International Journal of Security and Its Applications
Vol.9, No.10 (2015), pp.267-274
http://dx.doi.org/10.14257/ijsia.2015.9.10.24

A Comparative Study of the Proposed National Cyber-terror Prevention Act

Dea-woo Park[1] and Jin Shin[2]

[1]*Department of Conversing Technology, Hoseo Graduate School of Venture, prof_pdw@naver.com,*
[2]*School of General Education, Dankook University, Corresponding Author : korjin@empal.com*

Abstract

Cybercrimes and cyber-terror attacks disturb national order, and can result in cyber warfare that ruins people's happiness, and destroys national security and people's safety. Cyber-terror attacks have occurred in the 7.7 DDoS attack, the 3.4 DDoS attack, the attack that paralyzed the NH Computer Network, the Jungang Ilbo Incident, The APT attack against KBS, MBC, YTN, the Shinhan Bank, and the NH Bank to stop computer operation. In 2013, the website of Cheongwadae was attacked through the 6.25 cyber-terror attack. In January, 2014, confidential personal information of approximately 85 million customers of 3 credit card companies of the Lotte Card, KB Kookmin Card and the NH Card was stolen. There is a need for real-time response system that can respond in real-time cyber-hacking attacks. However, acts and regulations are insufficient, the budget and the policies and institutions of national cyber security is needed to support the organization. In this study, we analyze and compare the two Cyber-terro Prevention Act was proposed to the National Assembly. And, triggered alarm in the control tower and cyber need for cyber security against cyber crisis.

Keywords: *Cybersecurity, Cyber-terror, Hacking. National Cybersecurity, Prevention Act*

1. Introduction

As information and communication technology and the internet network develop, information exchange in the cyber space is closely associated with our daily living. Information resources for operating national infrastructure, for example, transportation, communication, gas, electricity, water supply, nuclear power and financial transactions are connected through the information and technology networks to build social and national infrastructure [1] and contribute to facilitating our daily living.

Exemplary cyber-terror attacks that have occurred in Korea include the 7.7 DDoS attack in 2009, the 3.4 DDoS attack in 2011, the attack that paralyzed the NH Computer Network, the Jungang Ilbo Incident in 2012, the APT (Advanced Persistent Threat) against KBS, MBC, YTN, the Shinhan Bank, and the NH Bank to stop computer operation and paralyze the nationwide computer network for banks. In 2013, the website of Cheongwadae was attacked through the 6.25 cyber-terror attack in 2013 to post the phrase 'Kim Jong-un, president of unified Korea. In January, 2014, confidential personal information of approximately 85 million customers of 3 credit card companies of the Lotte Card, KB Kookmin Card and the NH Card was stolen. In May, 2014, confidential personal information of KT's 12 million customers were stolen [2].

In particular, organized cybercrimes and attacks from other countries [3] steal people's confidential information [4], national cutting-edge technology and national secrets [5]. Continuing cyberattacks [6] against national infrastructure is increasing potential cyber-terror attacks against Korean society and national infrastructure.

ISSN: 1738-9976 IJSIA

2. Comparative Study of National Cybersecurity Act

The cyber world made by connecting countries in the world with the internet is developing into a borderless cyber world for exchanging information with the world by means of wireless communication terminals, for example, personal smartphones [7].

As described above, negative functions rather than positive functions of the cyber world globally connecting people cause national and social issues in relation to cybercrimes [8] and cyber-terror attacks. In particular, while cyber-terror attacks occur between countries in each region of the world, the cyber warfare as a skirmish of wars between countries is a great threat to national security, it is thus necessary to study and establish regulations for national cybersecurity.

The technology in the cyber world is further complicated and advanced, and has less temporal spatial restrictions. It is almost impossible that departments of the government or individuals tackle infringements, cybercrimes and terror attacks.

In particular, the threat to national security through cyber-terror attacks gives people in the real world with direct and indirect damages. In addition, cybercrimes and terror attacks disturb national order, and can result in cyber warfare that ruins people's happiness, and destroys national security and people's safety.

Overseas governments lead response to the cyber-terror attacks. The US Central Command is a control tower for all sorts of cyber warfare, and supported by private, public and military organizations. The People's Liberation Army General Staff Department of China plans and performs cyber warfare, and controls private organizations provided with an optical communication network and IP for national management.

Major countries including the USA, the UK, and China in Table 1 have their own legislative and institutional systems for national cyber crisis management. In the US, the Department of Homeland Security responsible for national infrastructure protection policies according to the Homeland Security Act is in charge of cyber-terror policies to protect cybersecurity as national infrastructure, and the president has a cybersecurity coordinator responsible for cooperation and adjustment between private, public and military organizations.

USA Cybersecurity Council appointed by the president, responsible for information protection industry and cybersecurity, focusing on cybersecurity technology, and cooperation with enterprises, universities and research institutes (synergy effect by the package of cybersecurity, training security experts and supporting the security industry).

Table 1. Legislation for National Cybersecurity in Major Countries

USA	o HSA(Homeland Security Act), FISMA (Federal Information Security Management Act) MB (Office of Management and Budget) specifies responsibilities of each institutions including enforcement of security policies for federal information resources to protect the government's computer network and key infrastructure. IS(Department of Homeland Security) is responsible for building the national cybersecurity action system, operating cyber threat tackling programs, and organizing risk management activities, for example, 'global cooperation according to NSSC (National Strategy to Secure Cyberspace).' 4 The Obama Administration positioned the Cybersecurity Advisor in the Presidential Office to establish the Cybersecurity Act of 2009.
Japan	o Basic Act on Advanced Information and Communication Network Society Formation (IT Basic Act) SC (National Information Security Center) under the IT Strategy Division is responsible for collecting cyberattack information, assessing risks, and instructing related institutions to establish risk management strategies.

China	o National Safety Act, Internet Safety Protection Management Act e Ministry of State Security and the National Administration for the Protection of State Secrets are responsible for cybersecurity and actions against cybercrimes. NCERT (National Computer Network Emergency Response Technical Team) under the Ministry of Industry and Information Technology is responsible for safety monitoring, warnings and technology support for the network of national authorities.
Germany	o BSI Act (Federal Office for Information Security Act) he BSI is responsible for normally operating key infrastructure and responding to crises according to the 'NPSI (National Plan for Information Infrastructure Protection) for protecting IT infrastructure'. e BSI prevents secret stealing, secures data safety and blocks network infringements. e BSI is establishing the Information and Communication Act to regulate the obligation of national key enterprises and information and communication suppliers to report safety incidents to BSI.
Canada	o CSIS Act (Canadian Security Intelligence Service Act) e CSIS is responsible for investigating and analyzing the effect of cyber threats on national security, and assessing threats and risks thereof. IRC (Canadian Cyber Incident Response Center) under PSM (Process Safety Management) monitors cyber threats in real time to protect national key infrastructure and control national response activities against cybersecurity incidents.
France	O ANSSI (Agence Nationale de la Securite des Systemes d'Information) established the Cybersecurity Act to tackle cyberattacks on private enterprises and national infrastructure industry and enhance cybersecurity.
Norway	o National Security Act - NSA(National Security Agency) responsible for information security specifies secret protection, password policy, certification and monitoring of information system security.

3. South Korea Acts Governing National Cyber-Terror

able 2 illustrates an analysis and comparison of regulations for national cyber security passed by the National Assembly of Korea and currently enforced, and those for tackling national cyber-terror attacks, pending in the National Assembly.

It is impossible to prevent or block all cyberattacks in real time. For example, the hacking attacks on national infrastructure that occurred in Korea and other countries, or those on KHNP by using the current regulations for national cybersecurity. They are just used for post-incident response.

Therefore, it is urgent that the National Assembly passes the regulations for national cybersecurity to be a real-time response system provided with teams and budgets.

Table 2. Comparison of Regulations for National Cybersecurity

Category	Regulations for national cyber safety management	Information and Communication Infrastructure Protection Act	Act on Promoting the Use of Information and Communication Network and Information Protection
Application	◦ Information and communication network of central administrations, local administrations and public organizations (§3)	◦ Key information and communication infrastructure (§1)	◦ Information and communication service providers (§3) ◦ Integrated information and communication system providers (§46①)

Conference	◦ National cyber safety strategy conference (§6,7)	◦ Information and communication infrastructure protection committee (§3)	
Enforcement	◦ National Cyber Safety Center (§8)	◦ Management (§8) ◦ MSIP (Ministry of Science, ICT and Future Planning), NIS (National Intelligence Service) (§5-2)	◦ MSIP
Planning	◦ NIS prepares and distributes cyber safety guides (§9③). ◦ Central administrations establish and enforce cyber safety actions (§9①).	◦ The management authorities establish and enforce protection measures (§5). ◦ Central administrations establish and enforce protection plans (§6). ◦ MSIP and NIS announce planning guidelines (§5). ◦ Central administrations establish their jurisdictional protection guidelines (§10①).	◦ MSIP and KCC (Korea Communication Commission) work out measures for protecting user's personal information (§4). ◦ MSIP announces information protection guidelines (§45).
Verification of performance	◦ NIS verifies information and communication network safety (§9④).	◦ MSIP and NIS verify performance of protection measures by management institutions (§5-2).	◦ Certification of information protection management system (§47).
Response, recovery	◦ Central and public organizations and local bodies take early actions, and NIS is notified of them (§12). ◦ Request NIS and related institutions to take measures for recovery and prevention of damage spreading (§12③). ◦ Organize and operate a government-wide cyber crisis action center for the critical stage (§13③). ◦ NIS investigates incidents and the organizations themselves investigate minor incidents (§13①). ◦ NIS organizes a joint investigation team in the action center (§13④).	◦ Take action for recovery and protection if infringement incidents against management authorities happen, and request support if required (§14). ◦ Organize an information and communication infringement incident action team if any incident has many victims (§15). ◦ MSIP and NIS notify guidelines for establishing countermeasures (§5). ◦ The central administration establishes protection guidelines for its jurisdiction (§10①). ◦ When an infringement incident occurs, the management authorities notify the related authorities of the incident, and the related authorities take necessary measures, e.g., prevention of damage spreading (§13①).	◦ MSIP (KISA) performs activities to respond to infringement incidents including emergency measures (§48-2). ◦ KCC organizes a joint private-public investigation team to analyze the cause of critical infringement incidents if they occur (§48-4).

Information sharing	◦ The government and public organizations notify NIS of cyber threat information (§10①). ◦ NIS takes measures following the notification of cyber threat information (§10②). ◦ The government and public organizations organize and operate a security control center (§10②).	◦ Information sharing and analysis center for each field, e.g., banking and communication (§16①). - Operate a real-time infringement warning analysis system.	◦ MSIP (KISA) collects and propagates information about infringement incidents (§48-2).
Issuing warning	◦ Issue warnings by levels (§11①). ◦ KCC issues warnings for the private sector; MND (Ministry of National Defense) issue warnings for the military sector (§18).		◦ MSIP (KISA) forecasts and warns infringement incidents (§48-2).

4. Comparative Study of the Proposed National Cyber-terror Prevention Act in National Assembly

The proposal suggested by assembly man Seo Sang-gi and pending in the National Assembly in 2015 has penal regulations for obligations and duties, applied to 'bodies responsible for prevention of cyber-terror attacks and risk management' including key private and public sectors.

The proposal in table 3 suggested by assembly man Seo Sang-gi and pending in the National Assembly in 2015 has penal regulations for obligations and duties, applied to 'bodies responsible for prevention of cyber-terror attacks and risk management' including key private and public sectors. The proposal suggested by assembly member Ha Tae-gyeong lays such obligations and duties mainly on central administrations, local bodies and public organizations.

Table 3. Difference between Regulations (Provisional) Suggested by Seo Sang-gi and Ha Tae-gyeong (Reference to South Korea National Assembly Information Committee)

Category	Proposal by Seo Sang-gi	Proposal by Ha Tae-gyeong
Application	Responsible public and private bodies and supporting bodies	Central administrations, local bodies, public organizations (not including independent organizations specified in the Constitutions)

Training for response	Carry out training according to the Presidential Decree (participants not specified)	Carry out training for responding to cyber crises in which responsible bodies participate.
Investigation of incident by head of NIS	Carried out investigation only when decided that critical impact is concerned on national security and interests.	Incidents that occurred in the information and communication network of central administrations, local bodies and public organizations
Military sector	No provision	The Minister of MND carries out the investigation.
Report to National Assembly	- The head of NIS checks performance of the enforcement plan by the responsible bodies and reports the assessment result every year. - Reason of issuing a critical cyber crisis warning.	
Who issues cyber crisis warning	Head of NIS (discussion is required with a secretary in the National Security Office responsible for critical cyber crises)	Head of NIS , Korea Communications Commission (private sector)
Conference	- Strategic meeting for national cyber safety (chairperson : head of NIS), conference between private and public organizations	Strategic meeting for national cyber safety (chairperson : prime minister)
Blocking malicious program from spreading	- Operators provide malicious program information. - The government deletes or blocks malicious programs.	—
Building infrastructure	R&D, supporting the industry, training human resources, publicizing training, global cooperation.	Training human resources and publicizing training
Penal regulations	Penal regulations for some violation of obligations	—

5. Conclusion

In South Korea, while the cyber environment of international society quickly changes, cyberattacks occur. The Cybersecurity Acts for national cybersecurity aim to build a general national action system by private, public and military organizations, detect cyber-terror attacks in advance to block potential attacks and early warfare and integrate national capacity for fast action if they occur.

Acknowledgments

"This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) Funded by the Ministry of Education in 2015"(No. 2013R1A1A2010118).

References

[1] D.-w. Park, "National Cybersecurity Policy Report", Forum of National Cybersecurity Policy, National Assembly, (**2012**) December 31.
[2] D.–w. Park, "Analysis of Acts for Cybersecurity", Military Forum, no. 75, (**2013**) November.
[3] D.-w. Park, "National Cybersecurity Act (Proposal)", Forum of National Cybersecurity Policy, National Assembly, (**2013**) May 14.
[4] I.-w. Park and D.-w. Park, "A Study of Intrusion Security Research and Smishing Hacking Attack on a Smartphone", Journal of the Korea Institute of Information and Communication Engineering, vol. 17, no. (**2014)** November, pp. 2588-2594.
[5] D.-w. Park, "Forensic Analysis Technique of Car Black Box", International Journal of Software Engineering and Its Applications, vol. 8, no. 11, (**2014**) November.
[6] D.-w. Park, "Extraction of Forensic Evidence and Hacking Attacks about IP-PBX", Journal of the Korea Institute of Information and Communication Engineering, vol. 16, no 6, (**2013**) June, pp. 1360-1364.
[7] D.-w. Park, "Analysis on Mobile Forensic of Smishing Hacking Attack", Journal of the Korea Institute of Information and Communication Engineering, vol. 18, no. 12, (**2014**) December, pp. 2878-2884.
[8] D.-w. Park, "Analysis of Internet Banking Security Crack through Messenger Hacking", Future Information Communication Technology and Applications, Communications in Computer and Information Science, (**2011**) September 22.

Authors

Dea-woo Park, he is an Associate Professor at Hoseo University in South Korea. Professor Park researcher of the Hacking Forensic, Information Technology Communication in Lab at Hoseo Graduate School, Professor Park received the B.S. degree in computer science from the Soongsil University in 1995. He received the M.S. degree in 1998. He received the Ph.D. degree from the computer science department of the Soongsil University in 2004. He has also been appointed Secretary General of Forum of National CyberSecurity Policy, and Chair of Korea Information Security Forum. Professor Park has been appointed Vice-Chairman of Korea Institute of Information Security & Cryptology, Korea Information and Communications Society, Korea Digital Forensic Society.

Jin Shin, he is a Professor at Dankook University in Korea. Professor Shin researches Information and Communication Policies, Industrial Organization, and Innovation Policies. Professor Shin received the B.S. degree in International Economics from the Seoul National University in 1983. And he received the Ph.D. in Economics from the Economics department of the Florida State University in 1991. He served as a president at Chungnam Technopark and also at Songdo Technopark. He also serves as a chairman of Korea Technopark Association and of Korea Technology Transfer Agent Association. He worked as a board member of Korea Technology Transfer Institute, Korea Ceramic Technology Institute, and Korea Evaluation Institute of Industrial Technology.