UNIVERSITY OF TARTU

Faculty of Social Sciences

Johan Skytte Institute of Political Studies

Erika Kumekawa

Cyber resilience of e-government:
Comparative case analysis of Estonia and South Korea

MA Thesis

Supervisor: Mihkel Solvak, PhD

Tartu 2021

Non-exclusive license to reproduce thesis and make thesis public

I, Erika Kumekawa 49301030090

1. herewith grant the University of Tartu a free permit (non-exclusive license) to

reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

my thesis
Cyber resilience of e-government: Comparative case analysis of Estonia and South Korea, supervised by Mihkel Solvak, PhD

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons license CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive license does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Erika Kumekawa

16/05/2021

Abstract

E-government has evolved throughout modern times and shaped the new norm of governance. While global society pays more attention to this next-generation platform than before, it is also true that state actors should build up a robust security strategy to protect e-government and their extended territory in cyberspace. At the same time, a high level of digitalization does not always mean their e-government framework is also strong enough to endure external threats. This thesis examines the difference in security preparedness of e-government by comparing a set of countries that have similarly well-developed online government but are lagging in the cyber defense aspect. In order to examine this, the research used cyber resilience as a conceptual framework to analyze several factors that cause differences. This concept overcomes the blind spot of the traditional cyber security approach and points out the relation with conventional hard security study. To uncover the differences in cyber security of e-government, this study picks up Estonia as a successful model and South Korea as the opposite. Based on cyber resilience, the thesis identifies external and internal factors including regional security, nature of neighbors, and internal factors triggering variance within these countries.

Keywords: e-government, cyber security, cyber resilience, cyber warfare

Contents

List of Chart

List of Tables

List of Graph

List of Scatter diagram

Abbreviations

Chief Information Security Officer (CISO)

Computer Emergency Response Team(CERT)

Computer Security Incident Response Team (CSIRT)

Denial of service (DoS)

Digital Adoption Index (DAI)

Distributed denial of service (DDoS)

Domain name servers (DNS)

E-government Development Index (EGDI)

Electronic government (E-government)

Human Capital Index (HCI)

Information and Communication Technology (ICT)

National Cyber Security Index (NSCI)

Online Service Index (OSI)Organization for Economic Co-operation and Development (OECD)

Shanghai Cooperation Organization (SCO)

Telecommunications Infrastructure Index (TII)

United Nations (UN)

United Nations Department of Economic and Social Affairs (UNDESA)

1. Defining e-government

This chapter presents the thesis's overall topic of how we can see the global security in the cyber realm based on the e-government framework. The key principles and the research question will lead the research findings in the next six chapters. This chapter concludes with an explanation of the general framework of the thesis.

1.1 What is e-government?

The definition of E-government (electronic government) is straightforward. According to United Nations, e-government is a tool that exchanges information between citizens, businesses, and the government. (United Nation, 2021 a) In other words, it is an online government platform that enables to governing bodies to manage social activities such as administration, business transactions, and elections without physical action. By utilizing technology, the government transfers its major functions from physical to cyberspace and increases transparency and efficiency in public service.

Transitioning from a one-way to a multi-way system in e-government radically improved its convenience and effectiveness. United Nations also explains the mainstream development of e-government in two phases. The early-stage started with the use of Information and Communication Technology (ICT) to improve the whole process of providing governmental service. However, states expanded their e-government framework to a wide range of interactions with citizens and businesses, and would continue to do so into the later stage of development. (United Nation, 2021 a) A remarkable point in the history of this development was when e-government transformed its delivery methods from one-way into multi-way systems. In the early stage, e-government simply worked as a one-direction tool to provide public service from the government to citizens. In the later stage, citizens and businesses also started to utilize this system as a multi-way interactive tool. As a result, individuals, entrepreneurs, and the government fully utilize e-government as an interactive platform and maximize its benefit. Therefore, the evolution of e-government caused a revolution in the social life cycle.

As a role model, Estonia is especially advanced in digital governance. The has country successfully improved the convenience of public service, increased transparency, and reduced workload by preparing a common platform that all government, companies, and citizens can directly participate in. According to Estonian officials, citizens are able to use 99% of public services online 24hours a day, 7days a week. (e-Estonia, n.d) This system highly contributed to improving convenience because citizens do not have to interrupt their social activity in order to action administrative works. Additionally, according to Estonian officials citizens are legally obligated to hold personal ID cards, through which all individuals, companies, and governments can track business transactions. Consequently, this system made the taxation process much easier than before. (e-Estonia, n.d) In terms of transparency, we can say this Estonian model builds trust as multiple actors can confirm the same transaction. A digital framework such as this is the basis for Estonia succeeding in saving 844 years of working time and costs regarding the administration process and maximizing economic profit. (e-Estonia, n.d) In this case, Estonia accomplished building up a high level of e-government system by several aspects such as convenience, transparency, and workload. These improvements directly connect to the advanced governance in the next generation.

1.2 Problematic area

Although online platforms can provide major benefits as mentioned in the previous section, it is also true that these opportunities come with problems that are inherent for the way e-government works, that is data exchange and dependence on the data. To be precise, more channels of communication and multichannel delivery of services automatically lead to a higher dependence on cybersecurity for the protection of information and data. As a most prominent threat caused by this dependence, scholars cautioned the danger of cyber attack. Zhao and Zhao said the popularity of e-government is growing in today’s world, but it can also be a potential cyberattack target. (Zhao and Zhao, 2010) In other words, e-government not only improves public service but also opens up a new vulnerability based on dependence on data.

The vulnerability outlined above has a severe impact on national security. By transferring the government’s function to cyberspace conventional sovereignty has also moved there. Hassan and Khalifa's research is helpful to understand the potential threat and security risk that the internet brings to e-government. According to their study, "threat" is unauthorized access, malicious damage, and data intercepts. On the other hand, security risk means a virus, a cyberattack, and key information leakage. (Hassan and Khalifa, 2016) These growing security threats and risks destabilize society through the digital framework. Since e-government is the core of the national structure, addressing these vulnerabilities means improving national defense directly.

1.3 Research problem

From the preliminary findings of the previous section, we can say the e-government simply opens up a new attack vector and raises the question of how to safeguard national sovereignty in the digital realm. However, in some countries we can observe a high level of digital government and an apparently low level of cyber defense. Hence, the research problem of this study is we can see differences in response to cyber threats for advanced electronic government countries.

1.4 Research questions

To form a research question from a research problem, it is necessary to outline the difference in the maturity of cyber defense strategy related to e-government. According to the UN's survey, 145 Member States have a chief information officer or similar position to modify organizational structure to support digital government transformation. However, the maturity of e-government in each state is different due to lack of digital condition, insufficient capacities, and capabilities. Also, we can observe the difference in cyber defense in some countries that face security concerns. (United Nations, 2020) This survey demonstrates that countries are actively promoting digitalization but the maturity of each e-government is different. In this case, maturity means the outcome of digitalization. Consequently, digitally advanced countries do not always mature in cyber defense. Furthermore, we also see that a set of countries with advanced digitalization are paradoxically quite different in their build-up cyber security levels. Considering the current global situation that surrounds the e-government of each state, the research question of this study is what explains the differences in cyber response for advanced e-government states?

1.5 Structure of the thesis

This study is composed of seven chapters. This first chapter has already explained the research problem and question. The second chapter will mainly review three areas of existing studies;1. a broad range of cyber security studies, 2. digital sovereignty study, and 3. e-government study. The third chapter will indicate what is missing from the current cyber security study, then we will explore hard security studies and apply findings to the cyber realm to define “cyber resilience” as the conceptual framework. The fourth chapter will explain the methodology of this research and case selection. The fifth chapter will analyze the study cases with the conceptual framework created in the third chapter in order to derive answers to the research question. The sixth chapter will address findings from the previous chapter and look at them more in-depth. The final chapter will attempt to answer the research question and conclude this research.

2. Concepts and theory of security in cyber space

As we have already defined in the previous chapter, the overall topic of this research is the security aspect of e-government. To set up the theoretical framework, this chapter consists of three parts.

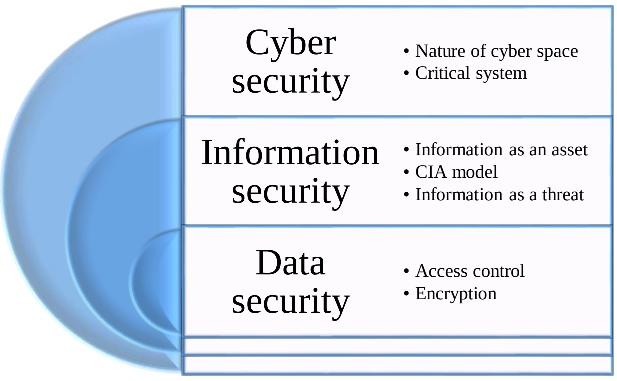


Chart 1: Security concepts in cyber space[1]

First, sections 2.1 to 2.3 outline security concepts in cyber study. It starts from the general understanding of cyberspace as the basic, then gradually shifts narrower scope to focus on specific security terms.

Second, section 2.4 outlines how the nation re-creates sovereignty in digitalized space. In this step, disciplines in the conventional physical security study can be expanded into cyberspace. In other words, although cyberspace has its peculiarities, we can still observe the same level of external threats that exist in the physical space. These threats possibly affect national sovereignty in the digital realm. Third, section 2.5 reviews the current study of e-government and its measurement.

[1] This chart is created by the author of this thesis

2.1 Cyber security

This section will explore the broad concept of cyber security. First, we will take a look at the nature of cyberspace. Cyberspace is the artificial electronic realm that is the relatively new base of social activities. In order to address how we can fully utilize cyberspace for the new generation of global governance, it is essential to make sure of the peculiarity of the digital field. Then, we will move on to the critical system that consists of the core part of cyber society. The concept of a critical system that exists in cyberspace is one of the vital elements when we focus on cyber defense strategies.

2.1.1 Nature of cyber space

The literature of cyberspace starts with the new norm of territory. As this study has already mentioned in the beginning, the definition of the state includes its territory. Traditionally, social scientists define territory as four components; land, sea, air, and space. Mutually connected networks and infrastructure using ICT create the artificial realm, namely cyberspace, which is the new territory of countries. Although it is not physical, cyber space emerged to become a fully-fledged element of the national territory with highly developed online infrastructure. Besides, the importance of cyber space has been increased after the 2000s in terms of national defense. Based on cyberspace, all kinds of political, financial, and social transactions or activities produce various profits for society. Thus, cyberspace is the new territory that each state has the right to protect.

On the other hand, cyberspace also can be the stage where someone who has animosity attempt obstructionism. (United Nation, 2011) In addition, Shea also stated that cyber space shows the most drastic manifestation of vulnerability that exposed to any kind of threat. The reason is it links the whole world in real-time, and it allows any actor to attempt intrusion from wherever they are. (Shea, 2016) This means cyber space undoubtedly contains vulnerability that can be critically damaged by attacks. While the danger against information systems, networks, and their compositing elements is diverse, protecting cyber space from threats is one of the most urgent agenda in international security study.

To confront external threats in the cyber space, scholars started using the concept of “cyber security”. International Telecommunication Union defined cybersecurity as “to protect cyberspace from threat”. In other words, cybersecurity is about how to protect information systems, networks, and composite elements such as computers that generate cyberspace, from various kinds of attack. (International Telecommunication Union, 2005) This definition demonstrates that cyber security is the comprehensive understanding of defense in cyberspace since this concept includes protecting everything related to ICT from devices to policies. To see why cyber security is the key component to building up and maintaining safety in digitalized space, it is helpful to review the role of “critical system”.

2.1.2 Critical system

Critical system is the essential concept in the cyber security study. United Nations defined "Critical system" as infrastructures that provide a critical function for society and economy such as telecommunication, financial transaction system, and power supply. (United Nations, 2011) Consequently, we can say the critical system is one of the most essential components for populations to maintain the minimum standards of wholesome and cultured living. United Nations also stated that technologically advanced states started installing ICT for national critical systems in the 1990s. Around that time, political authorities of each county began to add the protection the critical systems from cyber attacks by either external states or terrorist groups to the national defense agenda. In this sense, cyber attack means intentional actions to change, interrupt or destroy a computer system and its network. (Ibid) To sum up, governments should strictly focus on national defense in cyber space because critical systems have already been gradually transferred there. Since these systems are the core part of modernized society, it is severe problem if they are exposed to threats and attacked by external hackers.

2.2 Information security

Information security is the protection related to information. In this section, we will take a look at two types of comprehension regarding information security. One is information security as an asset, and the other is as threats. The criteria are 1) How state actors perceive information and 2) What they need to protect from who.

2.2.1 Information as an asset

Information security is a vital concept in cyber defense study. To define the concept, we need to understand the definition of information first. According to Solms and Niekerk, “Information” takes various forms. (Solms and Niekerk, 2013) For example, both paper-based name list on the desk and electronic contracts stored in cloud storage are taken in different forms but the equally same "information". Additionally, we can also conceptualize “information” as valuable assets (Ibid) as information can provide a certain benefit to users. For example, customers’ preference at the restaurant helps marketing in the food industry. On the other hand, it is also true that external actors attempt to invade the system to steal valuable information. In this sense, information is surely an asset and needs to be secured.

Public sectors have been struggling with the transformation of stored data from paper-based to digitalized form. Traditionally governments stored documents containing personal data in physical space, therefore making it harder for someone to destroy or steal a huge amount of physical data.

On the other hand, we can observe different situations for information stored in the digital space. Cyber threats take advantage of the reversibility of the internet that opens up the new vulnerability in terms of information security. For example, the United States experienced a massive scale of data breaches in 2015. Wagstaff, Eng, and DeLuca explained that unknown users hacked the database of the Office of Personnel Management (OPM) via computer network and personal information including social security numbers, information on family members, health and criminal records were among the stolen data. This is incident is officially estimated to have affected 21.5 million people in the United States. Furthermore, since the stolen information includes fingerprints records of 1.1 million people, it could be utilized for the other criminal activities. (Wagstaff, Eng, and DeLuca, 2015) This case clearly demonstrates any kind of data center can easily become a target for hackers. This example concerned a centralized model database but can happen to distributed type as well. What we need to remark from this example case is that utilizing the advantage of digital governance also opens up new vectors, such as showing where attackers should hack.

2.2.2 CIA triad

To secure valuable information as assets, it is necessary to set up three criteria; confidentiality, integrity, and availability. According to Solms and Niekerk, confidentiality means the information is not seen by someone who does not have authority. Integrity indicates that information should not be changed, deleted, or added without permission. Availability meaning that users can see and use information anytime they need it. (Solms and Niekerk, 2013) Scholars take the first letters of these three criteria and call it as “CIA triad”. Thus, the general term “information security” is about protecting information from external actors and preserving it under the CIA triad.

Cyber security and information security are closely connected concepts. While cyber security is about maintaining cyberspace safely and protecting any existing components such as network, data storage, and stored information from threats, information security is centered in the safeguarding of the wide variety of information. In this sense, we can see some compatibility between these two concepts. For instance, CIA triad in information security is also applicable when it comes to securing information in cyberspace. System administrators apply CIA triad to make sure a high standard of security when they build cyber space using information systems and networks. However, this model is also quite useful to countermeasure attacks that damage information through cyber space.

2.2.3 Information as a threat

Information security has another interpretation that is entirely different from the definition in the previous section. Information as an asset has a specific value and is what should be protected from external threats. On the other hand, Kello pointed out the later interpretation shows information as a threat. In this case, information is harmful when it threatens the domestic regime. The most obvious example is internet censorship where the government limits nationals’ use of access to the world wide web because the information in the transnational digital space might contain potential harm to threaten the nation. In this sense, potential harm might impact the social-political system such as terrorism against the government. (Kello, 2013)

To determine which states perceive the information as a threat that produces a negative influence on the domestic regime, it is helpful to look at Shanghai Cooperation Organization (SCO). SCO is the multilateral regional organization that promotes cooperation in various fields such as exchanging culture, security, and regional stability. Member states are China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, India, and Pakistan. (Shanghai Cooperation Organization, n.d) Hitchens and Nilsu Goren explained "Cooperation in the Field of Ensuring International Information Security" that member states of SCO signed in 2009. This agreement emphasized that states enforce sovereign power to control information flow to prevent external harm. In detail, the member states view that spreading harmful information for the social-political system, psychological, moral, and cultural environment is a threat. (Hitchens and Nilsu Goren, 2017) In this sense, it is important to note that SCO recognizes information that exists in transnational cyberspace as potential threats no matter if it is surely harmful to the state or not. These member states share a common understanding regarding information security and cooperate how to protect their domestic regimes from external information.

To sum up, information security is about protection but has two types of interpretations. One is to protect information as an asset. In this definition, the information should be protected from external threats or attacks. The other interpretation as information as a threat that provides negative influence for the domestic regime, as the information might destabilize the it, the government limits access, and nationals cannot reach external information.

2.3 Data security

This section will take a look through the definition of data security and its use. This concept is a narrower definition of information security but has some parts in common. First, we will figure out the basic understanding of the concept, then we will move on to how these two concepts are related. Lastly, access control and cryptography, a technical take on the requirement for data protection will be detailed.

2.3.1 Definition of data security

Data security is simply about protecting data that is stored in hard devices or digital space. According to Iyobor, Kwadwo, and Asante, the aim of data security is to protect data and to ensure its privacy. (Iyobor, Kwadwo, and Asante, 2012) While in information security studies it does not matter what form information takes, data security solely focuses on digitalized data, giving data security a much narrower definition than information security.

2.3.2 CIA triad in data security

CIA triad is an overlapping core element in data security and information security studies. As we have already mentioned in section 2.2.2, the CIA triad is a useful assessment to secure information. To protect data in digital space, CIA triad is the essential criteria to ensure the strength of the security system. Warkentina and Orgeron conducted empirical research regarding the security aspect of blockchain technology. Blockchain is well known for using distributed ledgers and decentralized networks instead of a single central database. We can say this structure is one of the advantages in terms of security to avoid the risk related to a single point of vulnerability. In this research, they used CIA triad to measure the validity of the security. When they analyze blockchain with this model, we can see integrity in the relation between data and participants. In this sense, participants mean related users in each field such as supply chain, financial transaction, and business process. These users are given the authorization to access the data and all of them equally hold identical copies of them. In this case, this structure has a high level of integrity because all stakeholders verify the same data. (Warkentina and Orgeron, 2020) From their study, we can say researchers can also apply CIA triad derived from from the information security study to the data security field.

2.3.3 Technical method to protect data

Data security has several technical methods to protect data such as authentication, backup and recovery, data masking, and tokenization (Looker, n.d), but access control and encryption play the most vital roles in data protection on e-government platforms. Sandhu and Samarati explained access control as regulating general users that can access data or device, while also controlling any alteration or deletions of data in the program. Most access control systems are based on the concept of "ownership", which means data or devices should belong to the authorized owners and they give access to only legitimized users. (Sandhu and Samarati, 1994) This concept indicates the limited number of users who have the authority that allows additions, changes or deletions on the system. In the e-government platform, access control generally regulates that only the owner of the data, system administrator, and users who are given authentication are allowed to access the arbitrary information. In this sense, access control is one of the key components to secure the data of the electronic government.

The other method of data protection in e-government is cryptography. In a nutshell, this technology protects data though converting the original into a different form. As a result, keeping the information in a secret form strengthens the overall security of the system.

Stinson and Paterson study gives an overview of subject where cryptography has a additionally more detailed process; encryption and decryption. Encryption is the process that converts the original to the encrypted data. Decryption is the opposite term which means reverting encrypted data using shared keys. The encrypting process is called an encryption algorithm that has several types. Safety and proceeding time differ depending on which type of encryption users choose. Also, users and receivers need keys that correspond to the encryption algorithm when they attempt at either converting or reverting data. (Stinson and Paterson, 2018) Based on the CIA triad, we can say cryptographic technology achieved a high level of confidentiality, integrity, and availability in encrypting and decrypting process. In detail, converting the original data to an unseen form keeps a high standard of confidentiality. In addition, this technology guarantees that no one breaches integrity since only users who have keys can open the encrypted data. Besides, the availability of encrypted data is assured as long as users and receivers are given valid keys to open them. To sum up, cryptography is a technology verified based on the CIA triad to ensure the security of data in e-government.

2.4 National sovereignty in digital era

This section focuses on how the nation recreates sovereignty in cyberspace through e-government. Although e-government shapes a new norm of national sovereignty, we can still apply some disciplines found in existing physical security study. In traditional security norms, we can see the vector that states the need for protection because they are always exposed to threats or can be attacked by external actors. In other words, security study secretly implies the existence of enemies. These basics are applicable in cyberspace as well. At the same time, we can see the same level of security threats in cyberspace as in the physical world. However, peculiarities of cybersecurity are technical protection such as access control and encryption like that are mentioned in the previous section.

As for the structure of this section, the next part briefly outlines the traditional norm of sovereignty in security study. It is important to note why sovereignty is one of the core concepts when we consider national defense. Then the later part demonstrates how we can stretch existing knowledge and apply it to the digital era.

2.4.1 National sovereignty in digital era

Sovereignty is one of the most important concepts when we look at global politics and also the starting point of international relations study. Scholars perceive sovereignty in three aspects. One is the domestic absolute power that is the right of decision-making as a whole. This power decides national preference and internal politics. (Hinsley, 1986) Another is governance power with constitutional independence. (James, 1986) This aspect is about governing nationals and territory as an independent country. As a practical tool, constitution shapes governing framework with legitimacy. The other is external independence as a nation. This element of sovereignty does not allow occupation or intervention by other external countries. (Biersteker, 2012) Based on this norm, all sovereign states should respect each other’s independence and strictly go along with the principle of non-intervention. With these three aspects, sovereign states effectively control the power over their own territory.

2.4.2 Digital sovereignty

When we apply traditional norms of the sovereign state to the digital world, we can see the exact same components and their related structure regarding the definition of state in cyberspace. Based on three essential elements being population, government, and territory which consist of state, we can observe them in cyberspace as below; 1) digital identification can reproduce its nationals in the cyber realm, 2) the government shifts its functions to cloud space, and 3) not only physical extent is the country's territory. Thus, the cyber study still sticks with the existed physical security norms but can expand them to digital space.

Estonian data embassy project nicely embodies how we can apply the security study regarding sovereignty to digitalized space. In the security study, threatening national sovereignty by an external power is a critical issue in terms of national defense. According to Kotka et al, Estonia stores information that they need to maintain themselves as a sovereign state in Brussels under bilateral agreement. In this case, information includes sovereignty, data protection, custodianship. (Kotka et al, 2016) This example demonstrates states can reproduce by transferring data from cyber realm into a specifically protected physical data center. Thus, it helps countries to protect themselves in case of external actor militarily attack. In that sense, it can also work as a deterrent power. As long as the state exercises its sovereign power in the digital space, it does not make sense for that the external force to attack that state and physically occupy it. Since it is obvious that physical invading is not worth it as the data embassy project work as deterrence against external actors.

2.5 E-government and cyber defense

The previous section illustrated a comprehensive understanding of cybersecurity study including the concepts of information and data security. Since this thesis addresses the security aspects of e-government, this section focuses on the analytical tools to measure digital governance.

Security for cyber defense is an essential function of e-government. As the section 2.1 has already mentioned, cyberspace is the new artificial territory of the state. In that sense, the state also needs to protect its territory even if it is not in a physical place.

Therefore, e-government should play a role as “goal keeper” of national defense in digital space. For nationals, functions of e-government that pursue efficiency such as paperless operation are more visible and look appealing, but these functions are based on a robust and secured national system.

2.5.1 E-government survey

To see the overview of global trend surrounding e-government, it is helpful to use United Nation’s research. For scholars in the digital governance study field, the "e-government survey" conducted United Nations Department of Economic and Social Affairs (UNDESA) is one of the most trustworthy data sources as it provides plenty of information about e-government, collected from 193 member states. This survey is important for the UN because promoting digitalization in the political field facilitates the delivery of fair and equal public service for all nationals in each country. For example, the digitalization of public service in elections, education, medical service, and other related fields contribute to reducing physical and social distance. (United Nations, 2021 b) Therefore, promoting e-government projects is one of the actions for worldwide sustainable development.

In their research, United Nation uses unique indicators that rate the performance of national governments, namely the E-government Development Index (EGDI) to define technologically advanced states. This indicator shows the access characteristic includes infrastructure and educational levels. At the same time, it demonstrates how each state utilizes ICT to provide access to the government for nationals. (Ibid) According to the latest survey with analysis of EGDI, fourteen countries include *“Denmark, the Republic of Korea, Estonia, Finland, Australia, Sweden, the United Kingdom of Great Britain and Northern Ireland, New Zealand, the United States of America, the Netherlands, Singapore, Iceland, Norway, and Japan”* (United Nation, 2020, p. xxv) marks top performance of e-government.

This data shows that 9 out of 14 countries most digitally advanced government in the world are located in Europe, considering this we can say Europe is the leading region of e-government since it hosts majority of successful e-governments. EDGI also gives us various perspectives of social phenomena such as the level of national literacy, maturity of digital infrastructure and regional tendency in terms of digitalization. Therefore, EDGI can be used for analysis in many sectors.

Table 1: Top 14 countries in e-government development

(Source from: e-government survey 2020, p.12)

Country	EGDI (2020)	EGDI (2018)	OSI	HCI	TII
Denmark	0.9758	0.9150	0.9706	0.9588	0.9979
South Korea	0.9560	0.9010	1.0000	0.8997	0.9684
Estonia	0.9473	0.8486	0.9941	0.9266	0.9212
Finland	0.9452	0.8815	0.9706	0.9549	0.9101
Australia	0.9432	0.9053	0.9471	1.0000	0.8825
Sweden	0.9365	0.8882	0.9000	0.9471	0.9625
United Kingdom	0.9358	0.8999	0.9588	0.9292	0.9195
New Zealand	0.9339	0.8806	0.9294	0.9516	0.9207
United States of America	0.9297	0.8769	0.9471	0.9239	0.9182
Netherlands	0.9228	0.8757	0.9059	0.9349	0.9276
Singapore	0.9150	0.8812	0.9647	0.8904	0.8899
Iceland	0.9101	0.8316	0.7941	0.9525	0.9838
Norway	0.9064	0.8557	0.8765	0.9392	0.9034
Japan	0.8989	0.8783	0.9059	0.8684	0.9223

2.5.2 Indicators in EGDI

As the previous section has already given an introduction of the EGDI, this section explains the detailed indicators that consist of EGDI, and its calculation. According to United Nations, EGDI are the numerical indicators that demonstrates the progress of development in e-governance. The range of total indicators are from 0.0 to 1.0 and the world average in 2020 was 0.60. As a statistic, the global average was gradually growing from 0.49 in 2016 to the current number. EGDI classifies member states into three groups; "very high" mark from 0.75 to 1.00, "high" marked from 0.50 to 0.75, "middle " marked from 0.25 and 0.50, and "low" marked from 0.00 to 0.25. (United Nations, 2021 b, p.2)

To look more in-depth at this measurement, a further three indicators give various angles to observe e-government. EGDI consists of three components; Online Service Index (OSI), Human Capital Index (HCI), and Telecommunications Infrastructure Index

(TII). Each component is also a numerical measurement. The calculation of EGDI is simply the average value of these three items.

1, Online Service Index (OSI)

According to United Nations, OSI measures the level of online service that each member states offers to their nationals. The level of online service in this sense means not only administration processes such as residence registration but also the availability of information online. For example, whether the government discloses appropriate information about their countries, and the ease of access to the information portal. To check these maturities and accessibility regarding online service, the research team assessed each state's national website such as national portal, e-service, e-participation portals. In addition, the range of surveys also includes the websites of government ministries of education, labor, social service, welfare, and other related areas. (Ibid)

2, Human Capital Index (HCI)

HCI is the second indicator of EDGI, which is specialized in the literacy of users. As the previous section said, OSI measures the level of online service. In other words, OSI is the indicator for the supply side. In contrast, HCI is more focused on the demand side. At the first glance, the user's literacy in member states does not look related to the development of e-government. However, since the e-government project is supposed to provide a better level of service for nationals, it also requires users to have a certain level of literacy.

United Nation explained four components that constitute HCI. First, "Adult literacy" is the percentage of adults who can read and write the necessary documentation that is required in daily life. Second, the "Gross enrolment ratio", which is a bit tricky. This ratio is the number of students at a certain educational stage divided by the official school-age population. The educational stage in this sense includes the primary, secondary, and tertiary levels of school. What we need to be careful here is age does not equally mean the school-age population. The third is "expected years of schooling". This indicator means the number of years of school education that children who have reached a certain age can expect to receive in the future. Fourth is "Mean years of schooling" which shows the average education years of the adult population. The adult population in this measurement means people who are older than 25 years old. (Ibid) Using these four components, HCI demonstrates the literacy level of expected users who accesses e-government.

3, Telecommunications Infrastructure Index (TII)

The third indicator is Telecommunications Infrastructure Index (TII) that shows the maturity of telecommunications infrastructure in each member state. This indicator is calculated using data from the World Bank and International Telecommunication Union. Researchers can analyze the digital infrastructure and environment that surround e-government and users with this measurement. United Nations explains TII has furthermore, four items that are set up as assessment; "*the number of internet users, number of mobile subscribers, active mobile broadband subscription, and number of fixed subscriptions*". (Ibid, p.232) Therefore, the high score in this indicator means nationals of those countries receive a high standard of availability regarding access to digital society.

3. Conceptual framework

This study uses "cyber resilience" as a conceptual framework to answer the question of "why we can see differences in response to cyber threats for advanced electronic government countries". It is one of the most remarkable concepts as it can solve the problems brought by traditional security approaches.

To build up the logical conceptual framework, this section has three phases. First, the traditional approach of cyber security will be examined along with how it addresses external threats. This phase will review the conventional cyber response strategy and point out its problematic aspects. Then, the next phase moves onto the basic understanding of "resilience" in the social science study, particularly the physical security area. Even though this research simply focuses on the cyber security study, the broad meaning of "resilience" is essential to build up cyber defense norms. In this sense, cyber resilience is one of the categories that a common understanding of resilience study can address. Therefore, we can simply transpose that onto the cyber realm. The last phase elaborates the existing framework of “resilience” and applies it to the digital space. This section will focus more on the technical functions that improve cyber security. Using these three phases, this section precisely demonstrates how we can understand conventional security studies and determine insufficient points of the traditional approach. Also, the latter section outlines comprehensive norm of resilience and apply it to cyber security.

3.1 Traditional approach in cyber security

Traditionally, the use of cyber defense focused on 1) deterrence theory as punishment and denial and 2) finding and stopping source of harm. These two focal points are common in physical security study as well.

First, scholars generally categorize deterrence theory as punishment and denial. Lindsay defined deterrence by denying that the defense side stops the attack by approaching the possibility of the offense side to achieve the goal based on the capability to stop physical attacks. On the other hand, deterrence by punishment means preventing attack by approaching the cost calculation of offense based on retaliation that brings critical damage. (Lindsay, 2015) Accenture also stated that both types of deterrence approaches share the ultimate goal to stop the invasion before reaching the core infrastructure of the defense side. Therefore, states have been trying to build up robust security walls to prevent interference by external actors. (Accenture, 2018) These concepts of denial and punishment are undoubtedly essential when it comes to cyber defense, however, we cannot say they provide perfect national defense as they do not guarantee flawless prevention against cyberattacks.

Second, traditional security foremostly prioritized the challenge of finding and stopping sources of harm. Helm explained the trend of cyber defense in traditional and modern times. In fact, the trend of security management until the 1990s were centered in controlling threats or sources of hazards. In this case, it is necessary to get prior knowledge of risks as preconditions to predict uncertain elements that could possibly threaten either nation or nationals. However, since the current world is more connected and complicated, we can see the limitations of this approach. It is simply impossible to prepare for all potential incidents. (Helm, 2015). Defense and offense play a “cat and mouse game" even if the defense improves security since cyber criminals also keep developing their methods of attack. As long as the defense solely focuses on stopping the invasion, this game is unstoppable.

To sum up, traditional cyber security countermeasures are not enough to deal with today's potential threats in the cyber field. Therefore, states have to develop a robust security system and build up the workflow to continue operation and retain essential functions even if it is under an emergency situation. The next section concentrates on "cyber resilience", which is also a cyber security concept but it compensates what is lacking from the current security study.

3.2 Resilience in social science study

This section will take a look through the overview to determine how we understand "Resilience". This concept is widely used by international relations scholars across many study areas. Helm explained the basic understanding of resilience as the *"behavioral property of a system as it responds to and recovers from the shock"*. (Helm, 2013, p.102) This term demonstrates the capacity to recover from unexpected incidents. In this sense, the system refers not only to the technical platform but also any kind of policy, strategy, and framework. The Organization for Economic Co-operation and Development (OECD) also illustrates this concept as it centers on solving the root causes of security incidents. At the same time, it is also about improving a system's capacity and capability to deal with threats, pressures, and shocks. (OECD, n.d a) This definition emphasizes not only the fight against direct threats but also the importance of the capacity and resources of the system. Considering these two explanations, resilience is the ability to withstand and recover from unexpected or unpredictable impacts.

This concept can be applied flexibly and widely across various fields such as financial or economic frameworks, labor markets, urban developments, refugee crises, cyber attacks, and national security. For example, OECD implements projects in a variety of areas considering the concept of resilience, such as a financial system project monitoring financial risks, analysis, and early warning. In their report, they defined Economic resilience as *"the capacity of an economy to reduce vulnerabilities, to resist* *shocks and to recover quickly."* (OECD, 2016, p.6) Another resilience related project is urban development. In this context, they define resilient cities as cities that can absorb, recover and prepare for the impact that can be predicted in the future by various aspects such as economic, environmental, social, and institutional. (OECD, n.d b) These examples show resilience is a commonly used concept and applied in many fields.

3.2.1 Resilience cycle

Resilience has furthermore detailed steps to enforce security. The OECD has been actively trying to shape a universal approach to resilience. This approach can be used across some different policy areas. According to OECD's definition, we can see resilience with four steps; plan, absorb, recover and adapt. These steps are the so-called "resilience cycle". Systems address emergency response based on this cycle. In the initial process, the system plans against external phenomena and then absorbs the impact of the incident. The latter process recovers from the damage and finally adapts changes. (OECD, 2016) The next section explains each step more in-depth.

First, the system prepares plans to reduce risks. In this sense, "plan " refers to preparing thinkable scenarios as much as possible and assesses various risks in advance. (OECD) In other words, preparations mean setting up countermeasures to sustain essential functions even if under severe situations. The OECD described evacuation training as one of the most obvious examples of strengthening resilience in this step. (Ibid) When we apply "plan" in resilience to evacuation training, we can say that organizers set up training based on estimated risks and scenarios.

Second, the system absorbs the impacts, effects, and results caused by unexpected incidents. At the same time, the system also retains necessary functions and keeps offering service. (Ibid) Therefore, this step is the most pivotal aspect of the resilience cycle. It is crucial if the system and organization can take the appropriate first action includes the set up the emergency response team.

Third, the system recovers the function damaged by the incidents. This process needs rapid recovery, but it might take effort and time depending on the scale of incidents, situation, and level of preparedness. (Ibid) Therefore, the more prepared in advance, as mentioned in the first step, the faster the recovery. In addition, the first and second steps are decisive factors that determine the quality of restoring process.

Fourth, the system adapts necessary changes. In this sense, changes mean building up a more resilient system and improving functions. Connelly et al conceptualized learning from incidents, unexpected attacks, and unauthorized access as "institutional memory". These memories are responsible for retaining learning from past challenges to the system. (Connelly et al, 2017) Therefore, institutional memory is like a "database" for the organization to store lessons from experiences. Using these memories, the organization can implement changes that are required to improve the system for the future.

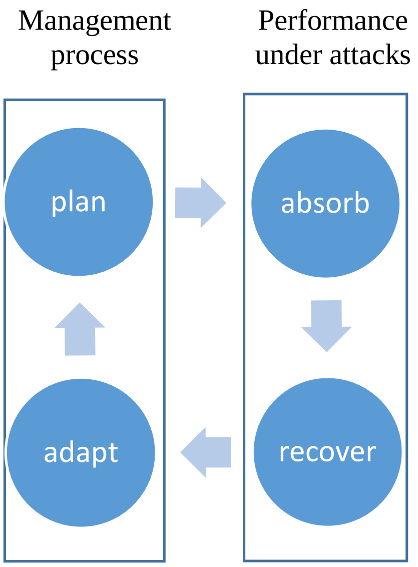


Chart 2: Resilience cycle

(Source from: National Research Council, 2012)

The chart on the left shows the continuous cycle of resilience. Like this section emphasizes resilience consists of four steps (plan, absorb, recovery, and adapt), the system repeats this cycle every time they face incidents. In addition, National Research Council classify these four steps by two groups. "plan" and "adapt" are management process, and "absorb" and "recover" are performance under attacks. (National Research Council, 2012)

Moreover, the organization accumulates lessons from each experience as institutional memory through this model. In detail, lessons defined in the fourth step provide a new point of view to prepare for the future incidents. Thus, the fourth step is directly connected to the first step. In conclusion, resilience not only reduces the risk but also contributes to strengthening the entire framework of the system by repeating this cycle.

3.2.2 Hard military resilience

As the previous section has already indicated, resilience is a broadly used concept in social science study. We can apply this concept to the hard security field as well. This section will demonstrate how we can see resilience in security studies.

To see a practical case that shows resilience in hard military security, it is helpful to examine The North Atlantic Treaty Organization’s (NATO) strategy. NATO is interstate cooperation to ensure freedom and security through political decisions and military operations for member states. (NATO, n.d) Thus, NATO as an institution is highly responsible for building up an effective defense strategy for all allies. NATO actively adapts resilience as the most suitable component in military operations. According to Shea, NATO recognized resilience as a part of comprehensive security strategy, especially in classic military field, it brings deterrence and reassurance. In 2016, NATO held a summit in Warsaw to define, assess and enhance "resilience" as a new concept to strengthen NATO's collective defenses. Based on the concept, NATO established cooperative baselines such as resilient energy supplies, resilient communication system, and resilient food and water systems. (Shea, 2016) Since NATO's purpose is collective security, it indicates each member state can cooperate to compensate if any one of these fields are attacked. Based on that recognition, member states apply resilience to each area. With these baselines, NATO addresses various kinds of crisis situations.

3.2.3 Resilience approaches in physical security study

This section categorizes resilience approaches in physical security study against threats. As a general understanding, security study has some approaches to solve problems and resilience is one of those strategies. Looking at each approach in detail helps us to define in which cases state actors apply resilience. Using these classifications of approaches, we can figure out why countries take different approaches when they faced with threats. As the structure of this section, we will look at the definition of each approach at first. According to Lawrence, Hard security study has three types of approaches to address threats; 1) Security as prevention, 2) Security as control and 3) Security as resilience. (Lawrence, 2013) Then, the latter part moves onto the type of threats that each approach addresses.

The first approach is security as prevention. In this method, states prevent threats that contain security concerns at the early stage of the predicted event. (Ibid) Therefore, this approach tries to eliminate root causes that have potential risks in advance. Thus, the state addresses latent dangers before they turn into manifest threats. Consequently, the state will not be damaged by hostile attackers. The second approach is security as control. This type of approach means countries actively involve themselves to control, defend or eliminate threats. (Ibid) On the contrary to the first approach, this method is for security incidents that have already been recognized as threats. At the same time, we can also see nations address issues with practical force. The last approach is security as resilience. According to Lawrence, the definition of this approach is focused on the social system that recovers from damage if threats cannot be controlled or eliminated. This approach involves the flexibility and adaptability of societies and additionally, it is also concerns how vulnerability to collapse society or cause a chaotic situation can be reduced. (Lawrence, 2013). Like section 3.2 of this research has already mentioned, the broad meaning of "resilience" is applicable to this approach. However, the point that is crucially different from the other two approaches is this method adapts to the existence of threats. Even though security study has some approaches, the decisive factor of these clarifications is the type of threats. In other words, features of threats determine how nations should implement security strategy.

Table 2: Security approach and type of threats

(Source from: Lawrence, 2013)

Security approach	Security as prevention	Security as control	Security as resilience
Type of threats	Mixed-structural and proximate cause	Visible and relatively simple cause	Complex cause

The table above shows what explains why countries need different approaches when they face threats. If the mixed-structural and proximate cause is the factor of threats, the state should apply 1) Security as prevention. Examples of these threats include financial inequality, low-quality governance, and political exclusion. (Ibid) These root causes can lead to unrest and civil war. If threats are already visible but the root causes are relatively simple, countries use 2) Security as control. In this case, governments have already clearly recognized what the threat is. In detail, we can see these threats as conventional military concerns. (Ibid) In cases where threats consist of too many elements and unknown numbers of actors might be involved, 3) Security as resilience is applicable. These types of threats produce non-reducible impacts and unforeseen shocks. (Ibid) Thus, this approach is suitable when threats have complex factors. Nowadays, global society is more connected than ever before and one of those factors is the emergence of the internet. By using modern technology, states have been shaping today's international society and therefore current social issues are likely to contain several complex elements. Similarly, in general this approach is being used more often than before.

To sum up, countries take different security approaches when they face incidents because the most suitable strategy depends on the analysis of the threat. Therefore, it is essential to precisely analyze and measure the threats themselves.

3.2 Cyber resilience

To address the vulnerability of existing cybersecurity norms, cyber resilience is an effective concept. Even if it is cyber space, we can still apply regulations and understandings of physical security study. In terms of resilience, what physical and cyber security have in common is not to eliminate threats completely but to focus more on the process after the incident.

According to Accenture, cyber resilience means the ability and mechanism that minimize the effect and restore system or data rapidly when unknown external actors attack the system in cyberspace. In other words, raising resilience works towards reverting the normal environment as soon as possible and resume essential functions of the system. (Accenture, 2018) In this concept, when setting up security strategy administrators should note as a precondition that hackers may attack or try to invade the system anytime. This precondition finds out how the system addresses the security incident and restores it to the original status.

We can see the difference between the traditional cyber security approach and cyber resilience in "what each strategy prioritizes the most". In the traditional method, the most important point is a countermeasure against cyber threats. In contrast, cyber resilience emphasizes the continuity of functions in the system. In addition, cyber resilience defines the priority inside the whole system and protects information accordingly. In case the hackers reach the firewall, the security system rapidly addresses recovering and tries to minimize the risk. Furthermore, the key components in cyber resilience can be classified by three elements; detection, response, and recovery. The next section will outline each function in detail.

3.3.1 Rapid detection

As the previous section has already mentioned, cyber resilience does not simply focus on blocking the external attack but more so concentrates on actions subsequent to an attack. According to Helm, it is essential to detect unknown access as soon as possible to conduct rapid recovery. This rapid detection enables a quicker recovery and sustains essential services even though the extraordinary situation that is brought on by the attack. Therefore, detection is the first gate of cyber resilience strategy. Based on this concept, administrators generally set up systems that detect cyber attacks on the gateway and inside the system. (Helm, 2015)

The recent study implemented by Accenture proves that detection is the first crucial element in cyber resilience. This study researched security incidents in 15 countries from 2017 to 2018. This period is particularly worth observing because a significant number of ransomware incidents such as WannaCry occurred. As statistical research, they conducted a large-scale survey with 4600 people who are in the position of cybersecurity or risk management chief executives. The data shows that the number of targeted attacks has increased from 106 in 2017 to 232 in 2018, which means almost twice larger than the previous year. On the other hand, the study indicated that the prevention ratio had significant improved, even though the entire case number had increased. In detail, the study’s statistics say that 201 out of 232 attacks were prevented in 2018. (Accenture, 2018, p.7)

The key factor of this ratio about the high standard of robust protection is highly linked to the speed of detection since the incident happened. In the same survey, Accenture said 89% of the total incidents detected unexpected errors or unauthorized access within one month in 2018(Ibid). From this example, we can say rapid detection is the first step of cyber resilience and it is essential to protect the system from external attack. To detect unexpected incidents, protection methods such as access control, encryption that have been argued as useful in data security (section 2.3).

3.3.2 Quick response and recovery

The rest of the essential elements in cyber resilience are response and recovery. These are substantial components that facilitate the sustainability of critical functions in the system even if it is under an emergency situation brought by an external attack. In detail, cyber resilience recommends an organization that manages a system to have an expert team that is in charge of response and recovery. In general, CSIRT (Computer Security Incident Response Team) CERT (Computer Emergency Response Team), and CISO (Chief Information Security Officer) are organizational models of core institutions to respond to security incidents.

According to Wara and Singh, CSIRT defines the range of estimated influence of attack and takes actions to sustain the essential function of the system. They collect information about attacks, analyze logs and infected devices, and coordinate between related departments, including external experts and system recovery. In short, they actively work not only with system administrators but also with the various fields of related departments such as administration and higher authorities who make decisions. In this stage, the vital role of CSIRT is to collect necessary information and suggest board executive members. (Wara and Singh, 2015) With this information, they are equipped to make appropriate decisions as the most crucial priority in cyber resilience is sustaining essential functions rather than eliminating threats. More specifically, appropriate decisions means which part of the system they should give up and how they use the workforce to retain critical functions. Thus, CSIRT is a supporting role that closely works in the decision-making process.

Wara and Singh also noted that it is not impossible to predict the lowest level of the pattern of attack as long as the organization prepares a security regime such as CSIRT. In addition, CSIRT offers solutions that detect attacks and unauthorized access with the recent development of AI and deep learning system.(Ibid) CSIRT addresses unexpected attacks from various angles, from investigating status to the prediction of future patterns of attacks.

Likewise, CERT is also a vital team in the organization that actively works against security breach incidents. Moyle said CSIRT and CERT are often used as nearly equal terms. Since both are cyber response units, practical affairs are the same, but we can see a subtle difference in the internal team's focus. CERT is more focused on an association with either external or internal actors when it comes to security improvement. (Moyle, 2021) Therefore, CERT is a security team not only organized to solve issues but also works by the meaning of cooperative approaches toward other related institutions.

On the other hand, CISO is an equally important position in security management, but more like a responsible role than CSIRT and CERT. Accenture defined CISO as an independent position from the IT team that manages the security regime of an organization. This separation aims to establish a framework in which executive board members can clearly understand security risks. (Accenture, 2018) The key point here is CISO should be apart from the main IT team of the organization and should analyze risk and the whole security structure from different angles. This independence provides an objective point of view and makes risk management ability much stronger.

3.4 Geopolitics and cyber threats

This section will outline geopolitics and how it relates to cyber secutity. Geopolitics is a comprehensive approach to the study of international relations, which has multiple facets such as cultural, economic, and security. Historically, most interstate conflicts have hugely relied on geographical factors. For example, "borders" are socially constructed lines that distinct one state from another. Various social elements such as economic gain, political ideology, and religion cause international conflicts across borderlines. Consequently, geographical elements are extremely connected to state-to-state security. Furthermore, we can now also see geopolitical concerns extending into cyber spaces in our current global society. This section will briefly outline the basic understanding of geopolitics and then transpose it to cyber realms.

Geopolitics is an approach that considers actions in international society and relations with between territories based on geopolitical preconditions. According to Flint, understanding geopolitics is to comprehend how international politics are related to geography, and how these relations explain contemporary conflicts and issues. (Flint, 2016) For example, we can see different defense strategies in countries that are surrounded by sea compared with others who share land borders with neighboring countries. Flint also explains that national defense and actions in international politics, and the global economy are closely related to geopolitical elements. In this sense, the most obvious benefit of geopolitics is to obtain perspectives that control other nations while putting themselves in a superior position. (Ibid) Using this advantage of geopolitics, it is possible to manage other countries without high-risk options such as invading the territory of neighboring states. In detail, low-risk control in this sense means, for example, importing materials from neighbors at a reasonable price.

As this section has already mentioned, the most obvious benefit of geopolitics is to control other nations. The central idea of this study is "balance of power". According to Morgenthau, the balance of power means *"to an actual state of affairs in which power is distributed among several nations with approximate equality."(*Morgenthau, 1960, p. 156) In other words, it means the balance of power is the mechanism of international relations that retains the world order by equaling power without granting one certain country overwhelming hegemonic power.

It is internationally recognised that geopolitical factors are now affecting cyber space as well. Geopolitical cyber crime is intensifying every year and its damage is not only impacting critical infrastructures, but also causing more economic loss and impacting business. Under these situations, states, sub-national units, and companies should swiftly protect themselves before their critical systems are exposed to threats. Thus, these entities should prepare appropriatly with enough ability to recover from attacks. The European Commission clearly stated that cyber offense is a significant new vector that gains military dominance, collapses social infrastructure, and greatly impacts the economy. In terms of geopolitics, cyber attack is a new instrument that affects politics, military, and international relations. (European Commision, 2017) Additionally, Crowdstrike describes improving cyber attack capability as an "arms race" to seek cyber superiority on the global stage. (CrowdStrike, 2019) In this sense, arms race literally indicates competition regarding offense capacity. Based on the "balance of power" theory, cyber attack is one of the means that reduce superior power in one region. Therefore, geopolitical elements are severely connected to cyber security study.

Furthermore, cyber attack is crucially different from conventional military actions in terms of cost and effect. According to Lipton, Sanger, and Shane, both state and non-state actors improve cyber tools as geopolitical approaches for three reasons; reasonable cost, effectiveness, and predictability. (Lipton, Sanger, and Shane, 2016)

Firstly, cost is one of the most prominent aspects of superiority of cyber space. CrowdStrike said the crucial difference between physical and cyber security is that anyone can potentially become a ruler in cyber space regardless of financial status. In fact, some of the poorest nations proved that they have the cyber ability to have an impact on the world order. (Crowd Strike, 2019) In detail, we can say military actions cost a lot in general, such as governments having to invest a lot of funds into the training for military units, costs of the necessary physical space kept for storing tools and camps, and in case the state wants to base their allies' army within their territory, they also need to set up daily infrastructure and supply basics. In contrast, cyber actions need initial investent such as computers and networks but it is still relatively low-cost compared to the hard security approach. Secondly, a cyber attack can give an effective impact with less effort. Either state or non-state actors can directly attack the critical infrastructure of the targeted organization or country. And finally, it is hard to predict what states are attempting an attack on which part of the critical system and how. As a precondition, we need to again highlight that artificial realms are unseen. Attackers will aim at vulnerabilities of the system from blind spots, thus the defense side can’t detect the tendency in advance.

To sum up, cyber attack is utilized for highly political reasons nowadays. Since it is a low-effort and high-profit tool to pursue geostrategic interests for state and non-state actors, international society should pay more attention to cyber security strategy.
From these facts, we can say cyber resilience that has been mentioned in section 3.3 is an effective countermeasure against geopolitical cyber threats. Features of cyberattacks mentioned previously clearly indicate why we need cyber resilience in terms of geopolitical perspective. The answer is straightforward, states need to build up resilience because it is impossible to establish a perfect defense. Geopolitics brings a perception that uneasy feelings of neighboring countries easily turn into tension as a visible form, and then transform as threats in the end. Moreover, cyber attack is a relatively low-cost and quick tool for affecting targeted states. Therefore, we can see the connection between geopolitics, cyber security, and the necessity of cyber resilience.

3.5 Expectation from concepts and theory

Concepts and theory indicated three expectations. First, geopolitical interstate tensions simply transpose to the cyber realm. Traditional geopolitics told us how states bring geostrategic elements into state-to-state relations. At the same time, geopolitics are closely connected to some social factors includinges economy, culture, and security to solve issues across borders. State actors apply the geopolitical approach to address interstate conflicts while putting themselves in a superior position with these factors. Likewise, cyber realm is a new norm of the national territory and , we can nowalso see geopolitical tension in cyberspace. Therefore, we can observe how several of those factors affect interstate relations, include cyber warfare and the necessity of a resilience approach through the geopolitical scope.

Second, analyzing the type of threats demonstrates what approach state actors should take and in which cases. According to hard security study, the decisive factor for state actors to take security approaches are features of threats that they need to address. In short, 1) security as prevention is for mixed-structural and proximate causes, 2) security as control is for visible and simple causes, and 3) security as resilience is for the complex causes with an unknown number of variables. These approaches and classifications are applicable in cyberspace as well, . tTherefore, state actors need to analyze types of cyber security threats and then apply appropriate approaches accordingly. We expected the pattern of security approach to cause differences in cyber resilience level.

Third, the technical components of cyber resilience refer to what is lacking from cyber security preparedness of each country. Cyber resilience has four components; retaining critical systems, rapid detection, quick response and recovery, and decision-making process. The main objective of this security approach is retaining critical systems rather than eliminating threats. Then, the system should detect security breaches such as unauthorized access or unexpected errors. In case of an accident, the system administrators should take quick responses and try to recover from the damage, Ultimately, the organization should take appropriate decisions to decide which part of the system should be the most prioritized even if they need to give up some others. Using these four components, we foresee what each e-government should improve for security preparedness.

4. Research design and methods

To answer the research question defined in the first chapter, an appropriate research design will be required to figure out the key factor that produces the difference. Although many countries in the world address installing e-governmental frameworks to increase the quality of public service as well as build up better national safeguard, similarity and difference regarding the maturity of cyber defense that each e-government has will give this study it's direction. In this sense, the direction means, "in what sense cases are similar", and "how much and why these are different".

Comparing of maturity of e-government by the national security aspect is not an easy method because each state has a different status, development, and precondition. However, this research set several criteria that have a numerical measurement that the next section will explain, to give rationales why selected cases should be compared. Also, these criteria give enough persuasive reasons of how we can equally observe selected cases. Therefore, we can expect this research will become essential and valuable for determining future national cybersecurity tactics.

This research uses "comparative study" as a research design to seek differences between the successful and undeveloped model of e-government regarding cybersecurity. The comparative study is one of the research methods that compare more than two numbers of objects, ideas, and cases. Using this method, researchers can compare selected cases and analyze similarities and differences. Esser and Viliegenthart gave a comprehensive overview of comparative study. This study method is generally recognized as the comparison between various types of macro-level units that include world region, nations, social environment, and language areas. In addition, comparative studies provide new perspectives when we focus on one object too much. Comparison raises awareness of other objects, patterns, or systems, therefore it enables us to contrast the original object more critically. (Esser and Vilegenthart, 2017)

To conduct effective research, it is also necessary to define case selection. Since this research addresses what produces the differences in response to cyber threats regarding e-government, it is necessary to simply focus on the cybersecurity aspect rather than other functions of digital governance. As this research has already mentioned in the first chapter, e-government has various functions such as delivering public service online, increasing transparency, and reducing the administrative workforce and load. However, the next empirical section will not be a comprehensive assessment of e-government, it will analyze the security dimension precisely. Therefore, cases that have equally high developed e-government but some difference in the cybersecurity realm are ideal.

Considering these preconditions above, this study uses Most Similar System Design (MSSD), a broadly used research method by scholars in the social science study field. According to Steinmetz, MSSD is one of the research strategies that compares cases which are significantly similar, but different in some parts. Meaning some parts in the structure or process of study cases produce a certain different results. The advantages of MSSD for researchers are 1) controlling elements that are not causal factors and 2) isolating key objects that explain the difference. (Steinmetz, 2021) In other words, the first step is finding similarities between both cases to eliminate factors that are not related to the result by comparing similar points. The second step is zooming into difference. With these two steps, the next empirical section will compare cases and find out differences and then elaborate on them for further analysis.

4.1 Case selection

To conduct the empirical section, the study picks up Estonia as a successful model and South Korea as the case that we can expect further improvement. As a rationale of these case selections, the four criteria mentioned below are helpful to understand the structure of comparison. The first, second and third criteria show that cases are at a similar level regarding the wide range of digitalization included in the e-governmental framework. On the other hand, the fourth criteria demonstrate that these cases produce a certain difference even though they have similarities. As the previous section mentioned research design, finding similarity eliminates these factors from the analysis subject and proves they are not related to the result. Thus, these four criteria are persuasive enough signify that the selected cases have validity.

- States have e-government with high performance.

The case study should have e-government that already has a certain level of high performance because we will focus on the aspect of cybersecurity rather than maturity of overall digital governance. Therefore, this study should select countries from these top 14 states.

- States have a high standard of digitalization

The study cases should have a high standard of digitalization because digital adaption is one of the preconditions that e-government works as a national framework. To assess the level of digitalization, Digital Adoption Index (DAI) implemented by The World Bank is the practical indicator. According to the World Bank Group, DAI measures the extensive range of technology utilization in each state, and it shows how technology is received by nationals. (The World Bank, 2016 a) Thus, we can see the standards of digitalization through these indicators.

- States that have geopolitical concerns

Comparing study cases that have geopolitical concerns is suitable empirical design to analyze the aspect of e-government in security study more precisely. As section 3.4 has already mentioned, geopolitical issues have emerged in cyber space. In addition, cyber security is the partially extended version of hard security study. Therefore, a set of countries that have security concerns with their neighbors brings a new perspective in terms of e-government as national defense.

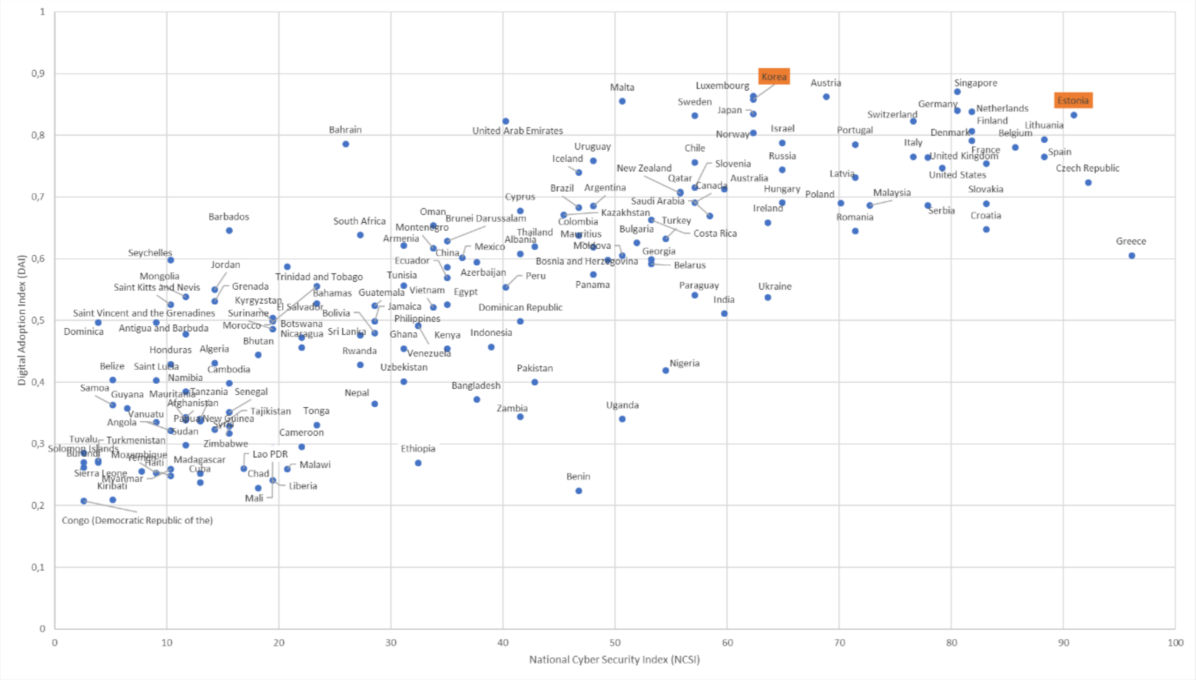
- States that are different in the level of cyber security

Since this study focuses on security issues in the digital field, the study case should differ in preparedness against cyber threats. In other words, the level of cyber security in each e-government is the outcome of the cyber strategy that countries have. This is the obvious variance in selected cases that the latter analysis part will look at more in-depth. To look into the gap between cybersecurity countermeasure of each country, National Cyber Security Index (NSCI) is a useful indicator. According to Maaten, this index shows the range of preparation to protect e-government from cyber threats. (Maaten, 2020)

Considered these four criteria for selecting study cases, the scatter diagram below shows Estonia and South Korea have highly developed digital standards but differ in terms of cyber security preparedness. Moreover, these two countries share the border with neighbors that have security concerns. Since they are in geopolitically similar situation and have high standards of digitalization but different regarding the preparedness of cybersecurity, we can see the puzzle here. Consequently, the goal of using this research method is to see what explains this puzzling difference.

Scatter diagram 1: Cross sectional data of DAI and NCSI

(source from: e-Governance Academy Foundation, n.d c, and The World Bank, 2016 b)



Besides Estonia and South Korea, we can also see some cases such as Malta and Singapore that have the same level of digitization and different status of cybersecurity maturity. As we can see in the diagram, Malta exhibits a high number of digital infrastructure. However, they are not in the top 14 countries of EDGI ranking. Therefore, we can say they have a high standard of digitalization but do not utilize its technology in developing e-government. On the other hand, Singapore also marks a high score of DAI and NCSI but they do not have emerged geopolitical concerns. Thus, we cannot see the linkage between e-government and the hard security field in this case.

The Estonian and South Korean cases seem similar but the difference in the outcomes could result from some hitherto unobserved elements in external factors. Furthermore, it is also vital to observe differences in internal factors analyzed by the cyber resilience framework. The next section will do an in-depth analyze of cyber security preparedness with NSCI and then apply cyber resilience framework to assess each strategy. Using the outcome of the analysis, we will figure out both external and internal factors that result in differences between the case countries. In this sense, this research sets up those three perspectives as factors; regional cybersecurity situation, nature of neighbors, and the country's internal dynamics. With these factors, this comparison illustrates how geopolitical perspectives motivate or have an impact on the e-government framework. At the same time, the analysis brings a new angle that perceives e-government on the extended line of hard security study.

5. Empirical data and sources

This study analyzes and compares the outcome of e-government in each targeted state. Although the global community recognizes that both Estonia and South Korea have highly developed e-government, South Korea is less prepared for cybersecurity, particularly so in terms of cyber resilience.

Since this study focuses on the security aspect of e-government, the selected cases should differ in preparedness against cyber threats. As this research has already mentioned in the beginning, the "e-government survey" conducted by the United Nation provides various aspects of e-government. In other words, the UN's survey has a comprehensive approach but does not have a specific scope to measure security strength more in-depth. Therefore, this empirical section should use the indicator that is more specialized in the security dimension of e-government.

To look into the gap between cybersecurity countermeasures, National Cyber Security Index (NSCI) is a useful measurement. According to Maaten, this index shows the range of preparation to protect e-government from cyber threats with a score of 0-100. Additionally, the index also addresses risk management and related processes after attacks. (Maaten, 2020) The next section will outline the framework for this measurement and describes detail structure and assessment.

5.1 Framework of NSCI

This section demonstrates components that consist of NSCI. First, it is necessary to precisely outline security threats that e-governments of each state have to face. E-Governance Academy Foundation clearly defined objects that e-government have to face in terms of national defense. Fundamental security threats are categorized by three types; 1) Denial of e-services, 2) Data integrity breach 3) Data confidentiality breach. (e-Governance Academy Foundation, n.d a) We can analyze these three classifications based on the "CIA triad". As section 2.2.2 of this research has already mentioned, the CIA triad (Confidentiality, Integrity, and Availability) is the common framework in information security study. Also, this model explicitly indicates the "worst scenario" that the system must avoid. Using CIA triad, we can explain the security threats that NSCI defines.

1) Denial of e-service

Denial of e-service loses "availability" of the CIA triad. In the case of cyber attack, a hacker group attacks an e-government and the system partially or entirely loses its part of the function. As the result, both demand-side (users) and the supply-side (government) lose the availability of the service.

2) Data integrity breach

Data integrity breach literally loses the "integrity" of the CIA triad. As we have already recognized, the e-government is the place where information that has a certain value as the asset is gathered. Therefore, it is quite likely that unknown users attempt unauthorized modification.

3) Data confidentiality breach

Data confidentiality breach is related to the "confidentiality" of the CIA triad. E-government has various types of e-services. For instance, an online electoral process demonstrates the expectation of confidentiality. In this example the ballot should have a high level of confidentiality otherwise the results could be hugely affected. In this sense, a cyber attack against e-government contains the possibility of a severe data confidentiality breach.

5.1.1 The structure of measurement

To assess countermeasures against security threats surrounding e-government, NSCI has three categories and four sub-categories. The three main categories are baseline cyber security, incident management, and general cyber security development. Baseline cyber security provides the protection of digital services, protection of essential services, e-identification and trust services, and protection of personal data. Incident and crisis management indicate cyber incident response, cyber crisis management, fight against cybercrime, and military cyber operations. General cyber security illustrates cyber security policy development, cyber threat analysis and information, education, and professional developmental contribution to global cyber security. In addition, each of these four sub-categories have multiple numbers of indicators. For example, “1. Protection of digital service” contains three indicators that assess 1.1Cyber secutity responsibility for digital service providers, 1.2 Cyber secutiy standard for the public sector, and 1.3 Competent supervisory authority. Likewise, the rest of other 11 sub-categories also have detail indicators. The total number of indicators is 46. To sum up, NCSI measures the security aspects of e-government from several categories with detailed indicators.

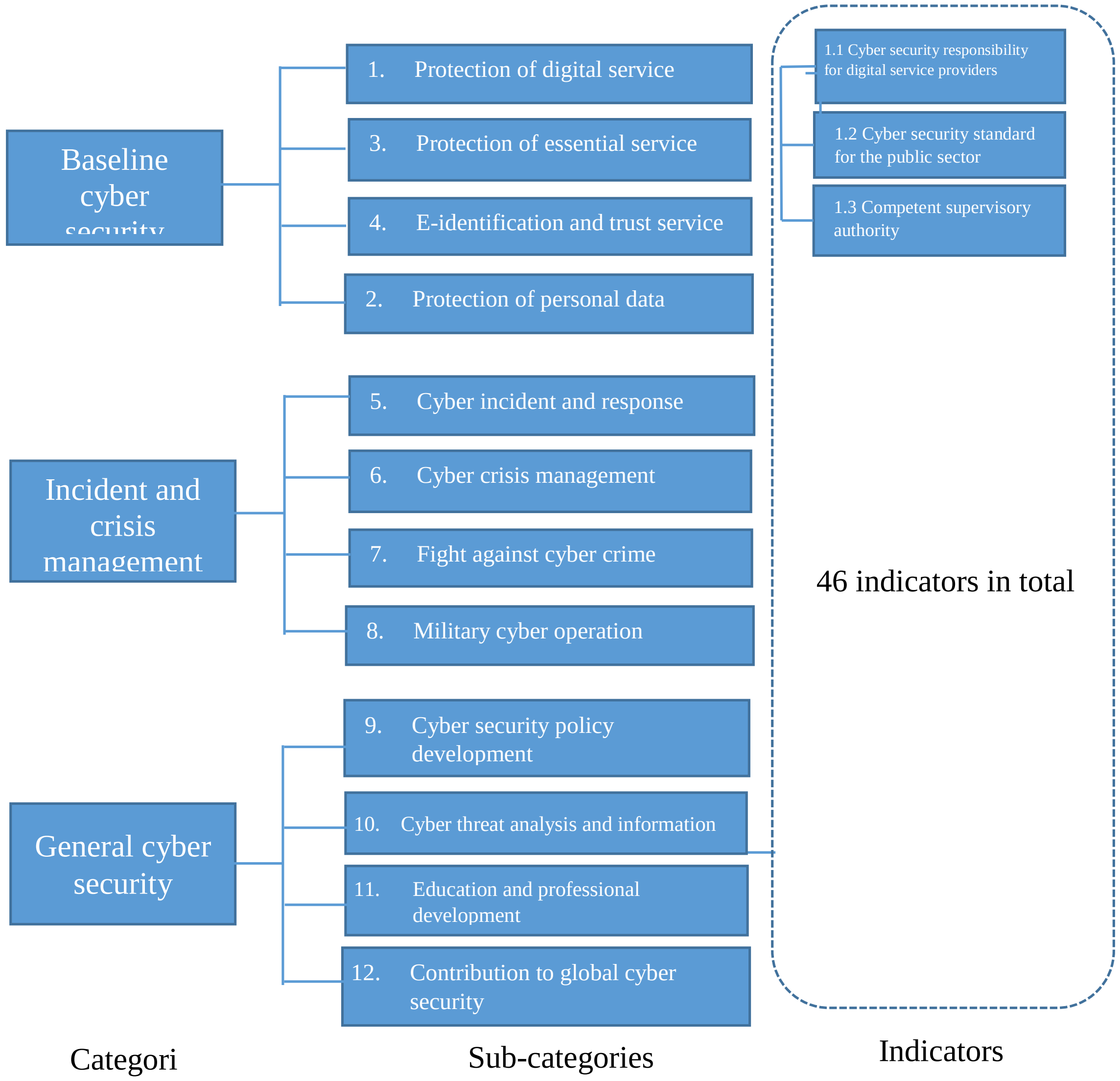

Baseline cyber security
1. Protection of digital service
3. Protection of essential service
4. E-identification and trust service
2. Protection of personal data
1.1 Cyber security responsibility for digital service providers
1.2 Cyber security standard for the public sector
1.3 Competent supervisory authority
Incident and crisis management
5. Cyber incident and response
6. Cyber crisis management
7. Fight against cyber crime
8. Military cyber operation
46 indicators in total
General cyber security
9. Cyber security policy development
10. Cyber threat analysis and information
11. Education and professional development
12. Contribution to global cyber security
Categori
Sub-categories
Indicators

Chart 3: Categories of indicators

(Source from: e-Governance Academy Foundation, n.d b)

5.1.2 Assessment

Each indicator has a different range of scoring. These scores demonstrate the relative importance of each indicator in NSCI. Ranges are; legal act that regulates a specific area for 1 point, specialized unit for 2-3 points, the official cooperation format for 2 points, and outcome or product for 1-3 points. For example, the “1.2 cyber security policy coordination format” is categorized as “the official cooperation format” in this scheme. Therefore, 2 points are given to this indicator as a full score.

Likewise, NSCI measures cyber security strength with 46 indicators assessed by 1-3 points. The total max score of 46 indicators is 77. NSCI scores are calculated as below

NSCI = country points * 100/ max points

For example, Estonia got a total of 70 points in the three categories. Using this value, we can calculate NSCI score as below;

Country points (70) *100/77=90.90909091

Points should be rounded up, so that the final score of Estonia is 90.91.

5.1.3 Data collection

Numerical measurement is not only the feature of this index, as NCSI also works as a valuable database for researchers in cyber defense and e-government study. Since the research team of NCSI collects publicly available information, scholars can access the indicated data or evidence and make sure it is valid. For example, the first category of general cyber security measures “9. cyber security policy development”. This category has a further four detailed measurements. One of those indicators is “9.2 cyber security policy coordination format” that assesses the organizational framework of the cyber defense field. According to e-Governance Academy Foundation, the definition of this criteria is that the government has a commission, assembly, specialized working group, and other related institution as a national level cyber security policy coordination. The research team checks either the official website or legal act as evidence to be assessed if the targeted country fulfills this requirement. (e-Governance Academy Foundation, n.d b) In this section, Estonia got a full score. According to the survey, 3rd paragraph of the first topic in the submitted website said *"In 2009, the Cyber Security Council was established at the Security Committee of the Government of the Republic. The task of the Council is to contribute to smooth cooperation between various institutions and conduct surveillance over the implementation of the goals of the Cyber Security Strategy. The Council is chaired by the Secretary-General of the Ministry of Economic Affairs and Communications.*" (Republic of Estonia Ministry of Economic Affairs and Communications, 2020, first topic, third paragraph) Based on the information from the website, we can say Estonia has the necessary institution to implement national cyber security. Likewise, the research team found all necessary data collection for 46 indicators and assessed the strength of cyber security in each country.

5.2 Case analysis of Estonia and South Korea

This section examines cyber security aspect of selected cases. First, we need to compare values that we can see in main categories and sub-categories to measure which part of the cyber defense strategy of each government is different in detail. As the previous section has already mentioned, these categories are helpful to understand classification.

Table 3: Comparison of cyber security/ categories and sub-categories

Source from: (e-Governance Academy Foundation, n.d b, and e-Governance Academy Foundation, n.d d)

	Estonia	**South Korea**
Baseline Cyber Security	**23**	**10**
1, Protection of digital services	5	2
2, Protection of essential services	6	0
3, E-identification and trust services	8	4
4, Protection of personal data	4	4
Incident and Crisis Management	**23**	**13**
5, Cyber incidents response	6	3
6, Cyber crisis management	5	3
7, Fight against cybercrime	6	7

8, Military cyber operation	6	0
General Cyber Security	**24**	**25**
9, Cyber security policy development	6	7
10, Cyber threat analysis and information	5	5
11, Education and professional development	7	8
12, Contribution to global cyber security	6	5

From the table above, we can observe two cases are similar in "general cyber security". Precisely, four sub-categories in general cyber security are not about the technical part of cyber security strategy. They are more focused on policy, analysis, education, and contribution to global cyber security. In other words, this category is the comprehensive framework of cyber defense. Since the study cases are similar in this category, the analysis part focuses on the rest of the two categories to seek the difference.

Although Estonia and South Korea are similar in "general cyber security", we can also see the overwhelming differences in "Baseline cyber security" and "Incident and crisis management". Roughly speaking, Estonian security strategies two times stronger than South Korea in these areas. Therefore, the next section does an in-depth zoom in on these fields and analyzes these features.

5.2.1 Applying cyber resilience framework

This section uses the cyber resilience framework as explained in the third chapter. Briefly speaking, cyber resilience is built on these basic factors; retaining critical systems, rapid detection, quick response and recovery, and decision-making process. Therefore, we will apply this framework to those two categories that we have already figured out in the previous section.

The analysis order is; 1) classify each indicator by core components of cyber resilience that are listed. 2) sum up scores based on classification.

Regarding classification, criteria are as listed below;

- *retaining critical system* - components that are related to maintaining the essential systems for the domestic society.
- *rapid detection* - technical schemes that detect unauthorized action or threats
- *quick response and recovery* - practical countermeasure against unexpected incidents
- *decision-making process* - supervisory authority that determines operations, or any actions related to critical decision for the entire system
- *other* - indicators that are not relevant to cyber resilience

1) Classify each indicator by core components of cyber resilience

Using the criteria above, we can analyze baseline cyber security and incident and crisis management for Estonian and South Korean cases, as seen below. Each category has four sub-categories, and then we can see furthermore multiple numbers of indicators. Each indicator is assessed on the scale of 1 to 3 (0- no exist, 1- weak, 2-moderate, and 3-strong).

Table 4: Baseline Cyber Security assessed by cyber resilience framework

Source from: (e-Governance Academy Foundation, n.d b, and e-Governance Academy Foundation, n.d d)

Baseline Cyber Security	**Estonia**	**South Korea**	**Category in Cyber Resilience Framework**
1.1 Cyber security responsibility for digital service providers	1	1	retaining critical system
1.2 Cyber security standard for the public sector	1	1	retaining critical system
1.3 Competent supervisory authority	3	0	decision making process
2.1 Operators of essential services and identified	1	0	retaining critical system
2.2 Cyber security requirements for operators of essential service	1	0	retaining critical system
2.3 Competent supervisory authority	3	0	decision making process
2.4 Regular monitoring of security measures	1	0	rapid detection
3.1 Unique persistent identifier	1	1	rapid detection
3.2 Requirements for cryptosystems	0	0	rapid detection

3.3 Electronic identification	1	1	other
3.4 Electronic signature	1	1	other
3.5 Timestamping	1	1	rapid detection
3.6 Electronic registered delivery service	1	0	rapid detection
3.7 Competent supervisory authority	3	0	quick response and recovery
4.1 Personal data protection legislation	1	1	other
4.2 Personal data protection authority	3	3	other

Table 5: Incident and Crisis Management assessed by cyber resilience framework

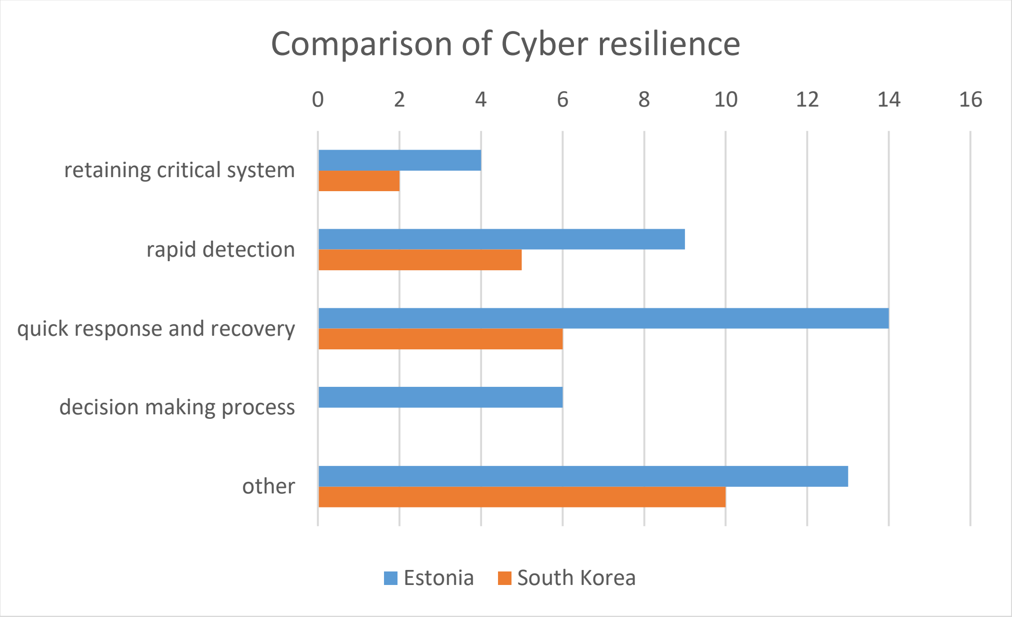
Source from: (e-Governance Academy Foundation, n.d b, and e-Governance Academy Foundation, n.d d)

Incident and Crisis Management	Estonia	South Korea	Category in Cyber Resilience Framework
5.1 Cyber incidents response unit	3	3	quick response and recovery
5.2 Reporting responsibility	1	0	quick response and recovery
5.3 Single point of contact for international coordination	2	0	other
6.1 Cyber crisis management plan	1	0	quick response and recovery
6.2 National-level cyber crisis management exercise	2	2	other
6.3 Participation in international cyber crisis exercises	1	1	other
6.4 Operational support of volunteers in cyber crisis	1	0	quick response and recovery
7.1 Cybercrimes are criminalized	1	1	other
7.2 Cybercrime unit	0	3	quick response and recovery
7.3 Digital forensics unit	3	3	rapid detection
7.4 24/7 contact point for international cybercrime	2	0	rapid detection
8.1 Cyber operations unit	3	0	quick response and recovery

8.2 Cyber operations exercise	2	0	quick response and recovery
8.3 Participation in international cyber exercise	1	0	other

2) Sum up scores based on classification

This section sums up all scores from each indicator per components in cyber resilience framework. Based on clarification, total scores from 1.1- 8.8 are categorized as below;



Graph 1: Comparison of cyber resilience[2]

Along with the concept of cyber resilience, these observations indicate two findings. One is that South Korea is not prepared if external actors attack them because their protection for essential service and operation is still weak. Cyber resilience's core factors are maintaining essential service and retaining operation even if external hackers attack them. However, Graph 1 indicates that South Korea is not ready for that. The other is that South Korean cybersecurity strategy is still focused on more deterrence by denial and punishment than resilience. At the moment, South Korean cyber strategy focuses more on fighting against cybercrime than other sectors.

[2] Created by the author of this thesis using table 4 and table 5

6. Case Analysis

To examine why South Korea's cyber resilience is comparatively lagging far behind to Estonia, it would explain differences in so-called hard security issues along the same lines. Helm explains resilience in security study provides more practical principles for insecure situations than risk management. Resilience is not only about reducing damage from attackers but also demonstrating how the whole process of security represents and adapts to internal and external factors. (Helm, 2015) We can see the same protocol in the cyber realm. These factors that lead to the lagging of cyber resilience can be divided broadly into internal and external elements. Therefore, this study explains three aspects; 1) regional cybersecurity situation, 2) nature of neighbors, and 3) the country's internal factors. 1) and 2) are categorized as external factors. It is the offensive cyber capabilities of the neighbors and the threat situation between the neighbors. On the other hand, 3) is the internal factor that describes how specific issues in the domestic area disturb building resilience in cyberspace.

6.1 Regional cybersecurity situation

In order to analyze the Estonian case, section 6.1.1 focuses on a massive cyberattack in 2007. The reason why we need to pick up particularly this even is that this case highlights the weakness of the conventional system and triggered to set up the current cyber defense strategy. Estonia and Russia have been under a certain level of tension for a long time. After Estonia experienced this large scale of cyber incident, this country has been trying not only to build a robust security wall but also preparing for the worst scenario based on cyber resilience. Therefore, this attack was the most prominent turning point for Estonia, and what comes after that is somewhat less important.

On the other hand, we need to address the multiple numbers of cyber attacks to analyze the South Korean case in section 6.1.2. As this section mentioned in the beginning, one large attack changed the paradigm of cyber security in Estonia. In contrast, South Korea has experienced more continuous incidents in cyberspace. Thus, this section 6.1.2 will take a look through the series of cyber attacks and observe how it has been changed. Using analysis, we can point out why we can see different levels of cyber resilience.

Like the Estonian case, the relationship between South Korea and North Korea has also been highly strained since the 1950s up until the present day. Park, Rowe, and Cisneros reported North Korean cyber attackers targeted both public and private sectors such as companies and media since 2009. In addition, hackers' intelligence has kept evolved and could destabilize South Korean digital society. (Park, Rowe, and Cisneros, 2016) Section 6.1.2 will focus on these events more in-depth and show how it relates to cyber strategies.

6.1.1 The history and observation of cyber attack in Estonia

This section will outline the historical background of cyber attacks in Estonia. As it is often mentioned in cyber security studies, Estonia experienced a large-scale cyber attack in 2007. This incident garnered global attention and was viewed from two angles. Foremostly, it was the first interstate cyber warfare in history which prompted serious concerns for European states in terms of national sovereignty in digital space. (NATO Strategic Communications Centre of Excellence, 2019) Considering the history of digital governance, 2007 was still in the early stage of digitalization, therefore this incident was a prominent example of how national sovereignty could be threatened in the digital realm. Secondly, the incident had the potential to undermine public's trust in the government's ability to protect the entire country from extraordinary threats. (Ibid) Around the 2000s, Estonia had already declared that it would be the leading state of digitalization in the EU. At the same time, their strong posture could be understood as the sort of commitment to promoting to build up digital society for Estonian nationals. Thus, emergency response under the attack and quick recovery from the damage was deciding factor for whether they would continue digitalization.

This incident strongly demonstrates how extending political conflicts transpose to cyberspace. Mattiise and Juurvee outlined the background information of tension between Estonia and Russia. Estonia had been struggling to obtain liberal democracy for a long time. During the second world war, they were under the control of Nazi Germany and the eventual entry of the Russian army into Estonia released them from the Nazi's occupation, however Soviet subjugation started instead. (Mattiise and Juurvee, 2020) In addition to the historical background, we need to emphasise that approximately 330,000 out of 1.3 million of the total population are ethnic Russians.

(Statics Estonia, 2020) From this information, we can say two facts; 1) Russian action released Estonia from Nazi but it does not mean Estonia got its own liberty. 2) 30% of the population inherited Russian identity and that needs to be considered and respected.

According to Mattiise and Juurvee, the Estonian government decided to relocate the "Bronze Soldier" in Tallinn which was the symbol of Soviet times. Russian residents in Estonia strongly opposed this because the decision ignores their part of ethnic identity. To support Russian inhabitants, Russian political authorities sternly expressed that defiling monuments is an insulting action against contributors who saved Estonia from Nazi occupation. On flipside, the Bronze Soldier reminded Estonian citizens of occupation and deportation by Russia. (Mattiise and Juurvee, 2020) Therefore, the statue constantly produces psychological pain for nationals. Conflicting perception of each group brought a certain level of tension to bilateral relations. Additionally, since Russia supported Russian residents in Estonia, this tension turns into conflict on an international level.

This series of high political tensions caused a massive scale cyber attack on 27th April, lasting for 22 days. Mattiise and Juurvee described these 22 days as "The Bronze Soldier crisis of 2007" and outlined detailed incidents chronologically. This cyber incident can be classified into five phases. In the first phase, relatively simple security breaches using denial of service (DoS) attacks were carried out from 27th to 29th April. Targets were mainly government and media websites, but it did not affect critical infrastructures such as transport and energy sectors. The second phase of the attack started on 4th April where websites and domain name servers (DNS) were attacked by distributed denial of service (DDoS). The third phase was from 8th to 10th April, still with intensified DDoS, but this time major Estonian banks were targeted, therefore having a huge impact on Estonian citizens and society. In the fourth phase on the 15th May attackers used approximately 85,000 hijacked computers to conduct DDoS attacks against government websites and large Estonian banks. The last phase on the 18th May consisted of a massive scale of DDoS attacks continuously interrupting governmental web portals and banks. (Mattiise and Juurvee, 2020)

This cyber-attack in 2007 clearly demonstrated the weakness of conventional security systems in Estonia, and the necessity of cyber resilience. In this case, the weakness of Estonian cyber security was that all necessary social functions were gathered in the centralized system. Consequently, once the external actor succeeds in attacking the core system, it destabilizes not only cyberspace but also brings critical damage to the base of the national structure. In fact, the attacker group targeted the Estonian representative server and conducted DDoS attacks from multiple botnets simultaneously. As a result, the whole series of attacks had been constantly delivering huge damage to Estonian social infrastructure for 22 days. Since its scale is too large, it was impossible to address these threats with traditional security approaches such as denial and punishment. Thus, this incident was the turning point for Estonian cybersecurity causing a shift towards a focus on cyber resilience.

6.1.2 The history and observation of cyber attacks in South Korea

South Korea and North Korea have had a long history of political conflicts. From an international relation's perspective, the tension between these two states is the highest in the East Asian region. Historically, they experienced physical conflicts using military force particularly around the 1950s, but we can still see offensive behavior in both the physical and cyber realms today. Since cyberspace is the new territory of nations, it is understandable that these interstate conflicts now turn into cyberwarfare in the present day.

We can categorize the history of cyber-attacks that happened on the Korean peninsula into three-time phases. The first phase was from 2009 to 2013 and was considered to be the early stages of the development of South Korean digital governance. In 2009, the first large-scale cyber attack seriously damaged the South Korean governmental platform. Hacker groups targeted governmental official websites and conducted DDoS attacks. (Ebert and Groenendaal, 2020) Since the mechanism of DDoS attack is simply sending the exceeding number of requests to the host computer until its overload, this incident was not highly complex. However, the impact was more severe than it looked because the government did not have any experience or matured strategy against unexpected cyber incidents at that time.

In 2011, another DDoS attack occurred and was so-called the "Ten Days of Rain". The impact of this attack was much larger than the previous one because the target was not only governmental function but also financial, media, and US military facilities based in South Korea. (Ibid) Considering South Korea has a tight alliance with the US due to regional security engagement, it is understandable that the US facility could also be the target of cyber attacks. At the same time, we can also observe that North Korea wanted to demonstrate that they have a power to destabilize the regional order.

In 2013, South Korea experienced another cyber attack dubbed "Dark Seoul". This attack targeted broadcasting companies and major banks. Ebert and Groenendaal commented that the previous two incidents in 2009 and 2011 were DDoS attacks in this incident hackers sent emails containing malware to South Korean organizations and companies. In this circumstance, the device became infected through the email if the receiver opened it. (Ibid) In addition, Marpaung and Lee assessed that this incident could have been prevented if the organizations appropriately instructed employees to install antivirus softwares and conducted security training. (Marpaung and Lee, 2013)

Ebert and Groenendaal assessed attacks in this first phase as *"disruption and social disorder with DDoS attacks on media corporations and broadcasting"*(Ebert and Groenendaal, 2020, p.6) As they described, the initial stage of major incidents were mainly DDoS attacks, and the purpose was to destabilized South Korean society itself. North Korea also targeted the US military facility in "Ten Days of Rain" because they considered the external relations of South Korea could be damaged as well. Thus, we can also say cyber attacks in the first phase were aimed to show North Korea has the technical capability to violate South Korean society and its international relations.

The second phase was from late 2013 to 2017. In the first phase, the purpose of cyber attack was more like damaging society itself. In contrast, Ebert and Groenendaal pointed out cyber attacks in the second phase focused on breaching information that the South Korean government and its related private sector held, which included information related to military and strategic capabilities. (Ibid)

In 2013, hacker groups conducted multi-faced malware attacks which targeted the ministry of reunification, a private maritime company, and strategic expert institutes that research defense analysis. (Ibid) Compared to cyber incidents in the previous phase, it is observable that attackers used more complex and malicious methods.

In 2014, Korea Hydro and Nuclear power were attacked. As a result, 23 nuclear reactors were hacked and the personal information of more than 10,000 employees was leaked. (Ibid) From a technical point of view, Kim observed that attackers used more developed hacking skills compared to incidents in the previous phase. They sent emails with malicious code and stole information related to nuclear power from the central institution. (Kim, 2015) From these security incidents, we can see the purpose of cyber offense shifted from simply attacking governmental platforms to collecting highly valuable information.

The third phase started in 2017 and the target of cyber attacks was still a valuable asset but its tendency shifted from espionage to cyber thievery. Ebert and Groenendaal reported South Korean cryptocurrency exchange platform experienced cyber attacks two times in 2017 and the total loss was roughly 20.6 million US dollars. (Ebert and Groenendaal, 2020) At the same time, cyber-criminal groups started using highly complex and more insidious technology. In fact, Wagstaff and Smith reported the number of cyber attacks requests for money by utilizing ransomware such as WannaCry has been increased in recent years. (Wagstaff and Smith, 2017) Mohurle and Patil explain WannaCry is one of the most common ransomware that encrypts data on infected devices and then informs the user that their files have been locked. The screen of infected devices displays that attackers request money instead of restoring data and in these cases attackers instruct users to pay ransom in Bitcoin by a fixed date. (Mohurle and Patil, 2017)

Overall, the history of the cyber attack on the Korean peninsula illustrates two observations for regional security order. One is the initial purpose of cyber attacks was to assault the country itself. As these two countries had a certain level of antagonism since the 1950s, political conflict morphed into attacks in cyber space. The other is high economic development gives additional value to the information as an asset. As we have already reviewed in 2.2.1 of this thesis, information is not only about the collection of data but also has certain values. Therefore, the highly developed economy in South Korea can be valuable for external actors as well. In fact, cyber attacks are a means to earn funds such as bitcoin through ransomware. With these observation, we can conclude South Korea could not build up strong cyber strategy build on cyber resilience because they simply faced to too many threats and constantly got a large scale of cyber attack.

6.2 Nature of neighbors

The scale of neighbors' cyber threats is closely related to understanding the differences in cyber countermeasures of Estonia and South Korea. To assess cyber strategy, it is also necessary to analyze which countries these two states try to protect themselves from. This section will demonstrate the scale of cyber threats of Russia and North Korea as neighbors of the case study countries. Also, we will seek out how the nature of neighbors relates to the lack of cyber preparedness using analysis.

As a starting point, we need to remark that both Russia and North Korea are internationally recognized as having a high level of cyber attack capability. The European Commission remarked that these two countries are constantly listed as major states that regularly commit cyber offenses. (European Commission, 2017) The current global society severely critiques these states that attempted large scale hacking incidents across borders. Cerulus and Braun reported the EU imposed the first sanction against cyber attacks on Russia, China, and North Korea. These sanctions include asset freezes and travel bans for both individuals and organizations who are related to ransomware and industrial espionage. In detail, hacker groups belonging to the Russian military intelligence service so-called "Sandworm" conducted the "NotPetya attack" against Ukraine in 2017. This attack caused huge damage for major companies and its influence spread worldwide. That the same year, the ICT systems of the United Kingdom's National Health Service were attacked by ransomware, specifically WannaCry. The investigation teams confirmed that this incident is attempted by Lazarus, a famous North Korean hacker group. (Cerulus and Braun, 2020) Both attacks using NotPetya and WannaCry are extremely malicious and aggressive behavior. Thus, the EU reached the conclusion that these attacks threatened international security. These actions considered, it appears that Russia and North Korea have enough capability to destabilize the world order through cyber space.

6.2.1 Overview of worldwide cyber offense trend

To see the overview of global cyber offense capability, it is helpful to look at data from quantitative studies. CrowdStrike, the American cybersecurity company, conducted research that measures the scale of cyber threats in several states. In this research, CrowdStrike has a massive dataset that shows security breaches that ocurred in 176 countries during 2018. This data includes incidents in both governmental and commercial areas. To see the level of cyber capability in each state, the research team focused on the speed of hacking and used "breaktime" as an indicator to measure how fast each country conducts intrusions. According to their definition, breaktime is " *the speed with which adversaries accomplish lateral movement in the victim environment after their initial compromise*. "(CrowdStrike, 2019, p.14) The team investigated the breaktime of all incidents and calculated the average.

The result of the top four countries was as follows; *“1st) Russia 00:18:49, 2nd) North Korea 02:20:14, 3rd) China 04:00:26, and 4th) Iran 05:09:04”.* (CrowdStrike, 2019, p.14) Overall, the result obviously shows the world's top elite hackers are based in Russia as the breaktime is overwhelmingly faster than other nations. North Korean groups are also marked as high rank. Therefore, we can say these two countries are the top first and second cyber attackers in the world. However, we can also see a huge difference between first and second actors in the ranking. While Russian groups can reach the central system within 20 minutes on average, North Korean groups need more than 2 hours to do the same things. It is roughly said that the Russian cyber unit is 7 times faster than North Koreans.

As a conclusion of this section, we can suggest that Russia and North Korea have the highest level of hacking skills in the world. Consequently, neighboring states have to face highly sophisticated threats compared to other nations. Thus, it is natural that neighboring countries are required to build up a high level of suitable cyber security strategy. The next section will have a comprehensive look at Russian and North Korean cyber capabilities.

6.2.2 The cyber capability of Russia and North Korea

In this section, we will outline the cyber capabilities and draw attention to the differences between Russia and North Korea with two-axis; human resource and type of motivation.

As the analysis of CrowdStrike has mentioned previously, Russia is apparently the strongest cyber offense actor in the world. What gives Russia such a high position in the world ranking is a political factor, concerning two aspects; 1) varied in human resource, and 2) political heritage from Soviet times as motivation. As a general understanding of cyber units in Russia, Shakarian et al noted hackers can be organized in various forms such as individuals with governmental sponsors, and hacktivists. Hacktivists being a portmanteau of hackers and activists, therefore, indicating highly motivated hackers with political reasons. (Shakarian et al, 2016) Since hackers are from not only from militarily special units but are also civilians with government backing, we can say resources are one of the factors that contributed to improving cyber capability. On the other hand, we can also observe that Russian behavior in cyber space is inherited from the Soviet era. Giles assessed the principle of Russian practice in terms of cyber capability as the reinvigorated dimension of subversion campaigns from Soviet times. Thus, Russia paid attention to adapt this principle to the digital era. (Giles, 2015) From his observation, it is clear that the political element is a huge motivation that boosts increasing cyber-attack capability alongside the hard security military arena.

Using the two-axis that this section mentioned previously, we can also convey two findings regarding North Korea; 1) a large number of hackers who need external support and 2) financial gains as motivation. To show how large the capability of cyber attack by North Korea is, Avery et al, 2017 reported that the estimated number of hackers in North Korea is approximately 3,000 to 6000. (Avery et al, 2017) Even though North Korea hires a large number of cyber combats, it has a certain limitation in terms of improving their skills because North Korean network is not open to the world. Like section 2.2.3 outlined, information is perceived as threat for North Korea and consequently the government does not allow nationals to use the internet. Thus, hackers cannot learn and adopt new technology themselves. To solve this problem, Avery et al, also remarks that the North Korean government send a certain number of students to Russia and China under tight cooperative negotiation and they provide cyber training. (Ibid)

In the case of North Korea, economic reasons are the trigger, as opposed to the political aspect strengthening Russia's cyber-attack power. As broadly reported by major news media outlets, North Korea has been accused of behavior such as violating human rights, nuclear deployment, and series of espionage. As a result, international society imposed critical trade sanctions on the North Korean government. These economic sanctions are even more damaging, as North Korea was already depleted of industrial resources. Today, cyber crime is one of the means for North Korea to earn capital and bring numerous benefits to their society.

As a conclusion of this section, we can say these two countries have large-scale cyber units but North Korea is lacking sophisticated skills due to their administrative framework. The political perspective encourages Russian hackers, meanwhile economic reasons motivate cyber units to conduct more efficient and effective cyber offenses. These two findings explain why we can see a huge difference between Russia and North Korea in terms of cyber capability.

6.2.3 Analyze the type of threats based on the resilience framework

As section 3.2.3 of this research has already mentioned, it is essential to analyze the type of threats when we apply resilience to defense study. This model comes from hard resilience but still applicable even in cyber space as well. In the case of the nature of neighbors, we can define the type of threats with the classification that we figured out in section 3.2.3; 1) Security as prevention, 2) Security as control, and 3) Security as resilience. First, 1) Security as prevention is not applicable for these cases because the threat has already emerged. Besides, the root cause that prevention approach should have been working is still invisible because it is unpredictable if Russian or North Korean groups are trying to attempt cyber actions. Second, 2) Security as control is also not suitable because both Russia and North Korea are the world's top countries regarding cyber-attack capability as we saw at the beginning of this section. As they have huge power in cyber space, it is not a realistic idea that Estonia and South Korea try to control them. However, when we consider North Korean economic capacity is significantly poor meanwhile South Korea is highly developed in that sector, security as control is partially applicable. Third, 3) Security as resilience is the most appropriate approach for these cases by the process of elimination. As the definition of this approach has already stated, security as resilience is effective for threats that consisted of an enormous number of unseen factors. Moreover, the resilience approach is valid for security concerns that cannot be reduced by its impact. To sum up, the nature of neighbors clearly pointed out the type of threats. Since the threat level is overwhelming and not manageable, both cases need resilience. However, South Korean security strategy should also partially include security as control as well, based on economic capability. Consequently, it looks like South Korea is lagging cyber in resilience, but it does not necessarily mean they failed to build up an appropriate strategy.

6.3 Country's internal factors

This section addresses how the country's internal factors work as explanations for lagging cyber resilience. As we have already figured out in section 5.2.1, South Korea is particularly insufficient regarding "quick response and recovery", and "decision-making process". To see how internal dimensions of e-government lead to these deficiencies, we need to look at 1) inter-institutional cooperation and 2) emergency response regimes. First, inter-institutional cooperation in both the public and private sector enables appropriate actions for quick response and recovery. Second, the distribution of responsibilities in cyber defense is organized differently institutionally. These responsible regimes that work for emergent security breaches directly affect decision-making processes.

6.3.1 Estonian Case; inter-institutional cooperation for quick response and recovery

First, we will analyze inter-institutional cooperation. Scholars assessed that the Estonian e-government model achieved a high level of cooperation between the public and private sectors. Luht states that protecting critical systems is one of the most prioritized tasks in internal security. In this sense, the state government is not the only provider, but the private sector has also taken on a vital role to deliver the service for society. (Luht, 2020) To conduct quick response and recovery under the attack, the government clearly defined which area of service should be primarily protected. Luht also reported that the Estonian Emergency Act of 2009 is a comprehensive framework with a list of 43 essential services that should be prioritized. The list includes vital services for the society such as electricity and natural gas supply and public broadcasting. (Ibid) This act is a coherent approach because it leads to efficient and quick emergency response. Furthermore, it is also helpful for both public and private sectors to make sure the whole structure of the critical system. Based on this list, the public and private sectors cooperate to seek the most effective way to retain the essential infrastructure in emergency cases.

6.3.2 Estonian Case; emergency response regime for decision-making process

This section will look at the organizational framework of Estonian e-government regarding the distribution of responsibilities in cyber defense. Estonia has a centralized and clear organizational structure to make decisions quickly. Maaten gives an overview of each organization in terms of national cyber defense strategy in Estonia. First, the "Security Committee of the Government of the Republic" is the top institution above all necessary subunits. The role of this committee is to analyze and assess the national security situation. In addition, they also arrange the actions of the authorities regarding executive power into planning, developing, and assembling national safeguards. (Maaten, 2020) As this model indicates, it is essential that emergency response strategy ensures the position and task of top authorities in that regime. As a result, this structure enables a top-down decision-making process. In an emergency response such as the situation under the cyber attack, it is crucial that the state makes appropriate decisions as soon as possible. Therefore, the top-down structure of the Estonian model is assessed as well-structured based on cyber resilience.

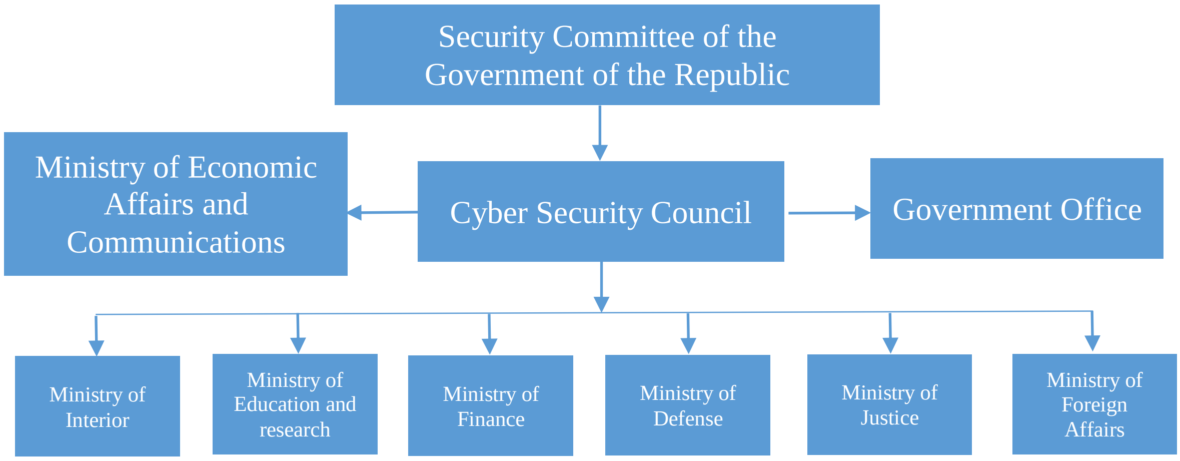

Security Committee of the Government of the Republic
Ministry of Economic Affairs and Communications
Cyber Security Council
Government Office
Ministry of Interior
Ministry of Education and research
Ministry of Finance
Ministry of Defense
Ministry of Justice
Ministry of Foreign Affairs

Chart 4: Institutional framework of e-government in Estonia

(Source from: Neeme, Maaten, and Rousku, 2020, p.31)

6.3.3 South Korean Case; inter-institutional cooperation for quick response and recovery

The coordination between public and private sectors against cybersecurity in South Korea is not strong enough because of its decentralized model. According to Lewis, South Korean e-government has three institutions that work for cooperation between public and private sectors. One is Korea Internet and Security Agency, generally called "KISA". This institution was founded in 1996 as the first step in the national cyber security arena. They are responsible for sharing threat awareness and related information with the private sector. Another organization is National Computer Emergency Response Team in Korea, so-called KrCERT. The role of the institution is based on the general terms of CERT, as mentioned in section 3.3.2, and they are directly controlled under KISA. They are in charge of coordination with the private sector in emergency situations. The final institution is The National Cybersecurity Center, namely NCSC. This is the joint organization of the military and private sectors. (Lewis, 2016)

The most obvious problem in the domestic cyber regime of South Korea is they have too many institutions established along the same line for cyber defense. While the Estonian model is simple and structured, the South Korean regime is scattered. In addition, Park pointed out the current problem in terms of institutional cooperation is how to unify its domestic national defense system in the cyber realm. (Park, 2016) To sum up, South Korean e-government needs to tighten cooperation between public and private but the current regime has too many institutions. As a result, missions of each institution look well-distributed, but it does not have coherence. Consequently, it leads to slow response, particularly in emergency situations where it takes more time to get a consensus between each institution to conduct necessary actions.

6.3.4 South Korean Case; emergency response regime for decision-making process

Same as inter-institutional cooperation, South Korean e-government has many different institutions that divide up decision-making responsibility. According to Ebert and Groenendaal, the South Korean e-government has three primary bodies; Presidential Office, the National security office, and the secretary to the president for national cyber security. These three institutions are the top authorities in order. A tech-specialized organization such as a national cyber security center is under those three institutions. (Ebert and Groenendaal, 2020) Compared to the Estonian model, it takes more time to get consensus within this hierarchal structured organization. Additionally, since the vertical structure makes it harder to get the necessary information from the bottom organizations, this model is not the best for the effective response.

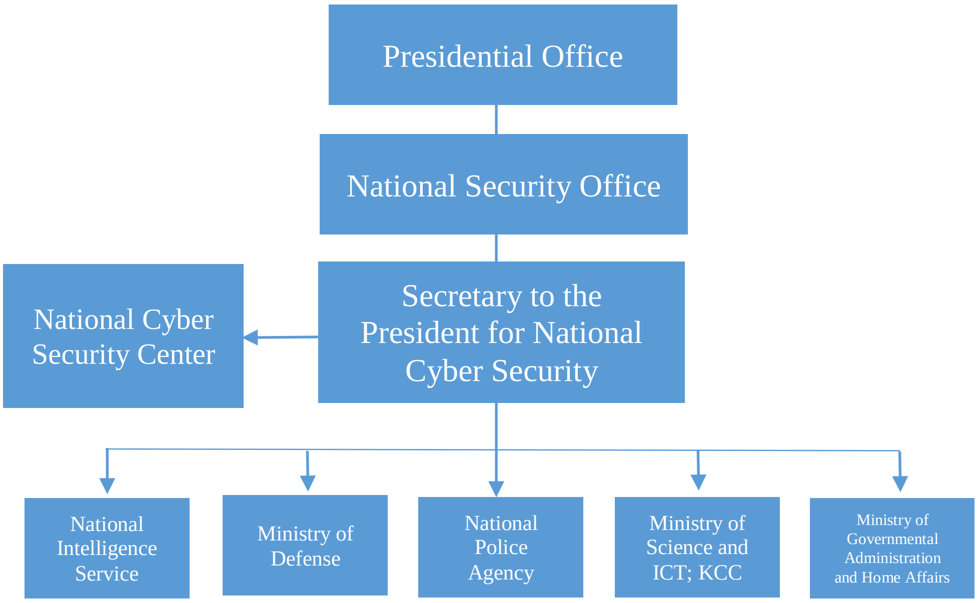

Presidential Office
National Security Office
Secretary to the President for National Cyber Security
National Cyber Security Center
National Intelligence Service
Ministry of Defense
National Police Agency
Ministry of Science and ICT; KCC
Ministry of Governmental Administration and Home Affairs

Chart 5 Institutional framework of e-government in South Korea

Source from: Ebert and Groenendaal, 2020 p.15

7. Conclusion

In this section, we will conclude this thesis by returning to the research question that has stated in the first chapter to give answers using analysis and findings previously conducted. The section will conclude with the final observation about comparing the e-government of Estonia and South Korea.

Research question;
What explains the differences in cyber response for advanced e-government states?

We have been evaluating some countries with advanced digitalization which are are paradoxically quite different in their cyber security development levels. Overall, we have seen the non-stop evolution of technologies, specifically in the e-governance domain throughout the whole digital age. This advancement provides overwhelming benefits to across various industries. Although many states attempt to improve their e-government and some of those countries achieved a high level of digital governance, it does not always mean they equal performance in the cyber security aspect. Even if some governments have a highly developed digital platform, we still see overwhelming differences in cyber defense. Accordingly, what we needed to look into was why technologically advanced countries have different responses in cyber defense.

To seek answers, this study had two steps to build up a theoretical framework. First, we look through concepts and theories of security in cyberspace in chapter 2. Basic understanding of these concepts and theories such as cyber security, information security, data security, digital sovereignty, and e-government study are basic components to set up cyber security approach. Second, chapter 3 constructed cyber resilience as a conceptual framework based on core elements of cyber studies found in the previous chapter. The concept of “resilience” comes from a broad range of social science research and often used in physical security studies. We can transpose principles, practices, and approaches from the hard security area to the cyber realm because digital space is essentially on the extended line of physical territory. Accordingly, we can see the same protocol in the artificial electronic field. Therefore, we can say cyber resilience is a combined concept of cyber peculiarities figured out in the previous chapter and resilience that comes from hard security study.

The theoretical framework indicated three expectations. First, geopolitical interstate tensions simply transpose to the cyber realm. Second, analyzing the type of threats demonstrates what approach state actors should take and in which cases. Third, the technical components of cyber resilience refer to what is lacking from cyber security preparedness of each country. Using these three expectations, we analyzed why each e-government is different in cyber security situation.

To see the difference in the security dimension of e-government, we picked up Estonia and South Korea as case studies by several applying several rationales. In order to analyze security aspect precisely, the empirical part used MSSD as a research design. Based on this design, we set up 1) high level of performance, 2) high standard of digitalization, 3) geopolitical concerns as similarity, and 4) the level of cyber security as difference. This structure simply focused on the difference and makes it more prominent.

Using the framework outlined in chapter 2 and 3, the empirical part illustrated three findings that explain why the South Korean e-government is lagging far behind the Estonian model in terms of the security aspect.

The first finding is the regional security situation is the trigger of cyber attacks. In addition, these root causes make it more difficult to build up cyber strategies. In the Estonian case, the trigger of cyber attacks was political and ethnical reasons. To be more precise, the support provided directly by the Russian state to Russian residents in Estonia directly impacts local ethnic identities and fosters cultural tensions. On the other hand, the initial root cause in the South Korean case was also a political perspective but the objective was gradually shifted to economic interest. Consequently, factors amount to the triggering of cyber attack increase its complexities. Since it is the more complex and mixed element, it makes setting up a cyber resilience strategy more difficult in South Korea.

The second finding is that the nature of neighbors affects the cyber resilience level because it shapes the different types of security threats. As we figured out in the second chapter, state actors take different security approaches depending on the type of threat. When we apply this framework to case studies, we found the nature of neighboring countries produces the difference. Undoubtedly these cases need a resilience approach as both cyber threats contain complex factors that are not manageable. To be more precise, both of their neighboring states have the largest scale of cyber attack capabilities in the world. However, South Korea partially includes security as control because its economic capacity is much larger than North Korea's. In this sense, it looks like South Korea is lacking cyber resilience but it does not necessarily mean they completely failed to set up a suitable strategy.

The third finding is that internal factors such as inter-institutional cooperation and emergency response regime disturbs quick and decisive actions against cyber threats. Like we outlined in the theoretical framework, quick response, recovery, and decision-making process are part of the essential components in cyber resilience. However, the South Korean e-government is overwhelmingly falling behind the Estonian system in these areas. Therefore, we can see that insufficient cooperation between domestic institutions and the inefficient organizational regimes had led to ineffective outcomes for the South Korean model.

With these three findings above, we explained why the South Korean e-government model is different from the Estonian case in terms of cyber security. In these cases, both external and internal factors significantly affect outcomes. On the other hand, this study picked up Estonian and South Korean case with specific criteria, but researchers might be able to discover a new element that causes differences if they pick up other country case studies. In the future, we can expect furthermore findings in e-government and cyber security.

Bibliography

Accenture. (2018). The Nature Of Effective Defense: Shifting from Cybersecurity to Cyber Resilience, https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/en/Accenture-Shifting-from-Cybersecurity-to-Cyber-Resilience-POV.pdf, Accessed on 16th May 2021

Avery, E.C., Rosen, L.Q., Rollins, J.W., and Theohary, C.A, (2017) North Korean Cyber Capabilities: In Brief, CRS Report Prepared for Members and Committees of Congress, Available from: https://fas.org/sgp/crs/row/R44912.pdf, Accessed on 16th May 2021

Biersteker, T.J. (2012). "State, Sovereignty, and Territory", *Handbook of International Relations pp.245-272*, SAGE Publications Ltd, Available from: https://sk.sagepub.com/reference/hdbk_interntlrelations, Accessed on 16th May 2021

Cerulus, L. and Braun,E. (2020). In a first, EU slaps sanctions on hackers in Russia, North Korea, China, Politico, Available from https://www.politico.eu/article/eu-slaps-sanctions-on-hackers-in-russia-north-korea-china/, Accessed on 3rd May 2021

Connelly, E.B., Allen, C.R., Hatfield, K. et al. (2017). "Features of resilience. Environ" *Syst Decis* 37, 46–50 (2017)., Available from: https://doi.org/10.1007/s10669-017-9634-9, Accessed on 16th May 2021

CrowdStrike, (2019), Global threat report Adversary Tradecraft and the importance of speed, Available from: https://www.africacybersecurityconference.com/document/CrowdStrike_GTR_2019.pdf , Accessed 15th Nov 2020

e-Estonia (n.d). e-governance, Available from: https://e-estonia.com/solutions/e-governance/, Accessed on 7th May 2021

Ebert, H. and Groenendaal, L. (2020). Cyber Resilience and Diplomacy in the Republic of Korea: Prospects for EU Cooperation, EU Cyber Direct, Available from:

https://eucyberdirect.eu/content_research/cyber-resilience-and-diplomacy-in-the-republic-of-korea/, Accessed on 16th May 2021

e-Governance Academy Foundation. (n.d a), National Cyber Security Index, Available from : https://ncsi.ega.ee/methodology/, Accessed on 9th May 2021

e-Governance Academy Foundation. (n.d b). National Cyber Security Index, 3. Estonia Available from : https://ncsi.ega.ee/country/ee/, Accessed on 9th May 2021

e-Governance Academy Foundation. (n.d c), National Cyber Security Index, Available from : https://ncsi.ega.ee/ncsi-index/ , Accessed on 9th May 2021

e-Governance Academy Foundation. (n.d d). National Cyber Security Index, 36. Korea (Republic of), Available from : https://ncsi.ega.ee/country/kr/, Accessed on 9th May 2021

Esser,F. and Vliegenthart, R. (2017). Comparative Research Methods, *The International Encyclopedia of Communication Research Methods*, JohnWiley&Sons,Inc., https://onlinelibrary.wiley.com/doi/epdf/10.1002/9781118901731.iecrm0035, Available from : 16th May 2021

European Commission. (2017). Building an Effective European Cyber Shield - Taking EU Cooperation to the Next Level, EPSC Strategic Notes Issue 24 8th May 2017, European Political Strategy Center, Available from: https://op.europa.eu/en/publication-detail/-/publication/bec56411-5ae4-11e7-954d-01aa75ed71a1, Accessed on 16th May 2021

Flint, C. (2016). Introduction to Geopolitics, 3rd edition, Routledge

Giles, K. (2015). “Russia's Toolkit”, *The Russian Challenge*, 40-49, Chatham House, London

Hassan,R.G., and Khalifa,O.O. (2016). “E-Government - an Information Security Perspective”, *International Journal of Emerging Trends & Technology in Computer Science* 36(1):1-9, Available from: https://www.researchgate.net/publication/307549055_E-Government_-_an_Information_Security_Perspective, Accessed on 16th May 2021

Helm, P. (2015). “Risk and resilience: strategies for security*”, Civil Engineering and Environmental Systems*, 32:1-2, 100-118, Available from: https://doi.org/10.1080/10286608.2015.1023793, Accessed on 16th May 2021

Hinsley, F.H. (1986) Sovereignty second edition, Cambridge University Press, Cambridge

Hitchens, T., and Goren, N. (2017). (Rep.). Center for International & Security Studies, U. Maryland. Retrieved May 15, 2021, from http://www.jstor.org/stable/resrep20426 https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index Accessed on 26th Jan 2021

International Telecommunication Union (2005). A Comparative Analysis of Cybersecurity Initiatives, WSIS Thematic Meeting on Cybersecurity 10 June 2005, http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_ Initiatives_Worldwide.pdf, Accessed on 16th May 2021

Iyobor,E.E., Kwadwo.G., and Asante, F.A. (2012). "Data Security Issues in Corporate Environment: A Case Study of Mining Companies in Ghana", *Journal of Digital Innovations & Contemporary Research. In Science and Engineering & Tech*, 5(2) 63-78, Available from: https://www.researchgate.net/publication/331833703_Data_Security_Issues_in_Corporate_Environment_A_Case_Study_of_Mining_Companies_in_Ghana, Accessed on 16th May 2021

James,A. (1987) Sovereign Statehood: The Basis of International Society, Allen & Unwin

Kello, L (2013). “The meaning of the cyber revolution: perils to theory and statecraft”, *International Security*, 38(2) 2013, 7-40, https://www.researchgate.net/publication/265959443_The_Meaning_of_the_Cyber_Revolution_Perils_to_Theory_and_Statecraft, Accessed on 16th May 2021

Kim, Y. (2015). KHNP hacking is attributed to North Korea, Available from: www.pressian.com/news/article.html?no=124755, Accessed on 16th May 2021

Kotka,T., Kask, L., Raudsepp, K., Storch, T., Radloff, R., and Liiv, I. (2016). “Policy and Legal Environment Analysis for e-Government Services Migration to the Public Cloud”, *ICEGOV '15-16: Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance*, 103–108, Available from: https://doi.org/10.1145/2910019.2910056, Accessed on 15th May 2021

Lawrence, M. (2013). Three approaches to security prevention, protection and resilience, Center for security governance, Center for security Governance, Available from: https://secgovcentre.org/2013/02/three-approaches-to-security-prevention-protection-and-resilience/ , Accessed on 15th May 2021

Lewis, J.A. (2016). Advanced Experiences in Cybersecurity Policies and Practices, Institutions for Development Sector Institutional Capacity of the State Division Discussion paper Nº IDB-DP-457, Inter-American Development Bank, Available from: https://publications.iadb.org/publications/english/document/Advanced-Experiences-in-Cybersecurity-Policies-and-Practices-An-Overview-of-Estonia-Israel-South-Korea-and-the-United-States.pdf, Accessed 15th Nov 2020

Lindsay, J.R. (2015). *“Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack*”, Journal of Cybersecurity, 1(1), September 2015, 53–67, Available from : https://doi.org/10.1093/cybsec/tyv003, Accessed on 15th May 2021

Lipton, E., Sanger, D. E, and Shane, S., The Perfect Weapon: How Russian Cyberpower Invaded the U.S., The New York Times online, 13 December 2016., Available from: https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html, Accessed on 16th May 2021

Looker (n.d) Data security, Available from : https://looker.com/definitions/data-security, Accessed on 13th May 2021

Luht (2020) “Critical infrastructure and cooperation with the private sector”, *National Cyber Security in Practice*, 35-41 , e-Governance Academy, Available from https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf, Accessed on 16th May 2021

Maaten, E. (2020) “How to develop a country’s cyber security? , Organisation of national cyber security”, *National Cyber Security in Practice*, 43-46 , e-Governance Academy, Available from: https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf, Accessed on 16th May 2021

Mattiisen, M. and Juurvee, I. (2020). The Bronze Soldier Crisis of 2007 Revisiting an early case of hybrid Conflict, International center for security and defense, Available from: https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf, Accessed on 16th May 2021

Marpaung, J.A.P. and Lee, H.J (2013). Dark Seoul Cyber Attack: Could it be worse?, CISAK 2013 – C1/O/8, Available from: https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/Dark_Seoul_Cyberattack.pdf, Accessed on 16th May 2021

Mohurle, S. and Patil, M. (2017) “A brief study of Wannacry Threat: Ransomware Attack 2017”, *International Journal of Advanced Research in Computer Science,* 8(5), May-June 2017, Available from: https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf, Accessed on 29th Apr

Morgenthau, H.J. (1960) Politics Among Nations: The Struggle for Power and Peace second edition, New York: Knopf

Moyle,E. (2021). CERT vs. CSIRT vs. SOC: What's the difference?, Search Security, TechTarget, Available from : https://searchsecurity.techtarget.com/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference, Accessed on 7th May 2021

National Research Council (2012) Disaster Resilience: A National Imperative, Washington, DC: The National Academies Press. Available from: https://doi.org/10.17226/13457., Accessed on 16th May 2021

NATO (n.d). What is NATO? Pick a topic and discover NATO, Available from :https://www.nato.int/nato-welcome/index.html, Accessed on 8th May 2021

NATO Strategic Communications Centre of Excellence (2019). Hybrid Threats: 2007 cyber attacks on Estonia(2019) in Aday S., Andžāns M., Bērziņa-Čerenkova U., Granelli F., Gravelines J., Hills M., Holmstrom M., Klus A., Martinez-Sanchez I., Mattiisen M., Molder H., Morakabati Y., Pamment J., Sari A., Sazonov V., Simons G., Terra J. (2019). Hybrid Threats. A Strategic Communications Perspective. Riga: NATO Strategic Communications Centre of Excellence, Available from: https://www.stratcomcoe.org/hybrid-threats-2007-cyber-attacks-estonia, Accessed on 16th May 2021

Neeme,E., Maaten,E., and Rousku, K. (2020) “Organisation of national cyber security”, *National Cyber Security in Practice*, 20-34 , e-Governance Academy, Available from https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf, Accessed on 16th May 2021

OECD (n.d a). Risk and Resilience, Available from: https://www.oecd.org/dac/conflict-fragility-resilience/risk-resilience/, Accessed on 27th April 2021

OECD (n.d b). Resilient Cities, Available from : https://www.oecd.org/cfe/regionaldevelopment/resilient-cities.htm, Accessed in 27th April 2021

OECD. (2016). Strengthening Economic. Resilience: Insights from the Post-1970 Record of Severe. Recessions and Financial Crises, OECD Economic Policy December 2016 No. 20, Available from: https://www.oecd.org/economy/growth/Strengthening-economic-resilience-insights-from-the-post-1970-record-of-severe-recessions-and-financial-crises-policy-paper-december-2016.pdf, Accessed on 16th May 2021

Park, J., Rowe, N. and Cisneros, M. (2016). South Korea's Options in Responding to North Korean Cyberattacks, Journal of Information Warfare 15(4) (Fall 2016), Peregrine Technical Solutions, 86-99, Available from: https://www.jstor.org/stable/26487553, Accessed on 16th May 2021

Park.D, (2016) Cybersecurity Spotlight: South Korea, East Asia Center, University of Washington, Available from https://jsis.washington.edu/eacenter/2016/01/12/cybersecurity-spotlight-south-korea/, Accessed on 6th May 2021

Republic of Estonia Ministry of Economic Affairs and Communications (2020). Cyber Security, Available from https://www.mkm.ee/en/objectives-activities/cyber-security, Accessed on 9th April 2021

Sandhu,R.S. and Samarati, P. (1994). “Access Control: Principles and Practice”, *IEEE Communications Magazine*, 32(9), Sept. 1994, IEEE, 40-48, Available from : https://ieeexplore.ieee.org/document/312842, Accessed on 16th May 2021

SCO (n.d) The Shanghai Cooperation Organisation, Available from: http://eng.sectsco.org/about_sco/, Accessed on 16th May 2021

Shakarian,P., Shakarian,J. and Ruef,.A (2016) Introduction to Cyber-Warfare: A Multidisciplinary Approach, Newnes, May 16, 2013 - Computers

Shea,J. (2016). Resilience: a core element of collective defence ,NATO review 30 March 2016, Available: https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html, Accessed on 27th April 2021

Statics Estonia (2020). Population by ethnic nationality. 1 January, years, Available from https://vana.stat.ee/34278, Accessed on 2nd May 2021

Steinmetz, J. (2021). Politics, Power, and Purpose: An Orientation to Political Science, Fort Hays State University, Available from : https://fhsu.pressbooks.pub/orientationpolisci/, Accessed on 16th May 2021

Stinson.D.R and Paterson.M (2018). Cryptography: Theory and Practice, CRC Press

Solms, R.V. and Niekerk, J.V. (2013) “From information security to cyber security”, *Computers & Security* 38, October 2013, 97-102, Available from: https://doi.org/10.1016/j.cose.2013.04.004, Accessed on 16th April 2021

The World Bank (2016 a) World Development Report 2016: Digital Dividends, Available from : https://www.worldbank.org/en/publication/wdr2016, Accessed on 16th May 2021

The World Bank (2016 b) Digital Adoption Index, Available from: https://www.worldbank.org/en/publication/wdr2016/Digital-Adoption-Index, Accessed on 16th May 2021

United Nations (2011). Developments in the Field of Information and Telecommunications in the Context of International Security, Disarmament Study Series: No. 33, Available from: https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf, Accessed 5th Mar 2021

United Nations (2020). E-Government Survey 2020, Department of Economic and Social Affairs, United Nations, Available from https://www.un.org/development/desa/publications/publication/2020-united-nations-e-government-survey , Accessed 15th Nov 2020

United Nations (2021 a). E-government, UN E-Government Knowledgebase, Available from. https://publicadministration.un.org/egovkb/en-us/About/UNeGovDD-Framework, Accessed on 26th Jan 2021

United Nations (2021 b). E-Government Development Index (EGDI), Available from https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index, Accessed on 16th May 2021

Wagstaff, K., Eng, J. and DeLuca, M. (2015). OPM: 21.5 million people affected by background Check Breach, Available from: https://www.nbcnews.com/tech/security/opm-hack-security-breach-n389476, Accessed on 29th Jan, 2021

Wagstaff,J. and Smith,J.,(2017). Multi-stage cyber attacks net North Korea millions in virtual currencies: researchers, DECEMBER 19, 2017 12:06, Available from https://www.reuters.com/article/us-southkorea-cyber-hackers-idUSKBN1ED0ZC, Accessed on 16th May 2021

Wara,Y.M and Singh, D. (2015). “A Guide to Establishing Computer Security Incident Response Team (CSIRT) For National Research and Education Network (NREN).”, *African Journal of Computing & ICT*, 8(2) June 2015, Available from : https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.697.1009&rep=rep1&type=pdf, Accessed on 16th May 2021

Warkentina,P.M and Orgeron,C (2020). “Using the security triad to assess blockchain technology in public sector applications”, *International Journal of Information Management* 52, June 2020, 102090, Available from : https://www.sciencedirect.com/science/article/pii/S026840121930060X, Accessed on 16th May 2021

Zebrowski, C. (2013). “The nature of resilience”, *Resilience International Policies, Practices and Discourses* 1(3), Available from: https://doi.org/10.1080/21693293.2013.804672, Accessed on 16th May 2021

Zhao, J.J and Zhao, S.Y. (2010). “Opportunities and threats: A security assessment of state e-government websites”, *Government Information Quarterly*, 27(1), January 2010, 49-56, Available from : https://www.researchgate.net/publication/240435472_Opportunities_and_threats_A_security_assessment_of_state_e-government_websites, Accessed on 15th May 2021