.

Although the Korean government has gradually increased the national cybersecurity budget, and has allocated greater resources towards developing more professional cyber security personnel, overall, the proportion of national budget allocated specifically towards cybersecurity lags far behind that of developed countries. Furthermore, due to the fragmented national cybersecurity governance among the public, private and military, the precise budgets for the public and private sector has not been indicated in this section.

#### **4) Public-Private Partnership**

The need for strengthening public-private partnerships has been identified in the National Cybersecurity Strategy paper, published for the first time in 2019. Among the six strategic tasks outlined in the National Cybersecurity Strategy the third strategic task concerns “establish governance based on trust and cooperation”, which incorporates facilitating public-private-military cooperation system, building and

facilitating a nation-wide information sharing system, and strengthening legal basis for cybersecurity.

Notwithstanding, currently as of April 2019, there exists no defined public-private partnership for national cybersecurity in Korea, and no formalized new public-private partnerships concerning cybersecurity. The Korea Internet Security Center (KrCCERT/CC) closely works with the private-sector in operating early warning system and coordinating incident response procedures, and offers Cyber Emergency Shelter program, which seeks to offer safe server environment for SMEs in the event of an adverse cyber incident. Likewise, although the KrCERT/CC cooperates with the private sector in terms of incident response duties, there is an overall absence of a formal public-private partnership for cybersecurity in Korea. Furthermore, the same situation as above holds true for sector-specific cybersecurity as well. Currently, there is a lack of public consensus on sector-specific security priorities, along with an absence of joint public-private sector plan to address cybersecurity.

Accordingly, public-private partnerships in cybersecurity in Korea is deemed minimal and inadequate in effective protection of Critical Information Infrastructures. Such lack of public-private partnership renders critical information-sharing pertinent to cyber threats particularly challenging.

## 5) Monitoring and Evaluation Systems

Monitoring and evaluation systems play a pivotal role in identifying the most valuable and efficient use of limited resources. More specifically, the monitoring and evaluation systems trace the progress of specific national cybersecurity goals, determine whether national cybersecurity related policies or programs have had any measurable impact and have been effectively implemented. It facilitates in the understanding and attaining of key information for policy makers, managers and implementers to reach informed decisions regarding cybersecurity program operations. Moreover, monitoring and evaluation seeks to yield objective and systematic data to guide strategic planning, formulate and implement policies or programs, and finally re-allocate limited budget in the most efficient manner.

The public sector cybersecurity performance evaluation is stipulated in the Information Security Industry Promotion Act of 2015: *The government shall reflect information security performance (i.e. managerial, technical and physical information security measures and the performance thereof) through an evaluation of the management performance of public sector organizations.*<sup>77</sup> On the other hand, for the private sector, The Ministry of Science, ICT and Future Planning is generally responsible for evaluating policy performance, and monitoring the proper implementation of national cyber strategy.

Nonetheless, comprehensive national-level cybersecurity monitoring and evaluation systems have not been formally established in Korea, although their

---

<sup>77</sup> Information Security Industry Promotion Act of 2015

necessity have been recognized in the 2019 National Cybersecurity Strategy paper. According to the strategy paper, the National Security Office is to frequently monitor the implementation of the indicated cybersecurity goals and strategy, and evaluate the appropriateness of the cybersecurity framework to implement the Strategy.<sup>78</sup> In doing so, the Office seeks to review the efficiency of cybersecurity execution strategies which reflects the rapidly evolving cyber-threat environment.

Pertaining monitoring and evaluation systems more specifically for Critical Information Infrastructure, the Strategy Paper seeks to formulate evaluation standards for sector-specific vulnerabilities and execute measures to promote uninterrupted availability of services. Further, to bolster Korea's cyber-readiness posture, information-sharing system, investigation and response by relevant agencies are to be evaluated. Specifically, the Ministry has revealed an intention to place greater emphasis on information security investment in evaluation programs to reinforce the security level of private entities along with the critical information infrastructure.

Likewise, the necessity and intentions to provide a national level cybersecurity monitoring and evaluation system has been identified; however, a more detailed, practical and systematic plans are yet to be established.

---

<sup>78</sup> Cheong Wa Dae, *National Cybersecurity Strategy 2019*, (National Security Office, 2019).

# **CHAPTER V**

## **Policy Measures to Consolidate the National Cybersecurity Governance System in South Korea**

This chapter seeks to contribute practical and specific policy recommendations to restructure cybersecurity governance in Korea. Although previous literatures have put forth constructive policy suggestions to rectify the highly fragmented cybersecurity governance in Korea, the suggestions are deemed rather general, offering recommendations broadly on “what” the country ought to pursue, or focus on one specific sector, when a comprehensive approach is required to consolidate national cybersecurity governance. Accordingly, this chapter seeks to extend the previous literatures broad recommendations by specifying “how” cybersecurity governance ought to be restructured by incorporating the requirements for the successful governance system. This chapter is divided into two sections, the first section intends to suggest the measures to create robust the cybersecurity governance system following the five dimensions of analysis mentioned in Table 2-1, whereas the second section seeks to suggest future policy direction to engineer a cyber resilient governance in order to pursue a sustainable national cybersecurity governance system.

## **5.1 Policy Suggestions to Consolidate the Cybersecurity Governance System**

### **1) Legal and Institutional Systems**

Enactment of integrative law and ordinance comprising the prevention of, responses to, and restoration from cyber attacks, the strengthening of cyber security, and the cooperation between public and private sectors is required. Currently, the relevant laws and systems underpinning national cybersecurity governance are generally scarce, and are characterized by high levels of fragmentation across different government departments and ministries, rendering it challenging to apply consistent laws. Accordingly, an integrative legislation pertinent to national cybersecurity is sorely needed. Should such integrated law be enacted, the director ought to be placed under the Prime Minister's Office, rather than at the National Intelligence Service, as the integration and coordination of law enforcement is smoother when pursued under the jurisdiction of higher government departments than other ordinary government departments.

The content of the relevant integrative cybersecurity Act should include provisions for each phase of cybersecurity and response to cyber attacks (prevention of cyber attacks, response systems and methods in the event of cyber attacks, rapid recovery and strengthening of existing systems, etc.) More specifically, the Act should include the status of the control tower, the scope of functions and roles of each government ministry, mandatory cooperation among different ministries, solutions to create, accumulate, archive and share information, the composition and functions of related committees, budget support, privacy measures, monitoring and evaluation

systems by the National Assembly or Independent administrative agencies, and procedures for objection applications and penalties. Furthermore, the provision of a law which enables the government regulation of cybersecurity violation in the private sector is also required.

Second, specific and feasible guidelines for performing tasks pertinent to national cybersecurity or response to cyber attacks should be created. This ought to be supervised by the Presidential Office or the Prime Minister's Office, and the National Intelligence Service and other relevant government ministries should work together to create official manuals or guidelines for the prevention and response to cyber attacks and distribute them to pertinent government agencies and private cybersecurity agencies. In the event of an actual cyber attack, such guideline or manual will facilitate in forming a more orderly and unified action among related entities.

Third, the system for protecting personal or sensitive information and prevention of human rights violations should be reinforced. Although prevention is the most critical and desirable element, cyber attacks can infringe upon personal information and privacy and on human rights under the pretext of prevention. Furthermore, there exists room for potential illegal inspection and behind-the-scene investigation. Therefore, detailed records should be traceable on the scope of pre-information collection for individuals, personnel for information collection, purpose of information gathering, contents of information collection, and details of information utilization. The traceable elements of a detailed record can prevent excessive abuse of personal or private information, and will facilitate rights relief in

the event of a mistake. Legal recourse through punishments for utilizing personal information for personal use or without permission should also be clearly outlined. The institutionalized information collection procedures or methods seeks to prevent unauthorized Information collection, and human rights violation in advance.

Fourth, measures should be developed to separately manage military and civilian information pertinent to national cybersecurity. Sensitive military Information should be prevented from information leakage by prescribing higher-level of confidentiality, while private information should be co-shared with public agencies and the private sector, except personal information, and information regarding people or domains which are at higher risk of cyber attack.

## **2) Administrative System**

First, tentatively named “National Cybersecurity Council” could be established as the cybersecurity governing body to strengthen the control tower functions within the government. The Coordination Committee should be formed around vice-ministerial officials from relevant agencies, including the Presidential National Security Office, the Prime Minister’s Office, the National Intelligence Service, the Ministry of National Defense, the Ministry of Government Administration and Home Affairs, the Information and Communication Committee, and the National Police Agency. Practical issues on the comprehensive prevention, response and recovery of cybersecurity should be discussed, with each ministry carrying out clearly allocated task, function, and coordination. This organization can be placed under the National Security Office at Cheong Wa Dae, or the National

Intelligence Service.

Second, since cyber attacks take place in a variety of sectors irrespective of department jurisdiction, and cybersecurity requires sophisticated technical expertise, the system of cooperation and coordination at the working-level manager should be reinforced. Thus, although national level coordination and cooperation is crucial, the frequent information-sharing among working-level staff in relevant agencies is critical to form a joint-response in the event of an adverse cyber incident. In particular, due to strong sectionalism in Korea's administrative organization, frequent information exchange among working-level officials, and establishment and operation of an adjustment system is required for joint-response to cyber attacks.

Third, national cybersecurity ought to be bolstered at the local government level. Currently, cyber attacks are not limited to the central government level, but also occur in areas directly related to the daily lives of citizens at the local government level. Such cyber attacks which intends to disturb public sentiment and foment social chaos are referred to as the rear infiltration method. In particular, the potential for cyber attacks on local government networks is deemed high due to their relatively vulnerable cybersecurity status. To illustrate, the local government water supply-related agencies are deemed highly susceptible as a target due to its lower cybersecurity levels and knowledge. Accordingly, the role of cybersecurity agencies should be strengthened at the local level, and in responding to adverse cyber incidents, measures ought to be clearly established to closely collaborate with the central government.

Fourth, cybersecurity monitoring system should be established. Prevention is an important element of cybersecurity, and information collection on individuals is required. However, collecting information on individuals also has a myriad of dysfunctions such as infringement of human rights and protection of privacy. Furthermore, inadequate management of the collected information could potentially lead to information abuse or improper leakage, which could rattle the foundation of democracy. Therefore, close monitoring and supervision of agencies and personnel in charge of cybersecurity is necessary. To this end, the government should supervise the Board of Audit and Inspection (BAI), which currently carries out its supervisory functions for government agencies, by incorporating a separate cybersecurity audit function. Meanwhile, external to the government, cybersecurity monitoring body should be established under the National Assembly's Intelligence Committee to place double layer of surveillance.

Fifth, proactive detection and prevention against cyber attacks should be strengthened. Cybersecurity begin with effective prevention against cyber attacks; therefore, raising awareness for everyday users of cyber devises, paying more attention to information security, and establishing a system for immediate cyber attack report is required.

Sixth, virtual cyber attack training system should be strengthened. Similar to the idea of a civil defence training which provides general training to prepare for enemy aggression, simulation training in preparation for cyber attacks can minimize confusion and expedite efficient response. For this purpose, cybersecurity related institutions within the government as well as quasi-public institutions such as the

Korea Electric Power Corporation, Korea Hydro and Nuclear Power Co. and Korea Internet and Security Agency should participate in the simulated training. Furthermore, major private-sector cybersecurity agencies should also selectively participate in the training.

Seventh, emergency response system against cyber attacks ought to be established. Cyber attacks are never pre-announced and launched in advance as is the case in a general warfare, but are launched without prior warning. Therefore, in the event of a cyber attack, the formation of rapid response systems should be established in advance for emergency recovery. This is a similar concept to the 119 system at the fire station or the emergency centre at the hospital.

Eighth, education and training on cybersecurity ought to be strengthened. Preventing cyber attacks and bolstering cybersecurity critically depends on the availability of competent cybersecurity professionals. Since the majority of private-sector officials lack the concept of national cybersecurity, education on overall information security, including national cybersecurity is required. Accordingly, various measures including the establishment of contract departments to foster manpower in University and graduate programs, regular education training for cybersecurity personnel in public or private institutions, and overseas field-training in advanced countries such as the U.S. should be undertaken.

### **3) Finance and Budget Systems**

First, the importance of national cybersecurity should be recognized, and appropriate levels of cybersecurity budget should be allocated. Due to the intermittent nature of cyber attacks, there is a proclivity to pay attention only during the event of an adverse cyber incident, and dismiss the importance of addressing the incident through the natural passage of time. Therefore, the institutions, organizations and budgets pertinent to national cybersecurity is characterised by instability. Accordingly, the National Assembly's Intelligence Committee and related government agencies ought to work together towards securing a more stable cybersecurity budget, by increasing the budget by a larger margin than its current allocation. As previously emphasized, since prevention is critical in cybersecurity, injecting budget for establishing preventative system is deemed fundamental.

Second, the Integrated Budget and Consolidated Financial Statements should be prepared for managing cybersecurity related budgets in a coherent manner. Currently, there is a lack of consensus on the concept and scope of national cybersecurity, and agencies in charge of national cybersecurity are scattered across various government departments and agencies. Simply put, the fragmented cybersecurity budget system renders effective control and coherent policy formulation challenging. Accordingly, budget planning by the Ministry of Strategy and Finance and budget review by the National Assembly should be organized separately by the aforementioned cybersecurity control tower organization. This is to draw up a consolidated budget report and formulate consolidated financial statements for systematically organized revenues and expenditures of the cybersecurity budget.

Such efforts would facilitate in clear trend identification in the annual cybersecurity budget, identification of which departments demand greater budgetary support, and prevention of fragmentation and lax operation of cybersecurity policies or programs. Currently, the rigidity and fragmentation of the government budget system is posing serious budgetary waste.

Third, the control function of the cybersecurity budgets should be strengthened. The current budget pertinent to cybersecurity is distributed among national security agencies such as the National Intelligence Service and the Ministry of Defense, rendering it difficult for the National Assembly or civic groups to effectively control the budget. Accordingly, appropriate controls as aforementioned are required, and to fulfil the objectives, budgets should be prepared specifically for each item of expenditure, along with an integrated budget statement to facilitate control. Budget controls should not only be controlled through the National Assembly Intelligence Committee and the Special Committee on Budget and Accounts, but also through the Board of Audit and Inspection and other internal controls.

Fourth, National Assembly's budget deliberation ought to be reinforced. Currently cybersecurity is led by Cheong Wa Dae's National Security Office and the National Intelligence Service, whereby the budget is primarily utilized by these agencies. However, these agencies tend to be somewhat opaquely managed, as budget disclosures and detailed budget items are not clearly indicated under the pretext of national security. Resultantly, the budget is not utilized as intended and often ends up serving political purposes. In order to prevent this, the National Assembly's Intelligence Committee and the Special Committee on Budget and Accounts, a budget

control organization, should strictly enforce budget review on cybersecurity. Although the cybersecurity budget review may have to remain confidential due to national security reasons, the internal budget details should be clarified and reviewed in accordance to the principle of budget.

Fifth, the budget for fostering cybersecurity personnel should be increased. Training professional cybersecurity personnel and enhancing their practical ability is essential to fortify national cybersecurity. In the fourth industrial revolution, cyber attacks will be launched through various new means such as Artificial Intelligence (AI), and Internet of Things (IoT), rather than through traditional methods of attack. Therefore, forming effective response strategy requires an ability beyond a simple operation of a computer, but a high-level of sophisticated and comprehensive cybersecurity expertise. This logically demands a more systematic training of professional personnel, and continuous re-education of personnel in charge of the relevant government and private institutions, which calls for sufficient budgeting.

#### **4) Public-Private Partnership**

Unlike the traditional perspective on government, in the governance perspective, the boundary between public and private sectors is blurred with significantly increased interdependence. According to the governance perspective, the private sector is actively involved in the whole process of policy making and implementation, whereas under the traditional concept of government, the policy process was managed exclusively. Accordingly, maintaining cooperation, communication, and coordination between the public and private sectors is essential for the governance

system to function properly. However, the current national cybersecurity system is managed within the closed policy-making and implementation structure, in the absence of proper engagement of the private sector, under the pretext of maintaining confidentiality on key sensitive information. The following measures are required for the cybersecurity governance system to be stable and robust with regard to public-private partnership.

First, an integrative information management system is needed to connect public sector cybersecurity information with that of the private sector. Currently, although major cyber attacks are launched against government networking and defense computer networks for military purposes, private industries such as high-tech industries, energy sector, finance sector and water industry, can also be targets of cyber attacks. Even regarding national defense, cyber attacks can be launched against industrial facilities such as power facilities, water supply facilities, nuclear power plants and hospitals in order to instigate social confusion and chaos. Logically following, drawing strict boundary between the public and private sectors becomes gradually difficult, which demands maintenance of intimate cooperation between the two sectors. To better respond to this changing environment, key cybersecurity information on the basis of the integrative information management system needs to be managed. In this case, establishing the integrative management system under the jurisdiction of relevant government departments to maintain information security is deemed realistic. Only small numbers of private security staff should be permitted to deal with secret information under a specific and limited purpose.

Second, introducing the shift work system as a way of strengthening the business cooperation between public and private sectors is recommended. Since the personnel expertise is essential in cybersecurity, opening up the channels for consistent cooperation and information sharing among key staff in the public and private sectors is required. The introduction or availability of superior means of cyber defense may be of limited value if critical pieces of information cannot be shared between public and private sectors, and when staff in charge are not ready to cooperate with each other. Therefore, holding periodic meetings between the cybersecurity personnel in public and private sectors, introducing the shift work system between the two sectors, and conducting public-private mock training in preparation for cyber attacks should be pursued. If necessary, formulating a task force team to treat common affairs together could be incorporated.

Third, special attention is demanded for the industrial areas and major companies exposed to cyber attacks. Currently, industrial areas such as nuclear power, electricity, telecommunications, finance and healthcare, are prone to be a target of cyber attacks. If cyber attacks are launched on these industries, whether in peacetime or during war, great confusion and chaos will be fomented nationally. Thus, designating the industries with high potential for cyber attacks as the object of cybersecurity, and to obliging them by law to establish their own cybersecurity management systems, maintaining professional cybersecurity manpower, sharing relevant information with the government, and reporting immediately in the event of cyber attacks are required. These kind of obligation can also be applied to major companies that also hold potential to be targets of cyber attacks.

Fourth, private industrial security should be strengthened as part of the national cybersecurity. Currently, industrial espionage activities to steal key information are frequent in high-tech industries. Unlike the past, such espionage activities are carried out today through hacking the computer network system. Accordingly, the National Intelligence Service (NIS) and relevant agencies strives to adopt various efforts to protect the critical information of domestic industries from foreign competitors. Despite such efforts, industrial information leakage continues to be frequent due to the lack of the integrative management system between the public and private sectors. Therefore, managing critical industrial information in the private sector as part of national cybersecurity is necessary, as opposed to leaving such management solely to the private sector. To this end, a formal platform for a public-private information-sharing needs to be established on a regular basis.

### **5) Monitoring and Evaluation Systems**

First, a standing monitoring and inspection system to routinely inspect current status and problem of critical information infrastructure cybersecurity should be established, and a clause to support this system should be incorporated in the integrated cybersecurity law. There is a tendency for relevant government agencies to be uncoordinated during the breakout of a cyber attack, but dismisses the incident as time progresses from the outbreak of the incident. However, cybersecurity requires the following series of process including prevention, response, recovery, and feedback to function routinely and organically. Therefore, throughout this entire process, continuous monitoring of the cybersecurity system function is required.

For such monitoring function, the National Security Office of the President Office should undertake general supervision; however, to enhance the effectiveness of monitoring, routine monitoring should be undertaken by the Office of the Prime Minister, or the President's Board of Audit and Inspection, as these departments possess greater power than normal government departments. Furthermore, other relevant ministries, including the National Intelligence Service and the Ministry of Defence should conduct regular monitoring of their respective inspection agencies on prevention, preparedness, and recovery plans for cybersecurity. Accordingly, a compact monitoring network must be established for national cybersecurity monitoring, starting from relevant government agencies' self-inspection, then to monitoring by the Prime Minister's Office or the Board of Audit and Inspection, then to Cheong Wa Dae National Security Office general supervision. There must be no single loophole or any minuscule neglect for strengthening critical information infrastructure cybersecurity.

Second, coherent guidelines should be prepared on the process and scope of monitoring. Monitoring should not be fictitious, but should be carried out in accordance to clearly established procedures and methods. The monitoring methods for cybersecurity systems should be periodically inspected by the government departments in charge of cybersecurity, by requiring them to report the status of their work and national cybersecurity trends on a monthly and quarterly basis. However, since there exists a limit to monitoring through only document reporting alone, the team should visit the site biannually, divided into first half of the year and second half

of the year, to conduct an on-site monitoring of current cybersecurity status and problems.

Pertinent to scope of monitoring, the government should inspect the comprehensive aspects of cybersecurity, including prevention, response, and recovery, but should particularly strengthen inspections of preventive systems. In the case of an on-site inspections, rather than merely relying on monitoring reports from the related ministries, the government should more proactively inspect the organization's preparedness against cyber attacks by conducting simulated drills reflecting a real cyber attack situation. Furthermore, the government should also inspect the details of cybersecurity budget spending in order to prevent lax spending, or out of purpose spending. Even in such case however, the budget controls should not be undertaken from an excessively legal perspective, but from a goal-oriented effectiveness perspective. Simply put, the relevant budget should be inspected on the basis of how effectively the resources are being utilised to fulfil the objectives of cybersecurity. In addition, the expertise of cybersecurity personnel, the sufficiency of manpower scale, and the status of personnel management ought to be examined, as cybersecurity heavily depends on the quality of personnel in charge. Other than these, monitoring should inspect the detailed contents of the programs under operation in relevant cybersecurity ministries, seeking out any unnecessary or overlapping elements, in order to enhance the relevance of the program.

Third, national cybersecurity performance evaluation system ought to be established. The aforementioned monitoring is a type of process evaluation, whereas the performance evaluation is a type of summative evaluation. Performance

evaluation should be conducted annually or every three years in order to identify problems in national cybersecurity system, and to provide fundamental solutions for improvements based on the problem identification. In the case of Korea, performance evaluation functions are deemed weak in almost policy areas, and policies or programs are often unsystematically managed, resulting in budget waste. Such holds true for cybersecurity as well.

More specifically, securing the independence of performance evaluation institutions is crucial to establish an effective performance evaluation system. Therefore, the executive body should not be in charge of the evaluation function, as it would be difficult to establish objectivity and reliability of the performance evaluations. Rather, placing the performance evaluation functions under the National Assembly's Intelligence Committee may be considered. However, due to the characteristics of politicians, there is a possibility of information leakage, which must be kept confidential to the media and other foreign countries.

Accordingly, should the performance evaluation function be entrusted in the National Assembly, the government must obligate relevant personnel against disclosing confidential information, and impose strict penalties in the case of violation. Further, since performance evaluation requires a high degree of expertise in IT devices, military information, hacking, etc., securing expert personnel to be in charge of evaluation is crucial. In this case, using a Task Force in the form of permanent agency, which only assigns professional personnel when necessary, is recommendable.

In conducting performance evaluation, undertaking the evaluation every two to three years in general is deemed more practical. Not only will the cost of evaluation increase if conducted annually, but the relevant government ministries will also spend more for personnel to prepare for the performance evaluations. For the method of performance evaluation, both document and on-site assessment should be undertaken, as determining accurate performance level is difficult when only referring to the reported document. With regards to the evaluation criteria, evaluation items and evaluation criterion must be established to assess the current state of cybersecurity in advance. The assessment scope can be organized by cybersecurity processes such as prevention, response and recover, and can be categorized into personnel expertise, budget appropriateness, management systems, facilities and equipment levels. Subsequently, specific assessment criteria should be formulated for each of these areas, and marks should be distributed accordingly. In setting the assessment criteria, heavy reliance on only quantitative criteria should be avoided by also incorporating an appropriate balance of qualitative criteria. Assessment marks should be evenly distributed across each assessment area, and greater weight should be placed on factors which directly affect the achievement of cybersecurity objectives as opposed to superficial factors.

Fourth, the results of performance evaluation ought to be compared between the relevant government departments and agencies, and an incentive system based on performance evaluation results should be established. The purpose of the performance evaluation is to analyze the current situation to identify problems, provide suggestions for improvement, and clarify the reward and punishment system

based on the performance evaluation results by linking it to the motivation of the personnel in charge of the relevant organization. Thus, each department in charge of cybersecurity should produce data which can be compared to the results of performance evaluations, then should undertake comparison of performance evaluation results annually. Comparison of the level of cybersecurity situation according to the year and government departments will be possible when the items, criteria and marks for performance evaluation are stably maintained. Nonetheless, it should be noted that referring solely to quantifiable indications of performance evaluation could lead to inaccurate judgments, as there exist limitations to uniform comparison of performance evaluation, considering that different government departments' situations and their area of importance varies.

When informing each government department of the evaluation results, the monitoring body, in addition to the results, should also advise them to formulate their own measures for improvement by clearly indicating how improvements can be made. Additionally, including how much improvements have been made based on previous assessment results should be required as part of the feedback.

Subsequently, the results of the performance evaluation should be used for penalizing the relevant ministries and officials. Incentives should be granted for good evaluation performance results, whereas penalties should be given for the opposite case. In general, measures are required to incentivize the top 30%, and to penalize the bottom 30%. For incentives, solutions for a small increase in the relevant budget at the ministry level, a reward for the officials in charge, and additional points for the personnel management are required. For penalties, the relevant department should

indicate solutions for improvement in the following year, and should performance evaluation be continuously low, certain measures such as warning the relevant departments must be undertaken.

## **5.2 Engineering Cyber Resilient Governance**

In addition to establishing coherent and integrative national cybersecurity management system, legal basis, and budget system, efforts towards a cyber resilient governance should be emphasized. Just as complete security is unattainable in physical security, such holds true in the sphere of cybersecurity. From a cybersecurity perspective, the single greatest threat is by far unpatched existing vulnerabilities. Cyber vulnerabilities exist on every level, and protection against every cyber risk is not only impossible but also impractical. Traditional defenses against cyber threats, such as building firewalls are deemed insufficient in this digital era due to the ever-evolving nature of cyber attacks, rise of sophisticated and diverse threat actors, motivations and tactics. Hence, engineering cyber resilience in the cybersecurity governance is deemed of utmost importance.

The term cyber resilience is understood and defined in various ways. The U.S. governmental agency, National Research Council (NRC) defines it as “the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events”, whereas the Presidential Decision Directive 21: Critical Infrastructure Security and Resilience (PDD-21) describes it as the “ability to prepare for and adapt

to changing conditions and withstand and recover rapidly from disruptions”.<sup>79</sup> Although there exists a conceptual elusiveness over the exact definition of cyber resilience, generally, it refers to the overall ability of systems and organizations to withstand cyber events and, where harm is caused, rapidly recover from them, and the overall key words attached to the definition of cyber resilience include prepare, absorb, recover and adapt to adverse cyber event.

In comparing cyber resilience and cybersecurity, cyber resilience is to complement existing cybersecurity, as the former acknowledges that regardless of how strong the security may be, modern systems will always possess vulnerabilities which attackers will be able to exploit. Therefore, cyber resilience assumes that the adversary will breach the system. This assumption of the cyber resilience perspective allows for a more proactive and holistic approach to deal with adverse cyber events than cybersecurity perspective which takes a rather passive and defensive posture, and the key difference between cyber resiliency and cyber security is that the former continues to deliver its function despite the unexpected cyber breach. Accordingly, cyber resilience takes a step further to complement cybersecurity, by incorporating a proactive and holistic approach towards better detection through enhanced situational awareness, better reaction, and better recovery.

---

<sup>79</sup> Presidential Decision Directive- 21 (2013): *Critical Infrastructure Security and Resilience*, available, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive>

**Table 5-1** Comparison of Cybersecurity and Cyber Resilience

	Cybersecurity	Cyber Resilience
Objective	Protect Information Technology systems	Ensure business delivery
Intention	Fail-safe	Safe-to-fail
Approach	External security	Internal security
Scope	Single organization	Network of organizations

Attaining cyber resilience is particularly imperative for mission-essential systems which serve as the fundamental groundwork for the national security, essential government services and the critical information infrastructures upon which the nation's economy depend on. As such services and key assets associated with economic and national security consequences demand uninterrupted availability, ensuring high level of resiliency is an important means to achieving the aforementioned goal.

In order to engineer the element of cyber resiliency in national cybersecurity governance, resilience as a shared responsibility among all stakeholders must be acknowledged. For this purpose, the government along with the private sector ought to first reach a consensus on the definition of cyber resilience, and such common definition is to encompass both the public and private sectors. Then, the government in collaboration with the private sector ought to develop a standardized cyber resilience framework, or a common metrics to measure the level of cyber-resiliency of a critical information infrastructure, and identify which infrastructure is the most vulnerable to adverse cyber incidents. In more detail, the government could initially

establish government-operated no-cost, voluntary cyber resilience programs such as the Cyber Resilience Review (CRR)<sup>80</sup> in the U.S., although further details of the program will not be discussed in detail as it is deemed beyond the purview of this paper.

For both restructuring cybersecurity governance and establishing cyber resilience, the importance of information-sharing between the public and the private sector cannot be overemphasized. Accordingly, the government in addition to the aforementioned provision of legal basis, ought to establish incentive mechanisms for information-sharing to bolster cyber resilient governance. Such incentive scheme is particularly important to resolve the discrepancy between private sector's economic objectives and public sector's national security interests, in which case the government provision of financial incentives for mission-essential private sector could encourage the adoption of cyber resilient measures.

---

<sup>80</sup> The Cyber Resilience Review (CRR) is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices. The Department of Homeland Security (DHS) partnered with the Computer Emergency Response Team (CERT) Division of Carnegie Mellon University's Software Engineering Institute to create the CRR. The CRR is a derivative of the CERT Resilience Management Model (RMM) (<http://cert.org/resilience/rmm.html>) tailored to the needs of critical infrastructure owners and operators. <https://www.us-cert.gov/ccubedvp/assessments>.

# CHAPTER VI

## Conclusion

### 6.1 Conclusion and Implications

This paper has sought to suggest practical, comprehensive, and detailed policy alternatives to bolster national cybersecurity in Korea based on the analytical dimensions consisting of the following components: legal and institutional systems, administrative system, finance and budget systems, public-private partnerships, and monitoring and evaluation systems. In doing so, the paper has identified high-levels of fragmentation and instability in Korea's national cybersecurity governance system. Currently, there is an absence of an overarching integrative cybersecurity legal system in support of both the public and private sector, and separate cybersecurity laws exist in support of the different sectors. Not only is such legal-institutional basis inadequate in responding to increasingly complex cyber attacks, but this has inevitably led to fragmented national cybersecurity administrative system, scattered cybersecurity budget systems, weak public-private partnerships, and unsystematic monitoring and evaluation systems. Although there have been multiple attempts to enact an integrative cybersecurity law, the controversy over where to designate the control tower, and high-levels of mistrust pertinent to private-sector information-sharing has impeded the passage of such law.

On the other hand, the U.S. has attained greater success in establishing a more stable and coherent federal cybersecurity governance system. In establishing an

integrative federal cybersecurity law, which mandates information-sharing between the public and the private sector, the executive branch has utilized various Executive Orders and Presidential Decision Directives to consolidate the legislative basis. Such legal provision has facilitated public-private partnerships in cybersecurity, and effective information-sharing between the public and private entities. Furthermore, in terms of the administrative systems, although every Federal agency is responsible for its own cybersecurity, the Department of Homeland Security plays a leading role in producing operational direction, offering technical assistance and overseeing the other agencies implementation of federal cybersecurity practices. The federal cybersecurity budget falls under the Federal IT spending, and is managed by the Office of Management and Budget. Federal cybersecurity spending has gradually increased over the years in proportion to the Federal IT Spending. The monitoring and evaluation for federal cybersecurity is undertaken in the OMB in collaboration with the DHS, which assists in more detailed evaluation of federal cybersecurity status.

In order to bolster national cybersecurity, and consolidate a more coherent and stable cybersecurity governance system in Korea, as is the case with the U.S., this paper has suggested the following policy alternatives. In terms of the legal-institutional system, first, integrative legislation pertinent to national cybersecurity ought to be established, with the the director placed under the Prime Minister's Office, instead of the National Intelligence Service. Second, guidelines for performing tasks pertinent to national cybersecurity or response to cyber attacks should be created. Third, the system for protecting personal information and prevention human rights

violations should be reinforced. Fourth, measures should be developed to separately manage military and civilian information pertinent to national cybersecurity.

For the administrative system, tentatively named “National Cybersecurity Council” should be established as the cybersecurity governing body, to strengthen the control tower functions within the government. Second, since cyber attacks take place in a variety of sectors irrespective of department jurisdiction, and cybersecurity requires sophisticated technical expertise, the system of cooperation and coordination at the working-level manager should be reinforced. Third, national cybersecurity ought to be bolstered at the local government level. Fourth, cybersecurity monitoring system should be established. Fifth, proactive detection and prevention against cyber attacks should be bolstered. Sixth, cyber attack simulation training system should be strengthened. Seventh, emergency response system against cyber attacks ought to be established, and continuous education and training on cybersecurity ought to be pursued on a national level.

Pertinent to the finance and budget systems, the importance of national cybersecurity should be recognized, and appropriate levels of cybersecurity budget should be allocated. Second, the Integrated Budget and Consolidated Financial Statements should be prepared for managing cybersecurity related budgets in a coherent manner. Third, the control function of the cybersecurity budgets should be strengthened. Fourth, National Assembly’s budget deliberation ought to be reinforced, and the budget for fostering cybersecurity personnel should be increased.

With regards to the public-private partnerships, the need for an integrative information management system has been highlighted to link the public and private sector cybersecurity information. Second, introducing work shift system as a means to reinforce business cooperation between public and private sectors has been recommended. Third, special attention is demanded for industrial areas and major companies exposed to cyber attacks. Forth, private industrial security ought to be strengthened by incorporating it into national cybersecurity.

For policy suggestions on monitoring and evaluation systems, a standing monitoring and inspection system which routinely inspects current status and problem of critical information infrastructure cybersecurity should be established, and a clause to support this system should be incorporated in the integrated cybersecurity law. For such monitoring function, the National Security Office of the President Office should undertake general supervision. Second, coherent guidelines should be prepared on the process and scope of monitoring. Third, national cybersecurity performance evaluation system ought to be established. Fourth, the results of performance evaluation ought to be compared by relevant government departments, and an incentive system based on performance evaluation results should be established.

Finally, on top of these policy alternatives, efforts toward bolstering cyber resilience based on rapid detection, reaction, and recovery has been suggested, since protection against all cyber attacks is not only impractical but also impossible. In order to do so, reaching consensus on the definition of cyber resilience between the relevant sectors, and establishing standardized cyber resilience framework has been suggested as the first step towards this objective.

## **6.2 Future Avenues of Research**

This paper has provided policy alternatives on domestic cybersecurity governance systems. However, since cyber attacks are not bound by physical borders, future studies could also delve into how national cybersecurity governance can be coordinated with regional and international cooperation. Furthermore, considering the existing military alliance between South Korea and the U.S., ways to strengthen cybersecurity partnerships can also be explored.

Further, although the policy alternatives in this paper sought to provide comprehensive yet detailed steps and suggestions on how national cybersecurity governance system ought to be managed, in terms of the analytical dimensions provided in Chapter II, future studies could contribute a more in-depth policy suggestions focusing specifically on one of the following components: legal-institutional system, administrative system, finance and budgets systems, public-private partnerships, or monitoring and evaluation systems. In doing so, future studies could indicate the advantages and disadvantages of the proposed suggestions, for policy makers to take into account in national cybersecurity governance policymaking.

## Bibliography

- Act on Promotion of Information and Communication Networks Utilization and Information Protection, Etc. available  
[https://elaw.klri.re.kr/eng\\_service/lawView.do?hseq=38422&lang=ENG](https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG)
- Ahn, Byung Young, "The Changing Role of the State in the 21<sup>st</sup> Century and Governance," *Idea and Ideology (the Quaterly)*, journal 44 (2000): 13-15.
- Bae, Young Ja, *National Cybersecurity*, (2016): 97-129.
- Boys, James. "The Clinton administration's development and implementation of cybersecurity strategy (1993–2001)," *Intelligence and National Security* 33, no.5 (2013): 755-770, DOI: 10.1080/02684527.2018.1449369
- Cho, Hwha Soon and Kwon Oung, "Comparing Korea and U.S. Cybersecurity Governance: from the Perspective of Cyber Threat Securitization Theory," *Information Society & Media* Vol.18, No. 2 (2017): 97-120.
- Christou, George. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, (London: Palgrave Macmillan UK, (2017): 53-83.
- Clinger-Cohen Act, available:  
<https://business.defense.gov/Portals/57/Documents/Federal%20Acquisition%20Reform%20Act%20of%201996%20Clinger-Cohen%20Act.pdf>.
- Cyber Legislative Proposal: Blueprint for a secure cyber future, (DHS, Nov 2011),  
<https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf>.
- Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*, (Washington, DC: Department of Homeland Security, 2013).
- EFTA, Electronic Financial Transactions Act, available,  
[www.moleg.go.kr/english/korLawEng?pstSeq=47594](http://www.moleg.go.kr/english/korLawEng?pstSeq=47594)
- Executive Order-13636 (2013): *Improving Critical Infrastructure Cybersecurity*
- Flick, et, al. "What is qualitative research? An introduction to the field." *A companion to qualitative research* (2004): 3-11.

- Gary, Thomas. *How to do your case study*, (London: Sage Publications, 2015)
- Gilbert and Terrell. *Dimensions of Social Welfare Policy*, (New York: Pearson, 2013).
- Government, *National Cybersecurity Masterplan Establishment* (Korea Communications Commission report, 2011)
- Jessop. "Liberalism, Neo-Liberalism and Urban Governance: A State Theoretical Perspective," *Antipode* 34, no.3 (2002): 452-472.  
<https://doi.org/10.1111.1467-8330.00250>.
- Kidera, Momoko and Sato Ryotaro. "North Korean hackers' evolution on display in US case," *Nikkei*, September 11, 2018, accessed March 13, 2019,  
<https://asia.nikkei.com/Spotlight/N-Korea-at-crossroads/North-Korean-hackers-evolution-on-display-in-US-case>.
- Kim, Sang Bae (2017), "National Strategy of Cyber Security"
- Kim, Do Seung (2017), "A Study on Law and Organization for Strengthening Cybersecurity," *Study on the American Constitution* 28, no.2 (2017): 99-130.
- Kim, Sangbae. *National Cybersecurity Strategy*, (Seoul: Critical Perspectives on Society Academy, 2017)
- Kim, Sangbae. "Cyber Security and Middle Power Diplomacy: A Network Perspective." *The Korean Journal of International Studies* 12, no. 2 (2014): 323-352.
- KISA, Korea Internet and Security Agency, <https://www.kisa.or.kr/eng/main.jsp>
- Kissel, Richard. "Glossary of Key Information Security Terms," National Institute of Standard and Technology, 2013 DoC. USA.  
<http://nvlpubs.nist.gov/nistpubs/ir2013/NIST.IR.7298R2.pdf>
- Klijn, Erik-Hans. "New public management and governance: a comparison." *Oxford handbook of governance* (2012): 201-214.
- Kooiman. *Governing as Governance*, (Sage Publications, 2003):114.
- Krippendorff, Klaus. *Content analysis: An introduction to its methodology*, (Sage publications, 2018).
- Kuehn A. *Extending Cybersecurity, Securing Private Internet Infrastructure: the US Einstein Program and its Implications for Internet Governance*, In:

Radu R., Chenou JM., Weber R. (eds) *The Evolution of Global Internet Governance*. (Springer Publications, 2018).

Kwangho Kim, Sangdon Park, and Jongin Lim. "Changes of cybersecurity legal system in East Asia: focusing on comparison between Korea and Japan." In *International Workshop on Information Security Applications* (Springer, 2015): 348-356.

Lee Myung-seok, "Conceptualizing Governance: Governance as a Social Coordination." *Korean Public Administration Review*, journal 36, no.4 (2002): 331-333.

Martin, Timothy. "North Korea While Professing Peace Escalated Cyber attacks on South," *Wall Street Journal*, May 25 2018, accessed February 10 2019, <https://www.wsj.com/articles/north-korea-while-professing-peace-escalated-cyberattacks-on-south-1527239057>.

Min Sik Kim et. al, "Research on the Need for an Integrative Cyber Crisis Management System: Comparing U.S. and Korea's Institution and Policies," *Journal of Information Security* 9, no.1 (2009).

Morgan, Steve. "Worldwide cybersecurity spending increasing to \$170 billion by 2020," *Forbes* March 3 2016, accessed February 12, 2019, [https://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/#5f8913876832\(2016\)](https://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/#5f8913876832(2016)).

Nanda, Ved P. "The "good governance" concept revisited." *The ANNALS of the American academy of political and social science* 603, no. 1 (2006): 269-283.

National Cyber Strategy of the United States of America 2018, available, <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

National Cybersecurity Protection Advancement Act of 2015, available, <https://www.congress.gov/bill/114th-congress/house-bill/1731>

National Presidential Security Directive 54: January 2008 Comprehensive National Cybersecurity Initiative (CNCI)

NIST, <https://www.nist.gov/cyberframework>

Nix, et al. "The law of cyber-attack," *California Law Review* 100, (2012): 817.

Nuclear Safety Act (Korea), available, [www.nssc.go.kr/nssc/en/nci/elif/Nuclear\\_Safety\\_Act.pdf](http://www.nssc.go.kr/nssc/en/nci/elif/Nuclear_Safety_Act.pdf).

- Office of Management and Budget Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2016.  
[https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy\\_2016\\_fisma\\_report%20to\\_congress\\_official\\_release\\_march\\_10\\_2017.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf).
- Office of Management and Budget, IT Dashboard <https://itdashboard.gov/> accessed 2019.
- Overview of cybersecurity, ITU-T X.120, available,  
[https://www.itu.int/rec/dologin\\_pub.asp?lang=s&id=T-REC-X.1205-200804](https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804)
- Park, Sang Don and Kim, Injung. "A Study on Tasks for the Legal Improvement for the Governance System in Cybersecurity," (2013)
- Pena, Jorge, J. Luis Guasch, and Alvaro Escribano. "*Reforming public institutions and strengthening governance: a World Bank strategy*," (The World Bank, 2000): 78.
- Presidential Decision Directive- 21 (2013): *Critical Infrastructure Security and Resilience*, available, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience>.
- Quadrat-I Elahi, Khandakar. "UNDP on good governance," *International Journal of Social Economics* 36, no. 12 (2009): 1167-1180.
- Randvanosky and McDougall. *Critical infrastructure: Homeland security and emergency preparedness, 4<sup>th</sup> ed*, (Florida: CRC Press, 2016).
- Rhodes. "Understanding governance: policy networks, governance, reflexivity and accountability," *Public Policy and Management*, Philadelphia, US. Open University, (1996): 252-254.
- Rohozinski, Farwell, James, and Rafal. "Stuxnet and the Future of Cyber War." *Survival* 53, no. 1 (2011): 23-40.
- Rosenzweig, Paul. "The Cybersecurity Act of 2015." *Lawfare*, (2015). <https://www.Lawfareblog.com/cybersecurity-act-2015>.
- Schatz, et, al. "Towards a More Representative Definition of Cyber Security," *Journal of Digital Forensics, Security and Law* 12, No. 2, Article 8 (2017).
- Schmitt, Michael. *Tallinn manual on the international law applicable to cyber warfare*. (Cambridge University Press, 2013), 45.

- Steve, Morgan. "Worldwide cybersecurity spending increasing to \$170 billion by 2020," *Forbes* March 3 2016, accessed February 12, 2019,
- Stevenson, Angus, and Maurice Waite, eds. *Concise Oxford English Dictionary: Book & CD-ROM Set* (Oxford University Press, 2011).
- Stoker, Gerry. "Governance as theory: five propositions." *International social science journal* 50, no. 155 (1998): 17-28.
- USA Patriot Act of 2001, 1016(e) (42 U.S.C. 5195c(e)).
- Valeriano, Brandon, and Ryan Maness. *Cyber war versus cyber realities: Cyber conflict in the international system* (Oxford University Press, 2015).
- Valeriano, Craig, Anthony, and Brandon. "Conceptualising Cyber Arms Races," *International Conference on Cyber Conflict* 8, (2016):141-158.
- Volz, Dustin. "Trump, Seeking to Relax Rules on U.S. Cyber attacks, Reverses Obama Directive," *Wall Street Journal*, August 15 2018, accessed April 12, 2019, <https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721>
- Weiss, Thomas. "Governance, good governance and global governance: conceptual and actual challenges." *Third world quarterly* 21, no. 5 (2000): 795-814.
- William J. Clinton, National Plan for Information Systems Protection Version 1.0: an invitation to a dialogue (Washington DC: The White House, 2000); George W. Bush, The National Strategy to Secure Cyberspace (Washington DC: The White House, 2003).
- Won, Byung Chul. "The Reality of Cybersecurity in Korea by Four Cybersecurity Experts," *Boan News*, November 12 2018, accessed February 10, 2019, <https://www.boannews.com/media/view.asp?idx=74530>.
- Yin and Robert K. *Case study research and applications: Design and methods*, (Sage publications, 2017).

## 국문초록

우리나라의 국가 사이버안보는 관리체계가 다양한 정부부처들 간에 분산되어 있음은 물론, 공공, 민간, 군사 부문들 간에도 조정과 연계체계 매우 부실하다. 따라서 고도로 지능화되고 복잡해 지고 있는 각종 사이버 공격에 제대로 대처하는 데 한계를 노출하고 있다. 그리고 사이버안보체계의 안정성 면에서도 문제가 적지 않다. 따라서 국가 사이버안보체계 전반에 대한 점검과 재구조화가 필요한 시점이다.

이러한 배경 하에서, 본 논문의 목적은 거버넌스(governance) 관점에 입각하여 핵심정보인프라 분야에서의 국가 사이버안보체계의 실태와 문제점을 분석하고 또한 미국의 사이버안보체계에 대한 사례분석을 행하며, 이를 토대로 핵심정보인프라 분야에서의 사이버안보체계 강화방안을 제언하고자 하는 것이다.

이러한 연구목적을 달성하기 위하여 본 논문은 우선 사회과학 분야에서 널리 사용되고 있는 거버넌스 관점의 등장배경, 의의, 거버넌스 능력 등에 관한 이론적 논의를 행하였다. 다음에는 이러한 이론적 논의를 참조하여 거버넌스의 구성요소, 거버넌스의 성공 요건 등을 중심으로 분석틀을 설정하였다. 이어서 일종의 벤치마킹을 위한 시도로 미국의 사이버안보체계의 실태를 거버넌스 관점에 입각하여 사례분석을 행하였다. 다음 장에서는 앞에서 설정된 분석틀에 입각하여 우리나라 사이버안보 거버넌스 체계의 실태와 문제점을 실증적으로 분석하였다. 마지막으로 미국의 사이버안보 거버넌스 체계에 대한 사례 분석과 우리나라의 사이버안보체계의 실태 및 문제점에 대한 분석을 토대로, 보다 안정적이고 지속가능한 사이버안보 거버넌스 체계를 구축하기 위한 구체적인 정책방안들을 제시하였다.

**주제어:** 사이버안보, 거버넌스, 핵심정보인프라, 사이버 공격