International Journal of Security and Its Applications
Vol.9, No.2 (2015), pp.13-20
http://dx.doi.org/10.14257/ijsia.2015.9.2.02

An International Comparative Study on Cyber Security Strategy

Kyoung-Sik Min, Seung-Woan Chai and Mijeong Han

Korea Internet & Security Agency
kyoungsik@kisa.or.kr, chaisw@kisa.or.kr, hmj@kisa.or.kr

Abstract

It is expected that utilization and expansion of cyber-space on the basis of big data, cloud computing and IoT(Internet of Things) will be a critical factor which determines national competitiveness. In the meantime, cyber threat accompanied by the utilization of cyber space, attacks targeting cyber space, became enhanced and complicated. Besides this, attackers were also more organized with economic and political intention. As a result, damage caused by the attacks targeting cyber-space has already brought about social confusion. This paper analyzes various countries' cyber security strategy by focusing on public-private partnership, which is one of the common grounds of the strategies. Especially, it focuses on how each country establishes institutional framework of the partnership related to infra-protection. The subject of analysis is limited to U. S. A, EU and Japan.

Consequently, the countries, to some degree, adopt intervention policy through cyber security strategy, and government control is changing from voluntary self-regulation to enforced self-regulation in general. Additionally, public-partnership is more and more emphasized.

1. Introduction

Due to rapid prevalence of internet and smart device, the use of 'cyber-space' becomes a part of daily life for many people. It is expected that the utilization and expansion of cyberspace focusing on big data, cloud computing and IoT (Internet of Things) will be a critical factor which determines national competitiveness. In the meantime, the damage caused by attacks targeting cyber-space has already brought about social confusion because the attacks has become enhanced and complicated and attackers have also been organized with economic and political intention.

Under this circumstance, many countries established Cyber Security Strategy or revised existing strategy. However, there is no internationally used and unified definition of cyber security and many countries individually define the meaning of cyber security. For example, Luiijf (2013) points out the possibility of causing confusion about joint response system toward cyber security because of no unified definition, as a result of a research on whether each country defines the meaning and scope of cyber security or not [1]. According to the research, only 8 countries out of 18, subject of analysis, have defined the meaning of cyber security nationally. ENISA (European Network and Information Security Agency)'s report published in 2012 [2] also puts an emphasis on the importance of internationally unified one

[1] Target of researches are 18 nations: Australia, Canada, Czech, Estonia, France, Germany, India, Japan, Lithuania, Luxemburg, Romania, Netherland, New Zealand, Republic of South Africa, Spain, Uganda, United Kingdom, U.S.A

[2] ENISA(2012a), National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace.
ENISA(2012b), National Cyber Security Strategies: Practical Guide on Development and Execution.

ISSN: 1738-9976 IJSIA

definition of cyber security, and points out that each country has different approaches to cyber strategy.

In fact, the concept of cyber security has been used since Y2K (millennium but) problem was discussed, and it was considered in earnest with 9.11 as a momentum. However, each country utilizes the concept in government paper based on independent interpretation because the concept was widely used and prevalent in spite of nonexistence of unified and standardized definition of cyber security. As a result cyber security of each country has different scope for targeting and various measurements to reach a goal [3].

Even though there are various definitions and different scopes, governmental cyber security shares four points in general according to OECD report in 2012 [4]. First of all, intra-governmental mediation during both of policy making and administration processes becomes more important. It is widely accepted that multiple organizations carry out a policy after intra governmental opinion coordination rather than single organization practices related policy. Therefore, strong leadership, capable of mediating differences of opinion among related organizations, is emphasized in this field. Secondly, private-public partnership is strongly emphasized. Cyber-space is mostly controlled and operated by private sector, thus cooperation between public-private sectors is essential in order to properly respond to current threat aimed to cyber-space. This part is noticeably different from general national security strategy, thus it is necessary to develop appropriate measures based on public-private partnership. Thirdly, many people started to recognize that international cooperation becomes important in this field. Cyber security related issues cannot be settled by individual state unitarily, thus international cooperation is one of the most important parts. However, international cooperation in this field is especially difficult because security policy generally involves confidential information as to national defense. Forth, so-called the fundamental values of internet are highly respected. In other words, the fundamental values of internet utilization such as privacy, freedom of expression and the free circulation of information in various countries' cyber security strategy are greatly emphasized. It clearly states that cyber security strategy is based on the values. This paper analyzes various countries' cyber security strategies by focusing on public-private partnership which is one of the common grounds of the strategies. Especially, it focuses on how each country establishes institutional framework of the partnership related to infra-protection. The subject of analysis is limited to U. S. A, EU and Japan.

Advanced researches that this paper refers to are researches on institution analysis conducted by Andersson and Malm (2007), Assaf (2008, 2009), Bauer and Van Eeten (2009), Dunn-Cavelty and Suter (2009), ENISA (2010), Irion(2012) and so on.

2. Analysis Model

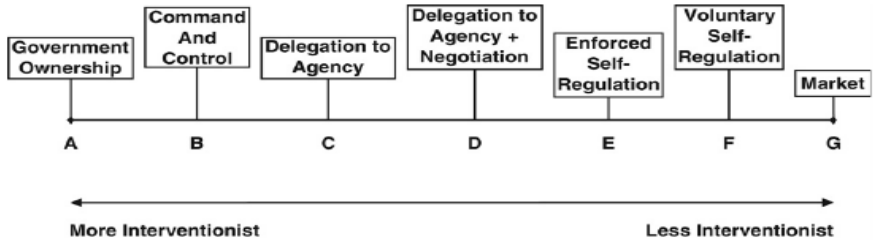
This paper develops analysis based on Assaf (2008)'s research on institution analysis about Critical Information Infrastructure Protection (CIIP). <Picture 1> states classification for government control type according to the degree of government intervention [5].

---

[3] ISO presented Guidelines for Cyber security in July 2012. According to this report, cybersecurity is related to information, network and internet protection and major infrastructure protection but it can specially be defined as countermeasures aiming at the maintenance of stability in cyberspace.

[4] OECD(2012), Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy, OECD Digital Economy Paper, No. 211.

[5] Assaf, D.(2008) ¡°Models of Critical Information Infrastructure Protection,¡± *International Journal of Critical Infrastructure Protection* 1:6-14.



Under 'Government Ownership' system, CIIP is owned and controlled by government. Command and Control regulates standards as to cyber security, sets up penalties when violating rules. Under Delegation to Agency, government authority such as security standard appropriation and monitoring is delegated to politically independent agency. Under the above stated 3 policies, government intervention is strong, on the other hand, the freedom of information protection by private industries is very limited.

Delegation to Agency+Negotiation is an institution that entrusted administrative organizations negotiating with private organizations set various standards. The various institutions that administration organizations promote is more precipitative than restrictive. The one more restrictive system is Enforced Self-regulation which private industries independently develop measures about risk, process, management and performance after autonomous consultation and then these steps are approved and supervised by administrative organizations. This is so-called 'Co-regulation' managed by both of public and private sectors. Under Voluntary Self-regulation system, private sector is able to set standard and various rules and execute them without government intervention. Generally, each industry has its own criteria and enterprises belonging to specific industry field are required to the standard. Additionally, Self-regulation of Market is totally based on market and each enterprise set their own by itself. Under this system, government's role is limited to supply of criteria for market stabilization and the implementation of information security measures according to customer's demand.

However, Assaf (2008)'s framework has, to some extent, limitation because it only measures the degree of autonomy of private sector and government intervention regarding major infrastructure protection. Thus, with his work, it is unable to know whether each country implement cyber security policy or not. Therefore, this paper also examines main contents of each country's cyber security policy and main policy factors of private-public cooperation as Luiijf (2013)'s research mentioned [6] The target of research are can be classified into 4 areas: policy, organization, legal institution and private-public cooperation system. Policy part examines whether the country implement cyber security policy or not. Organization part evaluates whether each country has department which is exclusively responsible for the implementation of cyber security policy and the department's role as control-tower. Legal institution part examines the level of law system maintenance. The last part evaluate whether the country has regular consultative group for the enforcement of private-public cooperation in order to improve the effectiveness of cyber security policy and the consultative group's communication skill.

Next session analyzes 4 factors by focusing on the US, EU and Japan and the degree of autonomy and government intervention of four countries based on Assaf (2008).

3. Analysis of Major Countries' Cyber Security Policy

[6] Luiijf, E., Basseling, K. and de Grasf, P.(2013) "Ninteen national cyber security strategies," *Int. J of Critical Infrastructures*, Vol.9, Nos. 1/2, pp.3-31

3. 1. The Cyber Security Policy of the US

The current cyber security policy of the US is based on Comprehensive National Cybersecurity Initiative (hereafter, CNCI) implemented by Bush administration on January 8th, 2008. Additionally, Obama administration which started in January 2009, put cyber security policy at the top of its agenda and presented (Cyberspace Policy Review (hereafter, CRP) in the same year [7]. Currently, various cyber security policy of the US is based on the CRP.

CRP suggests 10 short-term tasks and 14 mid-term tasks and also presents the establishment of effective information sharing and emergency response system as short-term projects. This project, followed by National Cyber Incident Response Plan (hereafter, NCIRP) presented by the Department of Homeland Security in September, 2010, paved way for the establishment of public-private information cooperation system. NCIRP, focusing on the development of response mechanism for 'critical cyber infringement accident', is aimed for the establishment of strategic framework such as the role and responsibility of organization, action plan, countermeasures and recovery plan to response cyber infringement accident.

Taking 9.11 as a momentum, US government included major infrastructure as a target of cyber threat and started dealing with this issue as national security and implementing related executive order. In March 2003, US government integrated exiting multiple departments charged of the protecting of infrastructure into one organization, the Department of Homeland Security, which is exclusively responsible for the protection of national infrastructure under Homeland Security Act enacted in November, 2002. In addition, Obama administration controls and directs the implementation of national cyber security policy by the operation of National Security Council under immediate control of White House and appointment of Direct General for Cyber Security.

Regarding public-private information cooperation, Executive Order 13636 for Improving Critical Infrastructure Cybersecurity signed by president Obama was presented in February, 2013. The executive order defines several things as follows. Firstly, it requests the Ministers of Homeland Security, Judiciary, National Information and Defense to voluntarily share information about cyber threat as a measure of information sharing in this field. Secondly, it requests the Department of Homeland Security to lead to form consultative group about the cyber security of critical infrastructure with stake-holders. Furthermore, under the leadership of National Institute of Standards and Technology (NIST), Baseline Framework to Reduce Cyber Risk to Critical Infrastructure was developed. However, the executive order has no right to establish and introduce framework, but only aims to support each organization to reinforce voluntary cyber security.

The degree of US government intervention in regard to cyber security policy and related public-private partnership are now based on Voluntary Self-regulation, and US government also try to remove obstacles for the promotion of self-regulation. Additionally, various information cooperation system and support organization were established under the leadership of the Department of Homeland Security. However they are not enforceable but play role as a mediator for effective information sharing. However, it is possible that US government intervention into cyber security policy can be strengthened as Assaf (2008) states that Enforced Self-regulation is implemented for chemical and energy industry.

As an indication of changing to Enforced Self-regulation, the implementation of cyber security law, which Obama administration carry out with the introduction of executive order-

[7] Whitehouse(2009) “Cyberspace Policy Review- Assuring a Trusted and Resilient Information and Communications Infrastructure”

13636, is highly possible to apply Enforced Self-regulation to various fields of industries other than chemistry and energy industries. Cyber security law has not still been specified because some parts of the law is overlapped with other laws, but US government still tries to change Voluntary Self-regulation to Enforced Self-regulation.

3.2. The Cyber Security Policy of EU

Cybersecurity Strategy of The European Union: An Open, Safe and Secure Cyberspace was presented by European Commission (EC) on February 7th, 2013. The strategy seems to be based on the action plan of 'Digital Agenda for Europe (DAE)' presented as EU's comprehensive cyber security strategy in 2010. DAE consists of 101 actions plans of 7 fields. 13 action plans out of 101 are related to cyber security. Additionally, the government placed 7 action plans on top priority tasks. The Cybercsecurity Strategy of The European Union can be evaluated as one of the achievements of the 7 action plans [8].

The Cyber Security Strategy presents 5 specific action plans and coordination scheme formation, consisting of stake-holders in related public-private organizations such as EC, ENISA(European Union Agency for Network and Information Security) and EC3(European Cybercrime Center) in oder to carry out the 5 plans.

Network and Information Security (NIS), which is enforceable to successfully carry out the plans with Cyber Security Strategy, was suggested. The NIS, aiming at the protection of information security by setting up unified EU standard, regulates the monitoring of online stability and the establishment of CERT.

The fact that existing voluntary regulation system of EU system had not responded to cyber infringement action and cyber threat enough played a role as a momentum of the suggestion of the NIS. Under this circumstance, EU suggests government guideline which allows more government intervention. Article 2 of NIS regulates minimum harmonization. Under provision 2, minimum unified cyber threat response measures are applied to EU member states and enterprises but a further implementation of security measures can be developed in accordance with each state's situation. In other words, the NIS regulates minimum responsibility that EU members have to comply with.

Moreover, ENISA established to support EU members's information security measures in 2004 plays an important role in the enforcement and management of various measures based on the NIS. Recently, ENISA presented National Cyber Security Strategies: Setting the course for national efforts to strengthen in Cyberspace as a security strategy guideline for member states in May 2012 [9]. Also, National Cyber Security Strategies: Practical Guide on Development and Execution was introduced in December, the same year [10]. Moreover, thanks to the foundation of the regulation of strengthening of function in June 2013, cyber security policy and legal institution related supports were expanded for ENISA. As a result, its right of intervention into member states' policy and institution was expanded as well [11].

For public-private cooperation of the EU, EP3R (the European Public-Private Partnership for Resilience), based on ENISA as an information sharing network, was established. E3R is a framework that encourages both of government and private sectors to participate in policy

[8] European Commission(2013) "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"
[9] ENISA(2012a) *National Cyber Security Strategies: Setting the course for national efforts to strengthen in Cyberspace.*
[10] ENISA(2012b) *National Cyber Security Strategies: Practical Guide on Development and Execution.*
[11] ENISA(2013) REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013 concerning the European Union Agency for Network and Information Security

making and strategic decision making for critical infrastructure protection and resilience strengthening [12]. Essentially, E3R aims at the construction of environment for trusted collaboration. For this, so called Voluntary Self-regulation system, which allows only limited member' participation, is applied. However, it is expected that EU also change its way to Enforced Self-regulation after the authority of E3R becomes strengthening with the enforcement of cyber security strategy and NIS.

3.3. Cyber Security Policy of Japan

Japan started to organize functions and system related to information security issues in order to strengthen government-centered system by reexamining government roles and functions regarding the issue in December, 2004. Furthermore, in April 2005, Japan also established National Information Security Center (hereafter, NISC) as the control tower of information security under the authority of government. NISC is responsible for forming national information security strategy and plays a role as all-source situation room under an emergency situation. Moreover, it also establishes safety standard which set up the level of protection measures for critical infrastructure and manages CEPTOAR-Council aiming at public-private cooperation as well.

Japan suggested the basic idea and policy direction of information security by establishing The First National Strategy on Information Security: Toward the creation of a trustworthy society in 2006. After this, Japan has been continuously establishing and modifying information security strategies, and finally founded cyber security strategies in 2013. In this strategy, the target area of protection was expanded to cyber security strategy recognizing the importance of cyberspace from information security centered strategy. Also, Japanese cyber security strategies have a lot in common with those of the US such as the establishment of public-private cyber security standard and the formation of information sharing system among stake-holders. Besides this, Japan also tries to exercise global leadership by presenting j-initiative for Cybersecurity. Especially, Japan also makes an effort to contribute to the formation of international cyber security standard.

In case of Japan, the degree of government intervention is defined by Voluntary Self-regulation and each government department manages public-private cooperation system. For instance, the Ministry of Internal Affairs and Communications organizes public-private council, so-called Telecom-ISAC Japan with communicative enterprises and the Ministry of Economy, Trade and Industry also manages information cooperation system with people engaged in manufacturing industry through Initiative for Cyber Security Information sharing Partnership of Japan(J-CSIP). In this case, each government department promotes its own cooperation with private sectors case-by-case. However, Japan expresses its willingness to implement government-driven strategies by forming cyber security governance council encouraging public-private partnership as a measure of overcoming difficulties in interdepartmental cooperation.

4. Conclusion

According to analysis, the US, EU and Japan carry out strategies from the perspectives of cyber security. In the case of the EU, member states are, to some degree, different from each other but every member state recognizes the importance of cyber security policy in common.

[12] EP3R(2010) “NON-PAPER on the ESTABLISHMENT OF A EUROPEAN PUBLIC-PRIVATE PARTNERSHIP FOR RESILIENCE (EP3R)”

The development of ICT and the entry into smart society surely makes our lives affluent and expose us to much threat at the same time. Every state shares the same concept regarding this issue and its countermeasures are also very similar. The important features are as follows; Firstly, it establishes strategies which comprehensively include cyberspace. Secondly, public-private cooperation system under the authority of government tends to be strengthened in order to smoothly respond to major cyber security accident before and after the accident. Thirdly, the way of government intervention into private sectors is changing to Enforced Self-regulation. This trend implies that cyber security related issues are too difficult to solve problems by completely relying on private autonomy.

References

[1] J. J. Andersson and A. Malm, "Public-private partnerships and the Challenge of Critical Infrastructure Protection", *International Journal of Critical Infrastructure Protection*, vol. 1, (**2007**), pp. 6-14.
[2] J. Bauer and M. van Eeten, "Cybersecurity: Stakeholder incentives, externalities, and policy options", *Telecommunications Policy*, vol. 33, nos. 10-11, (**2009**), pp.706-719.
[3] M. Dunn-Cavelty and M. Suter, "Public-Private Partnerships Are No Silver Bullet: and Expanded Governance Model for Critical Infrastructure Protection," *International Journal of Critical Infrastructure Protection*, vol. 2, (**2009**), pp. 179-187.
[4] ENISA, *Incentives and challenges for information sharing in the context of network and information security*, (**2010**).
[5] ENISA, National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace, (**2012a**).
[6] ENISA, National Cyber Security Strategies: Practical Guide on Development and Execution, (**2012b**).
[7] K. Irion, "The Governance of Network and Information Security in the European Union: The European Public-Private Partnerships for Resilience (EP3R)," in Gaycken, S., Kruger, J. and Nickolay, B (Eds.), *The Secure information Society*, Berlin: Springer Publ., (**2012**).
[8] E. Luiijf, K. Basseling and P. de Graaf, "Nineteen national cyber security strategies", *International Journal of Critical Infrastructures*, vol. 9, no. 1/2, (**2013**), pp. 3-31.
[9] White House, "Cyberspace Policy Review", http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

