International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.105-112
http://dx.doi.org/10.14257/ijsia.2015.9.11.11

Draft of National Cybersecurity Act

Dea-woo Park

Department of Converging Technology,
Hoseo Graduate School of Venture
prof_pdw@naver.com

Abstract

The world has actually been attacked from other countries by means of cyberattacks against national infrastructure and cyber-terror weapons. In December, 2014, a hacker stole the nuclear power data including key nuclear power technology to infringe people's assets and further increased damages and people's uneasiness about cyber-terror attacks against national infrastructure. The National Cybersecurity Act in response to cybercrime and cyber-terrorism and cyberwarfare citizens, public agencies, and experts in the military to establish a comprehensive response system for participation. National Cybersecurity Council should respond to cyberattacks, defense, media psychological warfare. National Cybersecurity Council is mutually share relevant information and real-time analysis, information sharing and coordination support. National Cybersecurity Act aim to build a general national action system by private, public and military organizations, detect cyber-terror attacks in advance to block potential cyber-terror attacks and warfare early and integrate national capacity for fast action if they occur.

Keywords*: Act(Draft), Cybersecurity, Cyberwarfare, Hacking. National Cybersecurity*

1. Introduction

As information and communication technology develops to facilitate working in the wired and wireless cyber space, cyber attacker [1] make a detour to conceal themselves [2], and collectively attack targets to commit cybercrimes [3] against people's living and social [4] and national infrastructure.

The world has actually been attacked from other countries[5] by means of cyberattacks against national infrastructure and cyber-terror weapons [6]. In 2007, the cyberattack weapons(malicious codes) including Stuxnet and Duqu [7] paralyzed the nuclear system of Iran to steal national secrets. In September, 2012, more than one million people participated in the agitation urged through the SNS to result in nationwide agitation leading to extreme conflict between members of the public, and ruin national economy in Mexico [8]. In 2013, information about the F-35 fighters was stolen through a subcontractor of the US Department of Defense. Confidential personal information [9] of approximately 6 million Facebook users in 2013 and approximately 38 million Adove users in October 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 increased damages and people's uneasiness [10] about cyber-terror attacks against national infrastructure.

The National Cybersecurity Act in response to cybercrime and cyber-terrorism and cyberwarfare citizens, public agencies, and experts in the military to establish a comprehensive response system for participation. National Cybersecurity Council should respond to cyberattacks, defense, media psychological warfare. National Cybersecurity Council is mutually share relevant information and real-time analysis, information sharing

ISSN: 1738-9976 IJSIA

and coordination support. In addition, the permanent council of the national constitution, government, and military operations

2. National Cybersecurity Act (Draft)

All Article 1 (Objective) : This Act aims to detect cyberattacks and cyber-terror attacks on a national basis, block potential cyber-terror attacks and warfare at their early stage, integrate national cybersecurity capacity when cyber-terror attacks and warfare occur for quick action to ensure people's safety and protect their interests.

Article 2 (Definition) : ① Definitions of terms used in this Act is described below. 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. A "cyber-terror attack" is the case that 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. A "cyberwarfare" means performance of physical, electronic, economic, mental and human warfare to do harm to country's safety 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. A "cyber-terror warning" is for providing information to take measures ideal for the risk or threat level and give warnings if signs of cybercrime attacks are detected, analyzed or identified or cyber-terror attacks and warfare are forecasted. " Cyber-terror management" means all national activities, for example, detecting, analyzing cyberattacks, sharing information, cooperating for response, investigating incidents, training human resources, punishing criminals, issuing warnings and cooperating between involved authorities in order to systematically respond to and tackle cyber-terror attacks and warfare. A "responsible cyber-terror attack management body ("responsible body")" is any of the following authority managing cyber-terror attacks. 1) National authorities, local bodies and public organizations organized in accordance with the Constitution of Korea, the Government Organization Act and other regulations. 2) Authorities managing key information and communication infrastructure according to the provisions described Article 8 of the Information and Communication Infrastructure Protection Act. 3) Integrated information and communication system providers according to the provisions described Article 46-1 of Act on Promotion of Information and Communication Network Utilization and Information Protection, *etc*., and major information and communication service providers according to the provisions described Article 45-3(1-1) of the same Act. 4) Enterprises or research institutes which own key national technology according to the provisions described Article 9 of Act on Prevention of Divulgence and Protection of Industrial Technology. 7. A "cyber-terror management authority ("support authority")" is any of the following authorities or enterprises for quickly detecting, responding to cyberattacks,

investigating the incidents, punishing the cybercriminals and addressing damages caused by cyberattacks. 1) Electronics and Telecommunications Research Institute according to the provisions described Article 8 of Act on the Establishment, Operation and Fostering of Government-Funded Science and Technology Research Institutes. 2) Korea Internet and Security Agency according to the provisions described Article 52 of Act on Promotion of Information and Communication Network Utilization and Information Report. 3) A person who produces or sells computer virus vaccine software as any one of persons who are registered as a software provider according to the provisions described Article 24 of Software Industry Promotion Act. 4) Information protection consultants specified according to the provisions described Article 17 of Information and Communication Infrastructure Protection Act. 5) Security control service providers specified by the minister of MSIP ② Definitions of terms used in this Act but not described in above (①) shall comply with the provisions described in the Information and Communication Infrastructure Protection Act, the Act on Promotion of Information and Communication Network Utilization and Information Protection, the Framework Act on National Information and the Telecommunications Business Act.

Article 3 (Link with other acts) : The provisions of this Act shall control over the Framework Act on the Management of Disasters and Safety and other acts for management of cyber-terror attacks and warfare.

Article 4 (Organizing national cybersecurity committee) : ① Organize a national cybersecurity committee (“Cybersecurity Committee”) controlled by the president for nation-wide comprehensive and systematic response and management of cyber-terror attacks and warfare against cybercrimes, cyber-terror attacks and warfare. ② The president shall appoint the chairperson of Cybersecurity Committee ("Cyber Chairperson") who sorts out and controls works with authorities involved in national cybersecurity. Teams and operation of the Committee shall be specified by the Presidential Decree. ③ The president can order the head of responsible bodies described in Article 2-1(5-1) to dispatch human resources and provide equipment if required for operating the Cybersecurity Committee specified in above ①. ④The National Assembly can state its opinion on report, operation and teams of the Cybersecurity Committee’s activities.

Article 5 (Organizing conference body by private, public and military organizations) : ① The Cyber Chairperson shall organize and operate a normal conference body by private, public and military organizations for sharing and analyzing related information in real time, sharing other information and taking cooperative response in order to effectively manage cyber-terror attacks and warfare, and respond to cyberattacks, defense, and psychological cyberwarfare. ② Provisions required for enforcing provisions in above ① shall be specified by the Presidential Decree.

Article 6 (Organization operation and making budget) : Give the following rights to relevant authorities and specify details thereof by the Presidential Decree in consideration that the cyber-terror attacks and warfare go on in Korea and other countries. ① Appointment and dismissal of team members ② Independent budgeting and the right of using the budget ③ Personnel management and administrative support depending on cyber-terror attacks and warfare

Article 7 (Establishing comprehensive management plan for national cyber-terror attacks and warfare) : ① The Cyber Chairperson shall establish a comprehensive management plan for national cyber-terror attacks and warfare in accordance with the provisions specified by the Presidential Decree, and then prepare cyber-terror attacks and warfare management guidelines and a response guide to distribute them

to the head of responsible authorities. ② The head of responsible authorities shall establish and enforce detailed guidelines and response guides in accordance with the cyber-terror attacks and warfare management guidelines described in above ①.

Article 8 (Confirmation and report of enforcing the cyber-terror attacks and warfare management guideline) : ① The head of central administrations can check performance of the detailed guide specified in Article 6-2. ② The head of central administrations can inspect and assess performance of the particular guides specified in Article 6-2 for the responsible authorities specified in Article 2-1 (5-1). The head shall generalize the assessment with the result described in above ① to report it to the president, and the result to the National Assembly. However, inspection and assessment of the National Assembly, the courts, the Constitutional Court of Korea, and the Central Election Management Committee (CEMC) shall be the case that the Secretary-general of National Assembly, the Minister of National Court Administration, the Secretary-general of Constitutional Court of Korea, and the Secretary-general of CEMC request the Cyber Chairperson to do the same. ③ The provisions concerning the procedure and method of above ① and ② shall be specified by the Presidential Decree.

Article 9 (Building and operating Cybersecurity Response Center) : ① The Cyber Chairperson shall build a system for detecting and analyzing cybercrime information to provide weakness information against cyber-terror attacks and cyberattack origin information, cyberattack analysis and response technology information. The Cyber Chairperson shall build and operate a cybersecurity response center (“Cybersecurity Center”), and commit the tasks to the Cybersecurity Center built and operated by the following authorities for cooperation. However, the Analysis Information Sharing Center according to the provisions in Article 16 of the Information and Communication Infrastructure Protection Act shall be regarded as the Cybersecurity Center. 1) NIS 2) Involved central administrations (involved authorities including Ministry of Education, MSIP (Korea Internet & Security Agency), Ministry of Justice (Supreme Prosecutors’ Office), MND (Republic of Korea Joint Chiefs of Staff, Cyber Command), Ministry of Government Administration and Home Affairs (National Police Agency), Ministry of Trade, Industry and Energy) 3) Cybersecurity control service providers specified in Article 2-1 (6-5) ② The Cyber Chairperson shall immediately report the detected cyber-terror attacks and warfare information to the president, and provide the information to the head of related central administrations. The Cyber Chairperson shall generalize and analyze the information to establish countermeasures and respond to the attacks. ③ The information provided according to the provisions specified in ② shall be properly used for cyber-terror attack and warfare management within the required scope. ④ The Cybersecurity Center shall be operated by each authority, in cooperation with the Cybersecurity Committee. ⑤ The standard for building and operating the Cybersecurity Center and managing security, the scope, procedure and method of providing cybercrime, terror attack and warfare information shall be specified by the Presidential Decree.

Article 10 (Response activity) : ① The Cyber Chairperson shall take immediate action to minimize damages by detecting and analyzing cyberattack information to block, respond to and prevent potential cyber-terror attacks and warfare. ② The Cyber Chairperson can request the head of involved central administrations and the president to provide required support to do the job described above in ①. ③ The head of involved central administration and the head of Cybersecurity Center shall take required measures, for example, providing human resources and technology, for quick response when they are requested to provide the support described in ②.

④ The head of involved central administrations and the head of Cybersecurity Center can request the head of relevant support authorities to provide necessary support for taking measures described in ③, and it is essential to notify the head of support authorities of the details and period of support in advance. ⑤ The head of involved central administrations and the president can provide required expenses to the head of administrations who request them to provide support according to the provisions described in ④, and the provisions required for the procedure and method of required expense support shall be specified by the Presidential Decree.

Article 11 (Investigation of incident) : ① The head of responsible authorities shall take immediate measures for analysis of causes, investigation of incidents, recovery and prevention of damage spreading if the damage level caused by cyber-terror attacks is critical. If cyber-terror attacks and warfare are suspected, the Cyber Chairperson shall quickly investigate the incident in cooperation with private, public and military organizations, immediately report the result to the president, and notify the head of central administrations of the result. ② The president can order investigation of the incident if he/she decides that the result of incident investigation according to the provisions described in ① is not satisfactory or the incident has a significant effect on national security and interests. ③ When the investigation of incidents according to the provisions described in ② reveals quick correction is required to recover from the damages and prevent the damages from spreading, the president can order the Cyber Chairperson and the head of central administrations to take required actions. In this case, the head of responsible authorities shall comply with the Cyber Chairperson's request if there is no special reason. ④ Nobody is allowed to delete, corrupt, or modify the data related to cybercrime terror attacks, warfare and cyberattacks before completing investigation of incidents according to the provisions described in ① and ②.

Article 12 (Training) : ① The government shall carry out training human resources as provided in the response guide for systematic efficient response to cyber-terror attacks and warfare. ② The training described in ① can be carried out regularly or irregularly every year, and the regular training can be carried out in parallel with the training for emergencies according to the provisions described in Article 14 of ' Emergency Resources Management Act'. ③ The provisions required for the method and procedure of training described in ① shall be specified by the Presidential Decree.

Article 13 (Issuing cyber-terror attack warning) : ① The government can comprehensively review Cyber Chairperson ' s request and the collected information for systematic preparation and response to the cybercrimes and 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). ② The Cyber Chairperson shall order the Cybersecurity Committee to take measures for minimizing the damages and recovering therefrom if cyber-terror warnings (at least step 3) according to the provisions described in ① are issued. ③ Provisions required for the procedure and standard of issued cyber-terror attack warnings and measures by the head of responsible authorities shall be specified by the Presidential Decree.

Article 14 (Organizing cyber-terror attack response center) : ① The government can organize and operate a cyber-terror attack response center (" Terror Response Center ") with integrated national capacity to take measures, for example, analyzing causes, investigating incidents, taking emergency response, and recovering from damages if cyber-terror warnings (at least step 3) are issued. ② The

head of Terror Response Center (“ Terror Response Center Head”) shall be appointed by the Cyber Chairperson or the government, and provisions required for organization and operation of the Terror Response Center shall be specified by the Presidential Decree. ③ The Terror Response Center Head can request the Cyber Chairperson and the head of supporting authorities to provide required human resources and equipment in order to organize and operate the Terror Response Center according to the provisions described in ①. In this case, the head of supporting authorities shall comply with the request if there is no special reason. ④ The Terror Response Center Head can provide required expenses to the head of authorities providing human resources and equipment according to the provisions described in ③.

Article 15 (Technology research, development and transfer) : ① The head of central administrations and the president can take measures for developing technology and equipment and improving technology required for tackling cyber-terror attacks and warfare. ② The president can specify any research institute as an institute for technology research, development and transfer by organizing it according to the provisions described in ① or in connection with education, research and security institutes and groups. ③ The provisions for procedure and method for researching, developing and transferring cyber-terror attacks and warfare management technology shall be specified by the president.

Article 16 (Training and securing specialized human resources) : The head of involved central administrations shall create national cyber safety infrastructure and be prepared for cyber-terror attacks and warfare to take following measures in order to train and secure human resources specialized in cybersecurity. 1) Train and secure specialized cybersecurity human resources. 2) Train human resources for researching and developing cybersecurity related technology. 3) Train human resources for cybersecurity in connection with middle schools, high schools, graduate schools, universities, military forces, training centers, government authorities, public organizations, enterprises, private, public and military research institutes.

Article 17 (Analyzing, sharing and spreading information) : The responsible authorities with specialized human resources for tackling cyber-terror attacks and warfare and having developed cybersecurity technology and equipment shall analyze information, and those not equipped with the aforementioned technology and equipment shall share and spread information with the other authorities, and exert the right of information investigation, and information request. The provisions for this process shall be specified by the Presidential Decree. 1) Cyber-terror attack-related investigation and analysis right 2) Cyber-terror attack-related information sharing right 3) Cyber-terror attack-related information request right.

Article 18 (Global cooperation) : The government can carry out the following tasks to enhance cooperation with international organizations, groups and other countries in order to identify the origin of and respond to cyberattacks from other countries. 1) Build a mutual cooperation system for tackling cyber-terror attacks and warfare. 2) Exchange information concerning cyber-terror attacks and warfare tackling technology and perform joint response. 3) Dispatch and training human resources in charge of tackling cyber-terror attacks and warfare.

Article 19 (Duty of confidentiality) : A person who is engaged or was engaged in tasks of tackling cyber-terror attacks and warfare according to the provisions described in this Act shall use the secrets known through his/her work justifiably, and shall not use them for other purposes than his/her work or disclose them to other people.

Article 20 (Prize) : ① The Cyber Chairperson can award a prize to any one of the following persons in relation to cyber-terror management and warfare, and give a reward as long as the budget allows. 1) A person who provides information about cyberattack attempts 2) A person who reports details of cyber attackers. 3) A person of significant merits for detecting, analyzing, responding to, and investigating cyberattacks, recovering from damages by the cyberattacks and establishing policies. 4) A person who incapacitated cyberattacks. 5) A person who contributes to cybersecurity, technology development, training and system development. ② Provisions required for rewards, .the standard of rewards, method and procedures of giving them, and specific amount thereof according to provisions in ① shall be specified by the Presidential Decree.

Article 21 (Penal regulation) : A person who falls under any of following categories shall be subject to imprisonment not longer than 5 years or a fine not more than 90 million won. 1) A person who violates the provisions described in Article 11-4 (Investigation of incident) 2) A person who violates the provisions described in Article 19 (Duty of confidentiality)

Supplementary Provisions : Article 1 (Date of enforcement) This act shall be in force on and after the date when six months from the date of promulgation elapse.).

5. Conclusion

Although increasing cyber-terror attacks and cyberwarfare threats cause tangible and intangible damages, Korea does not have established regulations and procedures to systematically tackle cyber-terror attacks and cyberwarfare on a national basis. National Cybersecurity Act aim to build a general national action system by private, public and military organizations, detect cyber-terror attacks in advance to block potential cyber-terror attacks and warfare early and integrate national capacity for fast action if they occur.

I 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.

Acknowledgments

"This research was supported by the Academic Research Fund of Hoseo University in 2015"(No. 2015-0107).

References

[1] D-woo Park, "National Cybersecurity Policy Report, Forum of National Cybersecurity Policy", National Assembly, Dec. 31. **(2012)**.
[2] D-woo Park, Analysis on Mobile Forensic of Smishing Hacking Attack, INFORMATION, vol.17, no. 11(B), Nov. **(2014)**, pp. 5683-5688.
[3] D-woo Park, "Analysis on Mobile Forensic of Smishing Hacking Attack", Journal of the Korea Institute of Information and Communication Engineering, vol. 18, no. 12, Dec. **(2014)**, pp. 2878- 2884.
[4] D-woo Park, Analysis of Internet Banking Security Crack through Messenger Hacking, Future Information Communication Technology and Applications, Communications in Computer and Information Science, (2011. 9. 22)
[5] D-woo Park, "Analysis of Acts for Cybersecurity", Military Forum, no.75, Nov. **(2013)**.
[6] D-woo Park, "Enhancement of Cybersecurity Capacity", Workshop for Information and Communication Security Officers, Office of ICT Management & Equipment of National Policy Agency, Nov. 19,**(2014).**

[7] D-woo Park, National Cybersecurity Act(Proposal), Forum of National Cybersecurity Policy, National Assembly,May 14 **(2013).**
[8] D-woo Park, "Forensic Analysis Technique of Car Black Box", International Journal of Software Engineering and Its Applications, vol. 8, no. 11, Nov. **(2014)**.
[9] D-woo 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, June **(2013)**, pp. 1360-1364.
[10] J. Shin, D-woo Park, "A User' s Guide for Countermeasures against Smishing Incident", Information-An International Interdisciplinary Journal(International Information Institute: vol 17. no. 11(B), Nov. 30 **(2014)**.

Author

Dea-woo Park, he is an Associate Professor at Hoseo University in South Korea. Professor Park researches 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. 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.

