2017 2(2) 11-14
Submission: 2017/11/10, Peer review: 2017/11/20, Accepted: 2017/11/25, Published: 2017/12/30

International journal of protection, security & investigation

Publication state: Japan
ISSN: 2423-8368

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: skcho@ikw.ac.kr

Peer reviewer
E-mail: editor@j-institute.jp

http://dx.doi.org/10.22471/protective.2017.2.2.11

Response of KOREAN Private Security against North Korean CYBER TERRORISM

Son Man-sik[1]

J-INSTITUTE, Kawasakishi, Republic of Korea

Jo Sung-gu[2*]

Kyungwoon University, Gumi, Republic of Korea

Abstract

Everyone in Korea uses smartphones and fast internet is available everywhere. The settlement of IT(Information Technology) living zone has led to high reliance on information communication, which poses a possible threat to the infringement of information communication.

In Korea, however, cyber attacks by North Korea have been found to be the largest among the infringements, and the amount of damage is said to be more than 1 trillion won.

Recently, cyber terror attacks by North Korea have threatened the information networks of private companies as well as major systems of the nation with increasing frequencies. However, the Korean government has limited capabilities to cope with such treats in the cyberspace in terms of manpower, time, and cost.

In order to overcome the limitations of the Korean government, an institutional system to guarantee the security of the cyberspace of Koreans is needed through the countermeasures of private security that is expanding the scope of civilian security more broadly in areas where the national influence does not reach.

Therefore, this study has begun with the need to discuss countermeasures to the cyber threats not only by the government but also by the private sector, after being confirmed the fact that South Koran bitcoin companies were hit by attacks linked to North Korea hackers recently and which was covered by the major news media around the world.

[Keywords] ***North Korea, Cyber Attack, Hacking, Bitcoin, South Korea***

1. Introduction

1.1. The need for study

Today, cyber attacks by North Korea are becoming more sophisticated and threatening the South Korean economy and society. Now, North Korea's cyber-attack capabilities are analyzing vulnerabilities on government agencies, financial institutions, media companies, and private companies in neighboring countries and making continuous and systematic attacks with detailed plans and various methods.

In addition, the type of attack is transformed into the form of promoting social disturbance and the cyber warfare among nations which is beyond the purpose of personal information leakage and financial gain acquisition, organizing the characters of terrorism that threaten social safety.

North Korea has been aware of the importance of cyber-power in the modern war and has been training excellent cyberspace experts each year in preparation for a full-scale cyber warfare ever since it observed the Gulf War in 1991[1]. Through this trained professional workforce, it is constantly threatening the cyberspace of South Korea. As the bitcoin market in South Korea has been expanding recently, the suspected hacking attacks in this area posed by North Korea have

*Funding Agency: This work was supported by Kyungwoon University Research Grant in 2017.

been confirmed. Thus, this study is to investigate effective countermeasures through the multifaceted approach of private security to solve the problems of cyber attacks by North Korea, which have been suspected in the meantime.

1.2. Preceding studies

There are preceding researches on the countermeasures of private sector against cyber terrorism of North Korea, including the topics of construction of civil cooperation system, fostering cyber security personnel, consulting work on cyber crime, expansion of private security business area, introduction of detective system, summarized in the following <Table 1>.

Table 1. Preceding studies.

Researcher	Contents
Shin (2016)	Seeking introduction of private investigation system through utilizing a national and private partnership for cyber crime[2].
Kim & Lee & Jang (2014)	Discussions on how to use private investigators in accordance with the situation in SNS era by analyzing the actual situation of terror crime[3].
Kim & Cho (2013)	Suggesting cyber crime prevention scheme using private expense and private resources, in addition to the efforts of the police to take measures against cyber crime[4].
Choi &·Ryu (2012)	As countermeasures against cyber terrorism in North Korea, proposing measures for building legal and institutional aspects, technology and operational aspects, international cooperation system and civil cooperation system[5].

2. North Korean Cyber Terrorism Cases

North Korea, currently, has been providing professional training courses on cyber terrorism at Kim Il-Sung University, Kim Chaek University of Technology, and Pyongyang University of Computer Technology since the 1990s, utilizing about 6,800 manpower to disturb the international community including South Korea through making use of cyberspace. In addition, the North Korean army is ranked fourth in the world after the US, China, and Russia in the field of cyber terrorism, which is regarded as a new threat to the international community.

North Korea is suspected of carrying out the most of attacks occurred in South Korea by its identified features of cyber terrorism until recently, maintaining consistent attack methods through using the DDoS attack or ATP attack to collect the information for social disorder ultimately. Since North Korea has obtained information on the South Korean society based on cyber terrorism for a long time, there is always the possibility of carrying out large-scale cyber terrorism based on APT[6].

Such cyber terrorism by North Korea continues to occur after the spread of the Internet, and it is gradually becoming more advanced. <Table 2> lists the representative cases of cyber terrorism turned out to be the acts of North Korea.

Table 2. North Korean cyber terrorism cases.

Serial number	Division	Contents
1	7·7 Didos attack	- July 7, 2009 - Government agencies such as Cheongwadae

2	3.4 Didos attack	- March 4, 2011 - Government agencies, Financial institutions, Internet companies
3	Nonghyup computer network paralysis	- April 12, 2011 - Financial institutions targeted
4	Hacking the Joongang daily	- June 9, 2012 - Media targeted
5	3.20 cyber terror	- March 20, 2013 - Broadcasting, Financial institutions targeted
6	6.25 cyber terror	- June 25, 2013 - Government agencies and media targeted

3. North Korean Cyber Terrorism and Countermeasures of South Korean Private Sector

The Korea Internet and Security Agency (KISA) is an Internet and Information Security Promotion Agency, established for the purpose of promoting the advancement and safe use of information and communication networks, analyzing the dysfunctions caused by the use of information and communication networks, and the management of Internet Address Resource based on Article 52 of the 「Act on Promotion of Information and Communication Network Utilization and Information Protection, etc.」. The KISA provides services to prevent and respond to cyber-infringement accidents in the private sector, to protect personal information and respond to the damage, to deal with the tasks of information protection industry and human resources, to carry out nationwide service for information protection, country domain(.kr/.Korea) service, and the grievances related to illegal spam. Especially, to prevent and respond to internet infringement, it monitors unusual signs of the Internet in real time, builds and operates a DDoS response system and cyber shelter, monitors key vulnerabilities and distributes security advisories, and prevents and responds to people's damage to electronic financial fraud such as phishing, pharming, smishing.

The Korea Internet Security Center(KISAC) is an organization under the KISA to prevent the internet infringement in the private sector in advance and respond rapidly in case of Internet accidents by curbing the spread of damage. It is conducting the activities such as prevention of computerized network infringement accidents, supporting the handling of infringement incidents, and participating in international accident response activities as a representative institution of South Korea. In addition to these, through the operation of the general situation room, it monitors abnormalities in Internet traffic 24 hours a day and 365 days a year in connection with major domestic telecommunications operators and security control companies and collects and analyzes information on security threats, such as security vulnerabilities and malicious codes, and shares information with domestic and overseas institutions on an ongoing basis, minimizing social and economic losses due to infringement accidents through rapid collaborative countermeasure[7].

4. Discussion

The security agenda since the Cold War in 1989 has begun to widen its concept to comprehensive security in the international community, whose representative type is cyber terrorism. Currently, the United Nations and other international communities are gathering opinions for taking an action against terrorism, but the number of terrorist attacks and the scale of damage is increasing.

Recently, the number of cyber crimes according to the statistics of the Korean National Police Agency(2016) has increased by

221.6% from 77,099 in 2004 to 155,366 in 2013. The number of arrests, however, increased about by 135.8% from 63,384 in 2004 to 86,105 in 2013. As a result of stern crackdowns, the number of cyber crime seems to have been declining a bit since 2010, which had been in a steep rise trend, this cannot be assured that cyber crime has been reduced only by a decline from the previous year due to the nature of cyber crimes that are very sensitive to the flow of society.

The demand for police service against cyber crime is continuously growing, In order to improve the quality of police service, it is imperative to take preventive measures such as detecting the sign of the occurrence of cyber terrorism and removing it for the large-scale crime in the cyberspace, rather than post-response, which takes defensive measures after the occurrence of an incident. However, it is the fact that there are limitations in terms of human, time, and economic problems to cope with the threat of cyberspace at the national level.

5. References

5.1. Journal articles

[1] Kim YH. A Case Study on the Cyber Terrorism of North Korea against South Korea. *Korean Terrorism Studies Review*, 7(2), 5-21 (2014).

[2] Shin HJ. A Study on the Private Investigator Usage for Cyber Crime. *Korean Security Science Review*, 46, 63-86 (2016).

[3] Kim HD & Lee KS & Jang DS. A Study on the Usage of the Private Investigator by Change for Terrorism in the Era of SNS. *Korean Terrorism Studies Review*, 7(2), 22-48 (2014).

[4] Kim SW & Jo HB. Prevention Methods of Cyber-crimes Using the Private Security. *The Journal of the Korea Contents Association*, 13(3), 141-151 (2013).

[5] Choi SW & Ryu CH. A Study on the Cyber Terrorism of North Korea. *Korean Associatin of Public Safety and Criminal Justice Review*, 46, 212-239 (2012).

[7] Kim TK. Institutional Issues and the Corresponding Measures of Crime Cyber Terrorism. *Journal of Law and Politics Research*, 14(3), 1337-1381 (2014).

5.2. Thesis degree

[6] Kwon YJ. Study on North Korea's Cyber Warfare Capability and Response Strategy of South Korea. Korea University, Master's Thesis (2014).

Lead Author
Son Man-sik / J-INSTITUTE Specialized Researcher
B.A. Kyoungwoon University
M.A. Kyoungwoon University
Ph.D. Kyungnam University

Research field
- North Korea's Cyber Attack: Terror Cases and Cyber Capabilities and Current State of Affairs of North Korea's Cyber Terror Force, International Journal of Military Affairs, 1(2) (2016).
- Search of Security Level of National Industrial Complex in Republic of Korea: Focusing on Gumi Area, International Journal of Potection, Scurity & Ivestigation, 1(2) (2016).

Major career
- 2009~2011. Republic of Korea Navy, Military Police.
- 2015~present. J-INSTITUTE, Specialized Researcher.

Corresponding Author
Jo Sung-gu / Kyungwoon University Assistant Professor
B.A. Kyungwoon University
M.A. Kyungwoon University
Ph.D. Kyonggi University

Research field
- China's Economic Growth and the Role of Criminal Justice Agency a Comparison between Ministry of Public Security of the People's Republic of China and the National Police Agency of Korea, International Journal of Justice & Law, 1(1) (2016).
- The Recognition of Koreans in Air Terrorism and Crime Outbreaks in Northeast Asia, International Journal of Criminal Study, 1(1) (2016).

Major career
- 2012~present. Kyungwoon University, Professor.
- 2015~present. J-INSTITUTE, Chairman.