International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.207-214
http://dx.doi.org/10.14257/ijsia.2016.10.10.19

Analysis and Comparison of Regulations for National Cybersecurity

Dea-woo Park

Department of Conversing Technology, Hoseo Graduate School of Venture, Seoul 06724, South Korea
prof_pdw@naver.com

Abstract

Cyber space moving at the speed of light is beyond the national boundaries and globalized, demonstrates the power of a country and affects people's living in the visible world. The technology in the cyber world is further complicated and advanced and it has less temporal spatial restrictions. It is almost impossible that departments of the government or individuals tackle infringements, cybercrimes and terror attacks. In this paper, the author studied_ a policy for national cybersecurity and research to make the laws on national cybersecurity. To do this, the author made a comparative study of the cybercrime, cyber terror, and cyber warfare. When a crisis occurs on the cyber security of the country, a study Analysis and Comparison of Regulations for National Cybersecurity that is currently in effect, and study the alert issued in step 5 of cyber crisis. The author will endeavor to establish regulations and systems and embody policies related to sustainable national cybersecurity policies for the country and people

Keywords*: Cybercrime, Cybersecurity, Cyber Terror, Cyber Warfare*

1. Introduction

Cyber space moving at the speed of light is beyond the national boundaries and it is globalized, it demonstrates the power of a country and affects people's living in the visible world. Recently, South Korea, phishing [1], pharming [2], such as smishing [3] cyberattacks [4] on people is growing. In addition, the country's infrastructure, finance, broadcasting, and cyberattacks on nuclear power is being executed [5].

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.

Exemplary cyber terror attacks that have occurred in South Korea include the 7.7 DDoS attack in 2009, the 3.4 DDoS attack in 2011, the attack that paralyzed the NH Bank 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 was stolen. In December 2014, a hacker stole the nuclear power data including key nuclear power technology like 'SPACE(Safety and Performance Analysis CodE)' managed by KHNP(Korea Hydoro & Nuclear Power Co., Ltd) to infringe people's assets and further increase damages and people's uneasiness about cyber terror attacks against national infrastructure [6].

The author held the workshop "National Cybersecurity Policy Forum" to analyze issues involved in current national cybersecurity policy, suggest alternative ideas for

ISSN: 1738-9976 IJSIA

national policy, establish regulations and consolidate people's safe living and national security [7].

The author will endeavor to establish regulations and systems and embody policies related to sustainable national cybersecurity policies for the country and people by holding national cybersecurity forum workshops with private, public and military experts specialized in legislation, the administration of justice, administration, national defense, communication, finance, education, information and criminal investigation to implement a national cybersecurity system to respond to hacking attacks from invisible locations against national infrastructure and people's living in real time[8].

Canada's Anti-Spam Law in Table 1 has been enforced since July 1, 2014. The Law stipulates that it is essential to send commercial e-messages after obtaining recipient's prior consent. If an enterprise sends an e-mail without recipient's prior consent, it shall be fined a maximum of ten million Canadian dollars and individuals shall be fined one million Canadian dollars.

Table 1. Details of Canada's 'Anti-Spam Law' Effective since July 1, 2014

Article	Regulation and activity for preventing spam e-mail
Article 6	Spamming: sending e-messages not requested are not allowed in the format of e-mail, text, social media or other communication means
Article 7	No hacking: changing transmitted data without permission is not allowed.
Article 8	No installation of malware: installing computer programs, producing, phishing, pharming, or spyware without a consent is not allowed.
Article 82(2)	E-mail harvesting: it is not allowed to use computer systems for collecting e-mail addresses without consent.
Article 82(3)	Infringement of privacy: unauthorized access to computer systems for collecting personal information without consent (means access to computer systems in violation of Canada's Federal Legislation)

In South Korea, Eight mails from August 2013 used the social engineering technique to steal e-mail recipient's personal information by phishing (100%).

Most of 58 spam e-mails in 2014 used the conventional social engineering technique by phishing (80.1%) by attaching malware to the e-mail, to lure victims to click the attached files and thus infect victim's computer or terminal with the malware. Among the e-mails, 10 (14.7%) were sent for smishing to steal victim's personal information, and three (5.2%) were sent for pharming to lure victims to go to a fake website to deceive victims and steal their personal information.

The 84 spam mails sent from January to July in 2015 include 53 mails for phishing (54.1%), 26 mails for smishing (40.0%) and 5 mails for pharming (5.9%), implying recent increasing attempts to steal victim's personal information through smishing [8].

Spam and cyberattacks from abroad leads to cybercrisis to the people and the country. In particular, the conflict of the country is being developed into an invisible cyber warfare.

It is impossible to prevent or block, in real time, all cyberattacks, for example, hacking attacks on national infrastructure that occurs in South Korea and other countries, it is 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 allocation [9].

The National Cybersecurity Act in response to cybercrime and cyber-terrorism and cyber warfare citizens, public agencies, and experts in the military to establish a comprehensive response system for participation. National Cybersecurity Council should respond to cyber attacks, defense, media psychological warfare. National Cybersecurity Council mutually shares relevant information and real-time analysis, information sharing and coordination support. In addition, the permanent council of the national constitution, government, and military operations [10].

2. Definition of Cyber Terms

A. Cyber Crime

A "cybercrime" is a criminal behavior which causes the country and people to experience damage by intruding into an information and communication network without permission for access to the network, threatening, disturbing, paralyzing, or destroying information and communication resources by means of hacking attacks, computer virus, service interruption, electromagnetic waves or remote control, stealing, distorting, propagating, infringing or draining information, misusing rights, operating illegal websites, corrupting or deleting information[10].

B. Cyber Terror

A "cyber terror attack" is a case where at least 2 cybercrimes including stealing, distorting, propagating national and social infrastructure information for national safety including foreign affairs, national defense, unification, administration, social living and people's safety information, infringing, draining the information, misusing the rights thereof, operating illegal websites, corrupting and deleting the information, simultaneously occur through an information and communication network. The cybercrimes then paralyze and break down national functions to result in issuing at least warnings or cause potential spreading of danger or damages [10].

C. Cyber Warfare

A "cyber warfare" means performance of physical, electronic, economic, mental and human warfare to do harm to the country's and its people's safety, including destruction of national infrastructure, command and control warfare, military information warfare, electronic warfare, psychological warfare through media, hacking warfare and economic information warfare to achieve military objectives through cybercrimes and terror attacks[10].

3. Comparative Study on Regulations for National Cybersecurity

As described above, although increasing cyber terror attacks and cyber warfare threats cause tangible and intangible damages, South Korea does not have established regulations and procedures to systematically tackle cyber terror attacks and cyber warfare on a national basis. Therefore, if cyber terror attacks and warfare occur, it can be a significant threat to national security and interests, and people's safety.

Table 1 illustrates an analysis and comparison of regulations for national cybersecurity passed by the National Assembly of South Korea and currently enforced [8], and those for tackling national cyber terror attacks, pending in the National Assembly.

Table 1. Analysis and Comparison of Regulations and Laws 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	◦ Key information and communication infrastructure	◦ Information and communication service providers ◦ Integrated information and communication system providers
Conference	◦ National cyber safety strategy conference	◦ Information and communication infrastructure protection committee	
Verification of performance	◦ NIS verifies information and communication network safety	◦ MSIP and NIS verify performance of protection measures by management institutions	◦ Certification of information protection management system
Enforcement	◦ National Cyber Safety Center	◦ Management ◦ MSIP (Ministry of Science, ICT and Future Planning), NIS (National Service)	
Planning	◦ NIS prepares and distributes cyber safety guides. ◦ Central administrations establish and enforce cyber safety actions	◦ The management authorities establish and enforce protection measures. ◦ Central administrations establish and enforce protection plans. ◦ MSIP and NIS announce planning guidelines. ◦ Central administrations establish their jurisdictional protection guidelines	◦ MSIP and KCC (Korea Communication Commission) work out measures for protecting user's personal information. ◦ MSIP announces information protection guidelines
Information sharing	◦ The government and public organizations notify NIS of cyber threat information. ◦ NIS takes measures following the notification of cyber threat information. ◦ The government and public organizations organize and operate a security control center.	◦ Information sharing and analysis center for each field, e.g., banking and communication. ◦ Operate a real-time infringement warning analysis system.	◦ MSIP (KISA) collects and propagates information about infringement incidents.
Issui	◦ Issue warnings by		◦Issuing warning

ng warning	levels.		
Response, recovery	◦ Central and public organizations and local bodies take early actions, and NIS is notified of them. ◦ Request NIS and related institutions to take measures for recovery and prevention of damage spreading. ◦ Organize and operate a government-wide cyber crisis action center for the critical stage. ◦ NIS investigates incidents and the organizations themselves investigate minor incidents. ◦ NIS organizes a joint investigation team in the action center.	◦ Take action for recovery and protection if infringement incidents against management authorities happen, and request support if required. ◦ Organize an information and communication infringement incident action team if any incident has many victims. ◦ MSIP and NIS notify guidelines for establishing countermeasures. ◦ The central administration establishes protection guidelines for its jurisdiction. ◦ 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.	◦ MSIP (KISA) performs activities to respond to infringement incidents including emergency measures. ◦ KCC organizes a joint private-public investigation team to analyze the cause of critical infringement incidents if they occur.

In particular, the threat to national security through cyber terror attacks gives people in the real world 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.

It is impossible to prevent or block, in real time, all cyber attacks, for example, hacking attacks on national infrastructure that occurs in South Korea and other countries, or those on KHNP by using the current regulations for national cybersecurity. It is 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 allocation.

The following items are things to be considered for a national cybersecurity.

The government should response to the cybercrimes, cyber terror, and cyber warfare, and issue a relevant warning in 5-step cyber terror attack warnings, that is, normal (step 1), caution (step 2), alert (step 3), terror attack (step 4) and warfare (step 5).

The government shall order the Cybersecurity Committee to take measures for minimizing the damages and recovering it from if cyber terror warnings at least step 3.

The government can organize and operate a cyber terror response team ('Team') for national security in order to analyze causes, investigate incidents, take immediate actions, and recover from damages if (at least step-3) warnings were issued.

It is allowed to take necessary measures to develop technology and equipment required for tackling cyber terror attacks and warfare and improve the technology.

It is allowed to train cyber experts, establish and enforce a plan for securing human resources to tackle cyber terror attacks and warfare.

The responsible bodies with specialized human resources, technology and equipment for tackling cyber terror attacks and warfare shall share and spread information with responsible bodies without human resources, technology and equipment.

The government can cooperate with international organizations, groups and foreign countries to tackle cyber terror attacks and warfare.

4. Conclusions

In this paper, the author distinguished three cyber crisis words, and defined in words cybercrimes, cyber terror, and cyber warfare. When the national cybercrisis, The author has to analyze and compare of Regulations for National Cybersecurity, it shall issue a cybercrisis alert Step 5. This paper will be used as a basis for national legislation related to cybersecurity.

It is necessary to further study the method of blocking cyberattacks by hackers and take legislative and institutional measures and manual against cyberattacks.

Acknowledgements

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] S. S. Kulkarni, M. Tomar, A. Mittal, S. Arondekar and A. Nayakawadi, "Survey on Phishing Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 2, **(2015)** Feb., pp. 501-504.

[2] I. S. Alfayoumi and T. S. Barhoom, "Client – Side Pharming Attacks Detection using Authoritative Domain Name Servers", International Journal of Computer Applications, vol. 113, no. 10, **(2015)** Mar., pp. 26-31.

[3] D.-w. Park, "Forensic Analysis of Smishing Hacking Attack in Smartphone", Information, vol. 17, no. 11(B), **(2014)** Nov., pp. 5683-5688.

[4] 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)** Jun., pp. 1360-1364.

[5] "Monthly analysis and trend of Internet Incidents: March", KISA , http://www.kisa.or.kr/ Korea, Korea Internet & Security Agency, **(2014)** Mar.

[6] J. Shin and D.-w. Park, "A User's Guide for Countermeasures against Smishing Incident", Information-An International Interdisciplinary Journal (International Information Institute: vol 17. no. 11(B), **(2014)** Nov. 30.

[7] D.-w. Park, "National Cybersecurity Policy Report", National Cybersecurity Policy Forum, National Assembly, **(2012)** December 31.

[8] D.-w. Park, "A Comparative Study on Cybercrime, Cyber Terror, Cyber Warfare", 2016 Asia Workshop on IT Convergemce of KIICE 2016, **(2016)**, Feb. 18, pp. 3-6.

[9] D.-w. Park, "National Cybersecurity Policy Report", National Cybersecurity Policy Forum, National Assembly, **(2013)** May 14.

[10] D.-w. Park, "Draft of National Cybersecurity Act", International Journal of Security and Its Applications, vol. 9, no. 11, **(2015)** Nov.

Author

Dea-woo Park, he is an Associate Professor at Hoseo University in South Korea. Professor Park researches of Cybersecurity, Hacking Forensic, Information Communication Technology in Lab at Hoseo Graduate School, Professor Park received the B.S. degree in computer science from the Soongsil University in 1995. And 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.

.