The Diagnosis and Prescription for Cybersecurity in Korea: Focusing on Policy and System

Sangdon Park[1], Il Hwan Kim[2], Jaehyoun Kim[3] and Kyung Lyul Lee[2]
[1] Base Technology Division, National Security Research Institute
P.O.Box 1, Yuseong, Daejeon, South Korea
[e-mail: sdpark@nsr.re.kr]
[2]School of Law, Sungkyunkwan University
[3]Department of Computer Education, Sungkyunkwan University
25-2 Sungkyunkwan-ro, Jongno-gu, Seoul, South Korea
[e-mail: {ilhwan, klee04, jaekim}@skku.edu]
*Corresponding author: Kyung Lyul Lee

Received September 27, 2017; accepted January 1, 2018; published February 28, 2018

Abstract

Cybersecurity has emerged as a serious problem in Korea and there have been relevant movements to improve domestic cybersecurity policy and system. However, discussions have yet to result in actual progress and the legislation for improvement of cybersecurity policy and system have been stagnant until now. As evidenced by the introduction of primary government legislation bill for national cybersecurity in 2017, the preparations for improvements to the policy and system are still in progress. However, we cannot be positive about the possibility of implementing these improvements during the process. Recognition of the importance of cybersecutiry has gradually risen and is more prevalent than in years past, however, in-depth discussions are not being made. In principle, misunderstandings about cybersecurity itself and insufficient understandings of the relevant legislation seem to cause such problems. Therefore, it is necessary to review key issues related to the improvement of cybersecurity policy and system and reconsider tasks for the future. Such issues include the relationship between cybersecurity and fundamental rights, establishing responsibility and capability of each of entities for cybersecurity, and the role of the military in cybersecurity. This type of in-depth discussion will be helpful for finding ways to improve upon cybersecurity policy and system. Moreover, this study aims to key issues with questionnaire survey and political and normative inquiry.

Keywords: Cybersecurity governance, information security, cyber war, cyber warfare, cybersecurity law

A preliminary version of this paper was presented at APIC-IST 2017, and was selected as an outstanding paper.

http://doi.org/10.3837/tiis.2018.02.018 **ISSN : 1976-7277**

1. Introduction

The improvement in information technology has changed modern life. Rapidity of such improvement and the consequent changes of social environments has demanded a new paradigm in the domain of laws. Failure of laws to adapt to such changes will result in massive social disorder. Therefore, it is urgently needed to prevent such failure [1]. Cybersecurity has been considered as the key to this problem. It is necessary to establish and promote policies to reinforce the cybersecurity system continuously and simultaneously maintain the safe and sound information-oriented society. Furthermore, the legislation also has to be ameliorated in order to provide sufficient institutional support [2].

Consensus on how cybersecurity legislation can be improved has already been established in Korea. The measures of the improvement of cybersecurity legislation presented in the previous studies vary a little among themselves. Still, all argue for the necessity of overall improvement [3]. The actual improvement in legislation, however, has been stagnant in Korea. Legislative bills for improving the quality of cybersecurity promotion system have been repeatedly proposed but abrogated. This is largely due to the fact that the compromise has never been reached within the 10-year period of each legislative session. Considering the importance of the matter, it cannot be ignored anymore. The time to make a conclusion on the improvement of legislation is drawing near.

This study is to determine why the improvement of cybersercurity policy and system in Korea keeps being stagnated and present several topics requiring the review with relevant opinions. A questionnaire survey was designed to ascertain opinion about some topics of cybersecurity policy and system. 72 people of three groups responded to the survey. One group consists of experts on national security policy and engineering (group A). Another is a group of experts on criminology (group B). The other is a group of police trainees (group C). This study combines survey analysis with political and normative opinion.

2. Discussion status and problems in the improvement of cybersecurity policy and system

2.1 Importance of cybersecurity

Information and communication play various roles due to the expansion and generalization of information and communication infrastructure in today's world. The function of information and communication can be largely classified into 7 functions. The first function is to improve safety and maintenance of order. Information and communication play an important function to protect the safety of society and prevent the occurrence of a disaster today. The second function is to develop knowledge and information. Due to the development of information and communication, a large amount of meaningless information owned by either individuals, organizations, or the state was converted into meaningful intelligence through a knowledge creation and distribution process. The third function is to increase the business efficiency of government institutions. Administrative information databases have been established and utilized to facilitate joint usage of information between government institutions. In addition, the electronic administration to utilize information and communication for public service including various civil affairs administrations is being introduced. The fourth function is to innovate economic activities. Information and communication are more frequently utilized in

economic activities today. Therefore, information and communication promote the development of various industries and contribute to economic development. The fifth function is to expand human relations. Information and communication provide communication technologies that can satisfy people's desire of interpersonal communication. This in turn facilitates the establishment of human relation through communication beyond space and time. The sixth function is to restore and develop the public sphere. Due to the development of information and communication infrastructure, the whole size and area of the public sphere has expanded farther than in the past. Furthermore, the freedom of expression and opinions via Internet platforms has spread to the whole world. The seventh function is to expand culture and education. Since a gap of time and space has been filled up by information and communication, efforts to create cultural exchanges that freely distribute culture to the whole world have been revitalized. In this light, we have seen improvements in learning efficiency and the effects of education [4].

Information plays some key roles in today's world. One of information' most important role is that it connects the entire world into one information-oriented society—a cyberspace, in which information affects the components of both virtual and real worlds. All countries in the world have subsequently come to rely onto one another through interaction allowed by the Internet and other means. As a result, one cyber-attack does not injure just one country or area, but the entire global community. The Internet itself has been used as a threat to the public information and communication infrastructure. Therefore, we cannot rule out the possibility that such damage may occur all over the world [4]. The need of protecting the cyberspace as well as the real world—land, sea and air—is now greater than ever. The infrastructure, under the emergence of e-government, is especially fragile against cyber-attacks due to its complete dependence on information technology. One cyber attack may result a critical threat to the national economy and the state management, of which the injury can damage all the other parts of the system [2]. The legal concept of national security must include the means to protect the functionality of e-government from a cyber threat from the outside [5].

2.2 Problems in the current cybersecurity policy and system

The surroundings of South Korea are not favorable to cyber security. Korea is located near both China and Russia, which are expected to be the major source of cyberattacks around the world. North Korea also possesses a threat due to its historically complicated relationship with the South. Cyberattacks against the national security occur frequently [6]. It is urgently needed to set up a sound security plan against cyberattacks and prepare for coming attacks. Legislative moves are the most important in establishing greater cybersecurity.

The legal action for cybersecurity began in the 2000s. The National Cyber Security Management Regulation was launched in 2005 for the unique purpose of handling the safety of cyberspace. However, it was merely a presidential directive which could be applied only to the public sector.

The existing cybersecurity-related lack completeness as a whole. Various divisions have their own scope and promotion in regards to cybersecurity. For example, the National Cyber Security Management Regulation has been applied to only the public sector. This had been as a major problem as its range of effects is severely limited. A presidential directive can affect only on internal administrative institutions while an act, a consequent enforcement decree and an enforcement rule have effects on the general public [3].

Therefore, it is necessary to properly draft the legislation in regards to cybersecurity. The new act has to account for all cybersecurity-related matters in both private and public domains. Basic principles shall be included in order to ensure its effectiveness [7].

There have been a number of attempts to enact a law in order to build a cybersecurity operation system and deal with a threat of national security that can affect both public and private sectors. A legislative bill for the prevention of future cyber crisis was proposed in the 17th National Assembly and a legislative bill on national cyber crisis management was proposed in the 19th National Assembly. Both legislative bills, however, were abrogated without even passing through the National Assembly Standing Committee. This was due to the fact they were proposed near the end of their respective sessions. A legislative bill on the prevention of national cyber terror, a legislative bill on the management of national cyber safety, a legislative bill on the prevention and response to cyber terror and a legislative bill on sharing of cyber threat information were all proposed in the 19th National Assembly but were also abrogated due to the same reason.

The press stated that, as of 2016, preparations for primary legislation for national cybersecurity have begun. Such legislative bills will incorporate proposals to solve problems indicated from the previous legislative bills, including management of cyber threat information. However, many have questioned why the Office for Government Coordination rather than an intelligence agency would handle information. As the argument is yet to end, there is still not much hope in the possibility of implementing the much needed legislation.

2.3 History of the cybersecurity legislation

The promotion system under the previous versions of legal system did not sufficiently secure the safety of either cyber space or national security. Therefore, there was a movement to establish an act including the contents to build a cybersecurity operation system to deal with a threat of national security to both the public and private sectors. Several cybersecurity bills were proposed in the National Assembly of Korea. Most of legislative bills were abrogated due to session culminating except Information Protection Industry Promotion Act, which was a measure that secured the revitalization of relevant industry's institutions. In the 20th National Assembly, as of 2017, new bills for national cybersecurity are introduced. At this stage it is known that such legislative bills incorporate proposals to solve problems indicated from the previous legislative bills. That being said, there is still little to be hopeful for in regards to the possibility of implementing much needed pieces of legislation. The lists of cybersecurity bills are shown in **Table 1**.

Table 1. Cybersecurity bills in the National Assembly of Korea

Session	Title	Last Action
17th	Act on Prevention and Responses to Cyber Crisis	disposed
18th	National Cyber Crisis Management Act	disposed
19th	Act on National Prevention of Cyberterror	disposed
	Act on National Cybersecurity Management	
	Act on Prevention and Responses to Cyberterror	
	Act on Cyber Threat Intelligence Sharing	
	Act on Information Protection Industry Promotion	Passed
20th	Act on National Cybersecurity	introduced
	National Cybersecurity Act	

2.4 Necessity of in-depth discussion on the of cybersecurity legislation in Korea

There are a myriad of causes for past stagnant rates of legislation for improvement of cybersecurity in Korea. First, the legislative body, the National Assembly, at the time could not yet recognize the importance of cybersecurity. There has been a gradually growing interest in cybersecurity due to a series of information leak accidents, yet despite this, the legislative body did not consider the matter to be of particular importance . This can be inferred from the fact that most cybersecurity-related legislative bills proposed until now have not even been properly reviewed by the National Assembly Standing Committee. Second, there have been no efforts as of yet to reconcile the differences in positions held by the different legislative bills. Since there has not been enough discussion due to the lack of recognition on the importance mentioned earlier, the basis for reaching an agreement has not yet been established [3]. The survey result shows the lack of sufficient discussion. Only one bill is known to the majority of all groups. The survey result on recognition of cybersecurity-related bills is shown in **Table 2.**

Table 2. Recognition of cybersecurity-related bills

Question: Which bills have you heard of?(multiple answers)			
Class	**Group A**	**Group B**	**Group C**
Act on Prevention and Responses to Cyber Crisis	28.6%	0.9%	11.1%
National Cyber Crisis Management Act	57.1%	0.9%	0.0%
Act on National Prevention of Cyberterror	57.1%	36.4%	29.6%
Act on National Cybersecurity Management	28.6%	0. 0%	3.7%
Act on Prevention and Responses to Cyberterror	71.4%	54.5%	33.3%
Act on Cyber Threat Intelligence Sharing	57.1%	0.0%	0.0%
Act on Information Protection Industry Promotion	71.4%	81.8%	59.3%
Act on National Cybersecurity	28.6%	0.9%	1.9%
National Cybersecurity Act	85.7%	0.9%	0.0%

Recently, recognition of cybersecurity's importance seems to have spread gradually in comparison with in the past. 100% of the group A, 81.8% of the group B and 88.9% of the group C agree that there are threats from cybersecurity incidents. The survey result on the Presence of threats from cybersecurity incidents is shown in **Table 3**. Group A and Group B think that control system is the most critical target of cyber attack. But Group C thinks that the most critical target is personal information. The survey result on the most critical target of cyber attack is shown in **Table 4**.

Table 3. Presence of threats from cybersecurity incidents

Question: Are there threats from cybersecurity incidents?			
Class	**Group A**	**Group B**	**Group C**
Strongly agree	42.9%	36.4%	35.2%
Agree	57.1%	45.5%	53.7%
Neutral	0.0%	9.1%	11.1%
Disagree	0.0%	9.1%	0.0%
Strongly disagree	0.0%	0.0%	0.0%

Table 4. The most critical target of cyber attack

Question: What is the most critical target of cyber attack?			
Class	**Group A**	**Group B**	**Group C**
Personal information	0.0%	18.2%	61.5%
Public data	14.3%	9.1%	9.6%
Information network	0.0%	27.3%	1.9%
Infrastructure control system	85.7%	45.5%	26.9%
The others	0.0%	0.0%	0.0%

However, in-depth discussions are still not being made. Both sides supporting and opposing the prospects of improving the current legislation in the political arena do not actually discuss points they think new cybersecurity legislation should actually cover. This situation does not help the actual development of cybersecurity at all. Meanwhile, in addition to occoassional misunderstandings, the configuration of roles within government ministries and organizations regarding cybersecurity is complex and sluggish. Due to such circumstances, the discussions on cybersecurity were made only superficially without conclusion, thus, discussions for improving cybersecurity policy and system became stagnant. A serious academic reflection on topics related to the eventual improvement of cybersecurity policy and system is required for the purpose of overcoming this exact situation. Further, the results of such reflection and discussion should be reflected in the legislative activity.

There are various subjects for discussion as stated above. However, such subjects can be classified into two main categories. The first of which is a problem regarding how the rights of the people should be protected under cybersecurity. Especially, we must consider a way to establish an act without damaging any fundamental right which are of constitutional value. The second category deals with issues regarding how to establish a mandate that ensures the governing bodies will carry out activities required for cybersecurity. These categorical issues can be considered from two viewpoints. One viewpoint is related to the establishment of responsibility and capability of each of entities. The other viewpoint relates to the confirmation of the military's role in cybersecurity. It is necessary to review each issues separately and find political and legislative tasks according to the review result.

3. The relationship between cybersecurity and fundamental rights

3.1 The protection and restriction of fundamental rights in general

People have fundamental basic rights that are guaranteed by the constitution. The fundamental rights are the main value of the constitution and the establishment and maintenance of constitutional law are systematized based on the fundamental right. The fundamental rights

derive its significance as an active value containing the demand to be protected specially as the right dictates [4]. Therefore, the fundamental rights should be protected as much as possible in principle. Nevertheless, the fundamental rights may be restricted according to unavoidable circumstances. The fundamental rights may be permitted to be restricted by the constitution directly or restricted based on the act. And, it should have a proper purpose and an appropriate measure according to the Principle of Proportion and its legal grounds should be clear and specific.

3.2 Distinction between fundamental rights related to cybersecurity and other fundamental rights

Some concerns of infringement on fundamental rights have also been raised when discussing the processes involved with cybersecurity. Fundamental rights are of principal values of the Constitution, and they can only be limited by law in the need for national security, maintaining orders and public interests. It is true that, while devising legislation related to cybersecurity, ways to prevent possible violation of fundamental rights must also be considered.However, there is also a concern regarding some fundamental rights that are irrelevant to cybersecurity. A typical example is the concern for freedom of expression through the Internet. Some non-governmental organizations even argue that cybersecurity legislation may violate the freedom of expression [8]. However, this is an opinion based on a misunderstanding. Cybersecurity should be focused on attacks by electronic means. Exercising the freedom of expression by publishing articles or posting things on the Internet is largely irrelevant to cybersecurity. It is necessary to correct and reconcile these misunderstandings and establish the relationship between cybersecurity and fundamental rights by relying onto facts. Irrelevant arguments prevent actually needed discussions, and result in losing an opportunity to reflect on the effective means to protect fundamental rights.

3.3 Cybersecurity and protection of personal information

The protection of cybersecurity is significant in that the safety of the people depends on major functions of the state, of which numerous require protection of several pieces of personal information. Cybersecurity has to be in harmony with the objectives of the constitution and cause no conflict with the protection of the fundamental rights of the people [9]. Cybersecurity can secure personal information and prevent its abuse or forgery. Therefore, cybersecurity has the potential to contribute to the protection of personal information [2]. The Protection of personal information is very important as a matter of cybersecurity in Korea. The most call for counsel is personal information relevant to cybersecurity in Korea, and the majority of group C says that the most critical target is personal information as shown in **Table 4.** The number of counsel on internet by Korea Internet & Security Agency(KISA) are shown in **Table 5**.

Table 5. Number of counsel on internet by KISA [10]

Class	2014Y	2015Y	2016Y
Personal information	155,908	149,835	96,651
Spam	134,297	117,704	81,631
Cracking or virus	153,046	122,475	67,779
Domain or IP	2,519	2,367	1,895
Others(irrelevant to security)	187,990	161,283	136,355
Total number	633,760	553,664	384,311

Meanwhile, some argue that, within the context of practical options, big data is the most effective form of regulation. Big data can be used to search, detect and block attacks directly or indirectly. It has thus been selected as the main implementing tool for cybersecurity. Yet the use of big data in this fashion needs personal information to be utilized as target data for management, searches and detection. Therefore, some argue that cybersecurity can infringe on personal information, while contributing to the protection of personal information at the same time [9].

3.4 Cybersecurity and the right to safety

The concept of the right to safety is has been legitimized and included as a fundamental right rather recently. The right to safety has been linked to the problems of the 'risk society', which is addressed at a later section in this paper. The right to safety must be accepted as a fundamental right, and the legislative obligation for realizing the right to safety can be granted therefore. If the right to safety is considered not a constitutional fundamental right but merely a legal right, the right to safety will arise only under a legislator's subjective discretion [11]. In this viewpoint, cybersecurity must actively protect the right to safety. Means to ensure security—including cybersecurity—serve to protect us from risks of infringements on fundamental rights, and make us feel safe by bringing stability to society.

3.5 Political and Legislative tasks for the future

Both freedom and safety are values respected by the constitution and the harmonious realization of both values together is one of the most important tasks for a legislator [11]. Therefore, it is important to protect and realize fundamental rights in the process of improving cybersecurity policy and system. However, it is necessary to keep two facts in mind.

First, a justifiable limitation for purposes of national security may arise. The limitation of fundamental rights may be justified if it satisfies constitutional standards. The survet result show that many people agree with this. 85.7% of the group A and 53.7% of the group C agree that it is possible to restrict fundamental rights for cybersecurity if necessary, and 36.4% of group B, meanwhile, take a neutral attitude and same number of group B disagree that. Except group B, the majority of respondents agree to resrict fundamental rights for cybersecurity. The survey result on limitation to fundamental right for cybersecurity is shown in **Table 6**.

Table 6. Limitation to fundamental right for cybersecurity

Question: Is it possible to restrict fundamental rights for cybersecurity if necessary?			
Class	**Group A**	**Group B**	**Group C**
Strongly agree	28.6%	9.1%	9.3%
Agree	57.1%	18.2%	44.4%
Neutral	14.3%	36.4%	25.9%
Disagree	0.0%	36.4%	20.4%
Strongly disagree	0.0%	0.0%	0.0%

Second, fundamental rights can be both limited and protected by cybersecurity. There are various fundamental rights related to cybersecurity, and it is necessary to also consider the target fundamental rights for protection in addition to the target fundamental rights for limitation. The goal for all of these discussions is to identify the type and category of relevant fundamental rights precisely. A discussion on irrelevant fundamental rights only produces

meaningless arguments and prevents actually necessary discussions so that we may miss an opportunity to reflect the protective device for required fundamental rights to the acts properly.

4. Establishing responsibility and capability of each of entities for cybersecurity

4.1 Feature of cybersecurity threats in modern risk society

Cyberspace is an electronic medium through which information is created, transmitted, received, stored, processed and deleted [12]. This is a new concept that appeared while the informatization movement along with the evolution of particular technologies were in their early stages of development. When one looks at the threats that occur in cyberspace, we can see several major characteristics. First, there is immediate damage in the target computer network when the attack begins. Second, a single cyber attack has the potential to damage numerous targets. Third, it is very difficult to clearly identify the attacker for such a cyber attack [13]. These characteristics can be considered as risks that are inevitably accompanied along with the development of today's modern information society. Since the social risks associated with modern society gained added attention when the concept of the 'risk society' was presented. It should be noted that the concept of risk society today is generally accepted in various fields of study. The characteristics of risk elements shown in the risk society are as follows. First, it is difficult to predict occurrences of risk. Even if such occurences can be predicted, it is not easy to figure out when, where and how they would occur. Second, when a risk actually occurs, it is difficult to control. Similarly, even if it could be controlled, a fatal risk has already occurred at the time of risk occurrence, so stability becomes difficult to rescue or restore. Third, the damage occurred is extensive, the results can also be fatal, and victims are distributed extensively over the area. Fourth, it is unclear to clarify who is responsible for the risk or what caused the the onset of the risk in the first place. Fifth, those who are most at risk are predominantly organizations or corporations rather than individuals. A new risk which appears in the current information society also falls under the problem of risk society. The phenomenon, according to the utilization of information and communication (such as the expansion of cyberspace), becomes a risk factor. This in turn characterizes the modern society into that of a risk society [14].

4.2 Necessity to promote the cybersecurity activities of each entity

Risk can be classified into 4 types including social sharing high risk, social sharing low risk, non-social sharing high risk, and non-social sharing low risk. These classifications can be viewed through differing variables. These include the sharing of information and the associated risks in terms of social impact and the risk of damage as exemplified by the risk society. A cyber crime has a severe level of risk for social damage. This type of indiscriminate social exposure is so drastic that it falls under the category of a social sharing risk. Facing social sharing high risks suggests a significant infringement of public nature regarding safety and the risk-consideration efforts of community members. Cybersecurity is required in order not to face such risky situations [15]. A threat to cybersecurity is also a risk related to information and communication so it has the essentially same nature of risk with a cyber crime. Therefore, cybersecurity activity falls under social sharing high risk type and, accordingly, all members of the social community should recognize and solve this problem.

4.3 Problems of sectoral separation and lack of autonomy in cybersecurity

The cybersecurity promotion system according to current acts in Korea was formed by some government actors in each sector. These parties undertook responsibility for the formation as well as implementation. This is a typical classification between the private sector, public sector and military. The IT authority for the private sector, the security authority for the public sector and the administrative authority in national defense for the military take full charge of responding. In particular, national security responses are actually limited to those within the public sector. As of 2017, authorities in cybersecurity promotion system are shown in **Table 7**.

Table 7. Competent authorities for cybersecurity in each sector in Korea

Sector	Authority
Private	Ministry of Science, ICT and Future Planning
Public	National Intelligence Service
Military	Ministry of National Defense

It is time to require the consideration of whether such a cybersecurity promotion system is appropriate or not. 100% of the group A, 72.8% of the group B and 85.2% of group C think that role of private sector is necessary in cybersecurity. The survey result on necessity of role of private sector in cybersecurity is shown in **Table 8**. So it is reasonable to assume that cybersecurity promotion system needs reformation. The vast majority of all groups think that new system with cross-sector cooperation is more effective than present system that separates sectors in cybersecurity. The survey result on effective system in cybersecurity is shown in **Table 9**.

Table 8. Necessity of the role of private sector in cybersecurity

Question: How much the role of private sector is required in cybersecurity?			
Class	**Group A**	**Group B**	**Group C**
Very necessary	71.4%	27.3%	38.9%
Necessary	28.6%	45.5%	46.3%
Neutral	0.0%	18.2%	13.0%
Unnecessary	0.0%	9.1%	1.9%
Very unnecessary	0.0%	0.0%	0.0%

Table 9. Effective system in cybersecurity

Question: Which System is effective in cybersecurity?			
Class	**Group A**	**Group B**	**Group C**
Present system with separated sector	14.3%	9.1%	16.7%
New system with cross-sector cooperation	85.7%	90.9%	83.3%

The fact that a small number of government organizations take full charge of the role means transferring many responsibilities, and this can also be considered as a shifting of responsibilities in some sense. This increases the burden of ministries and organizations in charge of each field. This method was appropriate at the time when information and communication and cyber space were considered special and used only in a part of the society. However, information and communication have become commonplace. The basis for performing all tasks in cyberspace is being utilized, so users should take it upon themselves to

maintain their safety. Especially, the current cybersecurity promotion system is not appropriate from the viewpoint that it is advisable for each entity to consider and make preparations for risks that may occur in future. Of course, the existence of competent authorities can still be positive. However, the detailed intervention of competent authorities including separate executions beyond coordination and management is no longer appropriate for cybersecurity.

4.4 Political and legislative tasks for the future

In terms of the protection of both information and communication as well as securing its citizens' safety, there are aspects that should be implemented by the state but within these there are also parts that can be performed by the private sector. For example, risk detection activities could be performed by a private security control company. Therefore, the safety of cybersecurity should be secured properly through measures of joint governance with the private sector, not through unilateral action taken by the state [4]. So legislation for new cybersecurity system seems inevitable. The majority of all groups agree that the legislation is necessary for granting of role of private sector in cybersecurity. The survey responses on necessity of legislation to promote private sector's participation in cybersecurity is shown in **Table 10**.

Table 10. Necessity of legislation to promote private sector's participation in cybersecurity

Question: How much the legislation is required for granting of role of private sector in cybersecurity?			
Class	**Group A**	**Group B**	**Group C**
Very necessary	42.9%	27.3%	18.5%
Necessary	28.6%	45.5%	59.3%
Neutral	14.3%	18.2%	20.4%
Unnecessary	0.0%	9.1%	1.9%
Very unnecessary	14.3%	0.0%	0.0%

It is necessary to establish an information sharing system and institutionally promote the revitalization of information sharing. Such action will facilitate smooth information sharing between government organizations, public organizations, private enterprises, and members of both the public and private sector [6]. Ultimately, it is necessary to aim at the establishment of self-regulating cybersecurity promotion system in the form that all entities related to cybersecurity assume responsibility within the range under the jurisdiction and prepare measures, and competent authorities specialized in cybersecurity support and the state assure cybersecurity[16].

It is difficult to say which authorities must have authority to control or to support with cross-sector cooperation. All of the group A says that the Blue House is qualified for the control tower of cybersecurity policy and National Intelligence Service is qualified for the supervisory organization for practical support in cybersecurity. But most respondents of group B say that the former is Cyber Warfare Command and the latter is Cyber Bureau of the National Police Agency. Meanwhile, most respondents of group C say that Cyber Bureau of the National Police Agency is qualified for both the control tower of cybersecurity policy and the supervisory organization for practical support in cybersecurity. It is assumed that such difference is due to the background of each group. So they must be designated from normative

viewpoint based on laws related government organization and security in Korea. The survey result on the control tower of cybersecurity policy is shown in **Table 11**, and the survey result on supervisory organization for practical support in cybersecurity is shown in **Table 12.**

Table 11. Control tower of cybersecurity policy

Question: Which is qualified for the control tower of cybersecurity policy with cross-sector cooperation?			
Class	**Group A**	**Group B**	**Group C**
The Blue House	100%	20.0%	4.7%
Office of the Prime Minister	0.0%	0.0%	4.7%
Ministry of Public Administration and Security	0.0%	10.0%	9.3%
National Intelligence Service	0.0%	0.0%	7.0%
Cyber Warfare Command	0.0%	40.0%	7.0%
National Counter-Terrorism Center	0.0%	0.0%	2.3%
Cyber Bureau of the National Police Agency	0.0%	0.0%	58.1%
Anti-Cybercrime Center	0.0%	10.0%	4.7%
The others	0.0%	20.0%	2.3%

Table 12. Supervisory organization for practical support in cybersecurity

Question: Which is qualified for the supervisory organization for practical support in cybersecurity with cross-sector cooperation?			
Class	**Group A**	**Group B**	**Group C**
The Blue House	0.0%	10.0%	2.3%
Office of the Prime Minister	0.0%	10.0%	2.3%
Ministry of Public Administration and Security	0.0%	10.0%	25.0%
National Intelligence Service	100%	0.0%	4.5%
Cyber Warfare Command	0.0%	30.0%	15.9%
National Counter-Terrorism Center	0.0%	0.0%	2.3%
Cyber Bureau of the National Police Agency	0.0%	40.0%	43.2%
Anti-Cybercrime Center	0.0%	0.0%	4.5%
The others	0.0%	0.0%	0.0%

5. Role of the military in cybersecurity

5.1 Excessive usage of terms including cyber war and cyber warfare

Cyber war denotes a situation of a military campaign with state intervention. It is a type of offensive attacks between states and an act shown during wartime or in a situation similar to wartime [12]. Cyber war or cyber warfare is based upon the premise of a military campaign. From here the question arises whether all security problems require a military campaign or not. It is important to note that the national security plays a key role in limiting a military campaign. The next question that arises is whether the problems of national security require a military campaign or not. The answer to this question is no. In the United States, the original role of the Department of Homeland Security (DHS) was to protect the homeland—a exemplary goal of national security. DHS is, however, not a part of the military. It also does not perform any military campaigns, as those solely belong to the works of the military. It can be determined, therefore, that the military plays only a partial role in both national security and security as a whole. This means that a cyber war is only a part of cybersecurity and the role of the military should also be limited accordingly.

5.2 Comparative review of the relationship between the military and other government organizations in cybersecurity

The United States' legal system and its contents show that the role of the military in cybersecurity is limited. According to U.S. Code, authorities related to domestic security found in Title 6 and the armed forces in Title 10 are distributed quite disproportionately. The Department of Homeland Security (DHS) is the part of the U.S. federal government that oversees and establishes the mandate of Title 6 and its closely. On the other hand, the one that is involved with Title 10 is the Department of Defense (DOD). The U.S. laws related to cybersecurity, included in Title 6, specify that the National Cybersecurity and Communication Integration Center (NCCIC) affiliated with the Department of Homeland Security (DHS) serve as the interface between the government and civilians(6 U.S.C. 148(c)(1)). The 'civilian' in this context is one who is covered within the private sector. The public sector is separate from the military in terms of the internal homeland security issue whereby any military offensives performed externally are excluded. As mentioned, the former is handled by DHS as a part of government organizations taking charge of civil affairs and the latter is handled by the DOD and the military.

It is also clearly shown in case of Japan that the role of the military is limited in cybersecurity. According to the Basic Act on Cybersecurity in Japan, the Cabinet Secretariat manages the Cybersecurity Strategic Headquarters that have affiliated National center of Incident readiness and Strategy for Cybersecurity (NISC) and manage all cybersecurity-related tasks. It is separated from the Self-Defense Forces that take charge of the military field which implies that all cybersecurity in Japan cannot be included in the category of military or become the subordinate concept of military.

5.3 Role and limitations of the military in cybersecurity under the legal system in Korea

According to the survey result, many are aware that the role of the military in cybersecurity is limited. Only 42.9% of the group A, 36.4% of the group B and 40.8% of group C think that a separated military organization is necessary in cybersecurity. The survey result on necessity of a separate military organization in cybersecurity is shown in **Table 13.** Concerning military

domain, most respondents of group A say that the role of the military in cyberspace is limited in physical counterattack, and most respondents of group B and group C say that the military's role in cyberspace is limited in advanced prevention. All groups have a negative attitude to offensive containment. The survey result on role of the military in cybersecurity in military domain is shown in **Table 14**. 100% of the group A, 72.7% of the group B and 44.5% of the group C disagree that military intervention is just for cybersecurity. The survey result on legitimacy of military intervention in cybersecurity affair at peace time is shown in **Table 15**.

Table 13. Necessity of a separated military organization in cybersecurity

Question: How much a separated military organization is required in cybersecurity?			
Class	**Group A**	**Group B**	**Group C**
Very necessary	14.3%	9.1%	9.3%
Necessary	28.6%	27.3%	31.5%
Neutral	57.1%	36.4%	22.2%
Unnecessary	0.0%	27.3%	27.8%
Very unnecessary	0.0%	0.0%	9.3%

Table 14. The military's role in cybersecurity in military domain

Question: Which is the limit of the military's role in cybersecurity in military domain?			
Class	**Group A**	**Group B**	**Group C**
Offensive containment	0.0	0.0%	7.5%
Advanced prevention	28.6%	45.5%	60.4%
Physical counterattack	42.9%	27.3%	3.8%
Non-physical counterattack	28.6%	18.2%	20.8%
Defensive response	0.0%	9.1%	7.5%

Table 15. Legitimacy of military intervention in cybersecurity affair at peace time

Question: Is military intervention in cybersecurity affair legitimate at peace time?			
Class	**Group A**	**Group B**	**Group C**
Strongly agree	0.0%	0.0%	3.7%
Agree	0.0%	9.1%	11.1%
Neutral	0.0%	18.2%	40.7%
Disagree	28.6%	54.5%	35.2%
Strongly disagree	71.4%	18.2%	9.3%

The role of the military confirmed under the Constitution of Korea is limited only to accomplishments for military purposes. Militarization in nonmilitary and private areas is not allowed. This is based on the principle of civilian supremacy or the principle of civilian control [17]. Therefore, the role of the military is primarily decided depending on whether a particular cybersecurity issue falls within the military's purview or not. While cybersecurity is not entirely irrelevant to the military, cybersecurity cannot also be recognized as the sole problem of the military. This line of thinking pertains to cross-national management of cybersecurity along with the management of military. It is difficult to find a reason why Korea should take any other stance.

The concept of defense against a cyber attack is established from the viewpoint that a cyber attack on the cyber infrastructure within our sovereignty can be considered as invasion of territory of the Republic of Korea. The defensive plans for various situations entails not just force, but also operations. However, confirming whether an enemy has conducted a cyber attack or not and whether it requires a military operation or not are also debatable. According

to the principle of proportion or the principle of subsidiarity for the right of general order of military operation, the acknowledgment of 'invasion' of 'enemy' during the emergence of cyber attack should be interpreted strictly within a significantly limited range [18].

5.4 Political and legislative tasks for the future

The possibility of cyber war cannot be undermined. It is necessary to establish the role of the military and reinforce the capability of the military in such a situation. However, it is advisable to appropriately adjust the expansion of the military's role during peacetime rather than wartime. It is needed to recognize the fact that a cyber attack affecting national security is completely different from the situation that requires a military. It is also important to make institutional responses based on such recognition. It is particularly important to keep the military from collecting information or making responses directly for a cyber attack, as such actions are irrelevant to information asset of military in peacetime.

6. Conclusion

A state does not gain the legitimacy of its existence in itself under the constitution. The legitimacy of its existence is acknowledged only when the state manages to protect life, health, and property rights from being infringed and maintains social order amongst the people [5]. The establishment of cybersecurity legislation is an assignment for the state to fulfill its role and prove its legitimacy. An information-oriented society needs to be built. The positive aspects of the newly developed technologies can then be highlighted while any accompanying negative aspects can be concurrently eliminated [2].

Active promotion of cybersecurity legislation has faced difficulty due to concerns about the possible infringements of the fundamental rights. To avoid such criticism, efforts to create a constitution conforming act that minimizes the infringement on the fundamental rights of the people are essential.

However, the sovereignty of the state is more closely connected to cybersecurity rather than unlimited flow of information.. This is because cybersecurity is closely related to safety, which is uniquely one of the roles of the state. Therefore, we should keep in mind that there are many parts of cybersecurity that should be performed directly by the government. Such aspects should be reflected through the establishment of a new act [4]. While there are some parts that the state shall implement, there are also parts that those in the private sector can implement. What can only be made by the state and what can be allowed otherwise must be identified and classified. Based on such a classification, it is also necessary to allow the private actors to perform a certain function by taking the role of society partially through the transfer of responsibility and implementation of tasks. This will be a path to realize the principle of the modern security state also in the realm of cybersecurity.

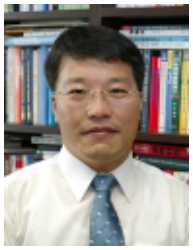
References

[1] Il-Hwan Kim, "Die Untersuchung über die Rolle und Funktion des Verfassungsrechts in der hoch entwickelten technologischen Gesellschaft," *Public Land Law Review*, vol. 37, no. 2, pp. 287-307, August, 2007. Article (CrossRef Link).

[2] Il-Hwan Kim, "Eine Untersuchung über die Änderungsnotwendigkeit des Datensicherungsgesetzes," *Public Land Law Review*, vol. 26, pp. 231-251, June, 2005. Article (CrossRef Link).

[3] Sangdon Park, "A Contemporary Study on Comprehensive Cybersecurity Legislation: Focusing on the Legislative Trends in the United States," *Legislation and Policy Studies*, vol.6, no.2, pp. 5-36, December, 2014. Article (CrossRef Link).
[4] Sangdon Park, "A Study on Constitutional State Responsibility for Information and Telecommunications Infrastructure," *Sungkyunkwan University Doctoral Dissertation*, 2016. Article (CrossRef Link).
[5] Jun-Hyeon Jeong, "A Study on the National Cyber-Security Laws in the high Information Society," *Dankook Law Review*, vol. 37, no. 2, pp. 441-473, June, 2013. Article (CrossRef Link).
[6] Sangdon Park and Injung Kim, "A Study on Tasks for the Legal Improvement for the Governance System in Cybersecurity," *Convergence Security Journal*, vol. 13, no. 4, p. 3-10, September, 2013. Article (CrossRef Link).
[7] Sangdon Park, "A Review of the Japanese Basic Act on Cybersecurity: Focusing on Implications for the Improvement of Legal System for Cybersecurity in Korea," *Kyung Hee Law Journal*, vol. 50, no. 2, pp. 145-175, June, 2015. Article (CrossRef Link).
[8] "Concerns still linger on anti-terrorism law" in *The Korea Times*, March 14, 2016. Article (CrossRef Link).
[9] Cheol-Joon Chang and Chae-Seong Im, "Cyberspace Security and the Constitution in the Age of Big Data and Cloud Computing," *Dankook Law Review*, vol. 39, no. 1, pp. 3-32, March, 2015. Article (CrossRef Link).
[10] NIS, MSIP, KCC, MOI and FSC, *2017 Gukgajeongbobohobaekseo(2017 White Paper on Information Security)*, 2017. Article (CrossRef Link).
[11] Wan Sik Hong, "Gesetzgebungspolitik für die Verwirklichung des Recht auf Sicherheit," *European Constitution*, vol. 14, pp. 225-250, December, 2013. Article (CrossRef Link).
[12] Godwin III, Kulpin, Rauscher and Yaschenko (ed.), *The Russia-U.S. Bilateral on Cybersecurity-Critical Terminology Foundation*, Issue 2, EastWest Institute and the Information Security Institute of Moscow State University, 2014. Article (CrossRef Link).
[13] Jae Ho Sung, "Computer Network Attack and Countermeasures in International Law: Focused on the Interpretation of the UN Charter," *Study on the American Constitution*, vol. 26, no. 2, pp. 199-227, August, 2015. Article (CrossRef Link).
[14] Kwang-Min Park and Sung-Dae Lee, "Countermeasures of the Criminal Law in Accordance with Appearance of "Risikogesellschaf," *Sungkyunkwan Law Review*, vol. 18, no. 3, pp. 513-533, December, 2006. Article (CrossRef Link).
[15] Sungman Hong, "Publicness in Risk Society: Focusing on Leakages of Hydrofluoric Acid and Radioactivity," *The Journal of Korean Policy Studies*, vol. 13, no. 2, pp. 117-135, June, 2013. Article (CrossRef Link).
[16] Sangdon Park, "A Study on Reform of Cybersecurity Governance in Korea in the View of Public Law," *Public Law Journal*, vol. 17, no. 4, pp. 345-373, November, 2016. Article (CrossRef Link).
[17] Kwang-Chan Ahn, "A Study on the Military System on the Basis of the Constitution: Focused on the Operational Command Authority of the Korean Peninsula," *Dongguk University Doctoral Dissertation*, 2002. Article (CrossRef Link).
[18] Jun-Hyeon Jeong, "Study on the Legislative Direction of National Security Laws," *Dankook Law Review*, vol. 39, no. 4, pp. 277-317, December, 2015. Article (CrossRef Link).

Dr. Sangdon Park researches cybersecurity law and policy as a senior researcher in National Security Research Institute. He received Ph.D. degree in law from Sungkyunkwan University. He have been a coeditor and coauthor of Gukgajeongbobohobaekseo(White Paper on Information Security) since 2009. His research interests include constitutional theory, administrative law theory, public law on ICT, security and privacy.



Professor Ilhwan Kim teaches Constitutional Law in Sungkyunkwan University Law School. He graduated from Sungkyunkwan University and studied at Mannheim University as a Ph.D. candidate. He is head of The Science & Technology law institute. And he was a member of Presidential Committee Personal Information Protection Commission (PIPC).

Professor Jaehyoun Kim received his B.S. degree in mathematics from Sungkyunkwan University, Seoul, Korea, M.S. degree in computer science from Western Illinois University and Ph.D. degrees in computer science from Illinois Institute of Technology in U.S.A. He was a Chief Technology Officer at Kookmin Bank in Korea before he joined the Department of Computer Education at Sungkyunkwan University in March 2002. Currently he is a professor at Sungkyunkwan University. His research interests include software engineering & architecture, e-Learning, SNS & communication, internet business related policy and computer based learning.

Professor Kyung Lyul Lee teaches Criminal Law at Sungkyunkwan University Law School. Prior to joining the law faculty in 2015, he was a professor at College of Law of Sookmyung Women's University from 2003 until 2014, including his career as the dean of the college. He was a former chief editor of Korean Association of Comparative Criminal law (2013~2014) and has been the incumbent of Korean Association of Criminology since 2017. He received first Ph.D. degree of Criminal Law at Sungkyunkwan University in 1994 and second Dr. ius at University of Cologne in 2002. He is coauthor of Organized Crime and Criminal Law (2004). He received awards in recognition of his research papers including <The Current States of Financial Crime and Socio-Legal Countermeasures in Korea> in 2003, <Über bleibende Frage nach einer nachträglichen Strafenbildung und Vollstreckung bei Tatmehrheit> in 2007, <Irrtum über Tatumstände und Seine Abgrenzung im §15 I des KorStGB> in 2014.