Journal of The Korea Society of Computer and Information
Vol. 21 No. 6, pp. 89-96, June 2016
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2016.21.6.089

Review on improving measurement of cyber terror management system

Jong-Ryeol Park*, Sang-Ouk Noe**

Abstract

Damage and attack size of cyber terror is growing to the national size. Not only targeting at a certain companies or individuals but number of cyber terror targeting government bodies or unspecific people is increasing. This is because compared to traditional weapon, input cost is very cheap but ripple effect and shock are much stronger, affecting not only certain groups but also each individuals.

'Anti-terror measurement for protection of nation and public safety' passed last month is one of the renowned measurement passed regardless of objection from opposition party. The opposition party went against this through filibuster for 192 hours but this finally passed National Congress due to lack of oppositions.

Korean government is taking post actions after passage of anti-terror measurement. Legislation of enforcement ordinance and regulations is due by 6th of next month. This regulation will be executed from June 4th after legislation.

Whenever there is any security issues such as hacking of Korea Hydro and Nuclear Power and National Intelligence Service happens, lot of attention is made to those hackers. However, social recognition or management of those hackers need lot more improvement. Especially, as market of internet of things is increasing, there is an increased anxiety on information security. But as we only rely on security solutions, this problems are keep happening. Therefore, active investment on nurturing hackers who play the role of 'spear and shield' shall be made. Government should put more efforts to allow white hackers to show their abilities. We should have a policy for supporting high-quality programs such as BoB. To make information protection industry into future growth engine, it is necessary to nurture professionals for information protection and white hackers through special programs.

Politicians should make related regulations as soon as possible to remove factors that prevent swift management of cyber attack due to lack of legislation. Government should pay lot more financial investment to nurturing professional manpower than now. Protecting life and asset of nation is responsibility and duty of our government. We all should recognize that controlling cyber attack is a part of national defense.

▸Keyword : cyber terror, white hacker, anti-terror measurement, cloud

• First Author: Jong-Ryeol Park, Corresponding Author: Sang-Ouk Noe.
*Jong-Ryeol Park(park3822@kwu.ac.kr), Kwangju Women's University, Professor.
** Sang-Ouk Noe (nosang2424@daum.net), Joongbu University, Professor
• Received: 2016. 05. 30, Revised: 2016. 06. 07, Accepted: 2016. 06. 20.

Ⅰ Introduction

We are living in a hyper-connected society, a society that is very closely linked by mobile and social network service (SNS). At the end of year 2014, the number of internet users reached 3 billion people and 7 billion people have registered to mobile communication service (International Telecommunication Union, ITU). There are more than 4.2 billion internet protocol (IP) addresses. The internet user rate in Korea is 82% along with 77% of distribution rate of high-speed internet, making it to be one of the top internet countries (Wall Street Journal). However, the fact that Mr. Kim disappeared in Kilis, Turkey had a contact with IS recently through SNS was a shocking news to the nation. Starting from this year, related organizations were busy with checking cyber security around the world.

As number of people using mobile payment is increasing, there will be more hacking attempts to mobile devices, Internet of Things (IoT) that are on all the time. This means that IoT, enabling exchanging of information between devices connected to the internet may turn into Internet of Threat (IoT). Dick Cheney, The Vice President of America halted remote controlling function of cardiac pacemakers in body in 2007 with worries of hacking. There are different types of cyber attack. For example, Hacktivism is leaking information of shutting down a website, cyber crime of stealing money from financial organization or individual and cyber spy of stealing industrial confidentiality. What is more, FBI defined cyber terror as 'a behavior of attacking computer system, program, and data for political purposes to bring a violent result.'

This research tries to draw status of cyber terror in Korea and its improvement measures as well as ways for enhancement.

Ⅱ. Status of cyber terror incidence in Korea and its improvement measures

1. Status of cyber terror incidence

The first cyber terror in Korea took place on the 25th of January 2003. It is also called as 125 Internet Chaos but this incidence was not an attack made by a certain group to paralyze internet network in Korea. It's actually closer to an accident that happened to internet service provider (ISP) which provides domain name service but did not update security patch properly.

As this is the case, it is more reasonable to consider "hacking of national organizations" in 2004 as the first cyber terror in Korea. This incidence became known when a researcher working in defence organization reported saying that he received a weird E-mail from an unknown person working in armament industry. Looking at it in more details, there was a Microsoft Word file attachment in the E-mail and it was set to activate virus program once the file is opened.

The function of this virus program was to outflow confidential document files installed in the computer and through this method of faking the sender, 222 computers in 10 public organizations including National Congress and Korea Atomic Energy Research Institute and 79 computers in private system were hacked. From 2005 to 2008, there were various hacking incidents or DDoS attack, however, all of them had financial purpose of stealing money by incapacitating all the services and nothing related to cyber terror. Since then, starting from 2009, 1~2 times of cyber terror accidents are happening every year. One of the well-known terrors include 77DDos (2009), 34DDos (2011), NH Bank hacking (2011), and Joongang Daily (2012). Nevertheless, cyber attack in 2004 is quite different from 'hacking of national organization.'

First of all, from subject of attack, those systems operated by government and military were the main targets but from '77DDoS incidence' this even included fraud towards financial organizations and IT companies. Especially, computers used by civilians were also attacked. In terms of networks involved in the attack, 'hacking of national organizations' was limited to few countries such as Korea, China, and America. However, from '77DDoS' server and computers used around the world were abused (77DDoS-61 countries, 34DDoS-70 countries). From method of attacking, in contrast to secret and private attack where targets did not realize that confidential information was hacked in this 'hacking of national organizations,' from '77DDos' they applied public methods such as DDoS attack or changing website. What is more, once attack is finished, they used zombie PC or destroying middle computers to avoid tracking.

Although 'hacking of national organizations' only resulted in information leakage but from '77DDoS' not only information was leaked but also service and hard disk were damaged. [1]

2. Improvement system for cyber terror

For controlling cyber terror in Korea, private sector is cared by 'internet attack control center' operated by Korea Internet & Security Agency and public sector is controlled by 'national cyber security center' in National Intelligence Service. The 'cyber headquarter' under Defense Intelligence Agency is a comprehensive control system across private, public, and military for military sectors. Different from this, National Police and Prosecution Service are also in charge of crime investigation for cyber terror.

3. Re-establishment of function and role

There are various regulations for cyber terror; Act of Information and Communication Promotion, Act on the Protection of Information and Communications Infrastructure, E-Government Act, and National Cyber Security Management Regulation. Sometimes, duties and responsibilities of organizations overlap. Therefore, although many organizations control cyber terror, when actual cyber threat happens, responsibilities and roles of each organization become unclear [2]. As this is the case, police should actively involve in the accident from the initial stage to accurately clarify the truth and inform this to the related department right after. A close cooperation system for this process shall be established.

III. Problems of current management system for cyber terror

1. Confusion in management system due to initial control and various regulations

1.1 Lack of systemized regulations

Characteristics of cyber terror is that it is hard to identify whether it is an individual, group of country in its initial stage. Therefore, it is not easy for military of information organizations to take a part from the beginning phase.

This perspective made a contradiction for investigators when 3.3 DDoS and 7.7 DDos turned out to be done by North Korea, not military investigation but regular investigators had to take the investigation. At the time, media criticized cyber headquarter that although those attacks were doubted to be done by North Korea, the organization was not able to carry out its role properly.

In consideration to problems of initial management, current regulations for managing cyber terror are made up of Act of Information and Communication Promotion, Act on the Protection of Information and Communications Infrastructure, and National Cyber Security Management Regulation (Order of President). Under system, Act of Information and Communication Promotion takes care of civil attacks, Act on the Protection of Information and Communications Infrastructure controls facilities based on information and communication, and lastly, National Cyber Security Management System is applied to management of information network of central government, local government, and public organizations. Such regulations are making them harder to have systematic management. In accordance to Article 3 of National Cyber Security Management Regulation, "this law is applied to information network of central government, local government, and public government organizations. However, in accordance of Article 8 of Act on the Protection of Information and Communications Infrastructure, such law does not apply to designated to main information and communication facilities." Management system for cyber terror in Korea is regulated by order of President and thus, roles and responsibilities between related organizations are unclear. Also, its binding force is very weak and has many limitations as it goes against to many upper regulations.

1.2 Lack of measurement system for initial threat

Threat in cyber space cannot be measured visually and it is also not easy for the government to access private system. Most regulations say that one should report to National Intelligence Service and Korea Communication Commission when there is cyber attack or infringement. However, these reports are not delivered to investigators and thus, cyber threat is not properly measured. As departments in charge of registering such infringement and cyber attacks are only focusing on prevention measurement, no threats are removed but just become latent.

1.3 Limitation of jurisdiction at initial stage of cyber attack

It is difficult to identify actual object of cyber attack in cyber space and therefore, it is not easy to confirm what kind of attack this it. That is, one can hardly find out whether subjects of cyber terror is individual, organization, or country at the initial stage. Therefore, it becomes more difficult for military of government organizations to participate in investigation without clearly knowing the subjects of cyber terror. In contrast, one advantage is that regardless of subjects of attack, any investigation organizations can be involved. The criminals of 7.7 DDoS attack and 3.3 DDoS attack in 2009 were turned out to be North Korea, however, this report was made based on tracking and investigation of regular investigator instead of military.

Based on this, regulations and comprehensive measurement related to cyber terror management mainly have explanations about roles of National Intelligence Service and Korea Communications Commission. There are no detailed information on roles of investigators. In contrast, in accordance to The National Strategy to Secure Cyberspace reported in 2003, "legal bodies and organizations for national security play an important role in preventing attack of cyber space and legal bodies are in charge of determining rights of criminal jurisdiction. Thus, legal bodies play an important role in determining jurisdiction of attack and this implies that role of legal bodies are considered important in America [3].

2. Limitation of cooperation of information organizations and lack of participation of legal bodies

Cyber terror is directly related to cyber security issues. However, in case of Korea, government organizations are participating in policy implementation. This leads to i) policy competition between organizations, ii) limitation of information share, iii) lack of legal foundation of information organizations, iv) lack of competence for international cooperation. Therefore, there will be many problems and limitations unless smooth cooperation network is made,

For controlling national cyber crime and cyber security legal organizations play an important role. In Korean master plan for cyber security no roles of police is clearly defined. This problem leads to limitation in dynamic control of cyber security as one part of tracking and arresting is not included.

3. Limitation of swift control based on public, private, and military management

Subject of cyber terror is limitless of country, public, private, and national defence. Cyber terror takes place regardless of the scope and as this is dealt by function, it is difficult to have a swift management. There was a suggestion of control tower and security center in the Executive Office of President was established but still, there is a limit to policy control. It seems there needs to be a consideration of new departments such as Cyber Bureau and Cyber Security Bureau shall be considered.

Furthermore, as the nation leads the policy private sectors are negatively taking a part in this. Social motivation for private sectors to actively prevent cyber terror and obtain cyber security is lacking. Usually, prevention of offline crime is responsibility of police or patrollers and is regulated by law. In contrast, looking at the cases of KaKao Talk, POS device, and messenger fishing, online crime prevention changes system of a certain company to achieve the instant performance of crime prevention. That is, cyber terror is done on the internet network and if company or private sectors managing this network work closely together it will be much easier for them to prevent cyber crime [4].

Ⅳ. Improvement of management system for cyber terror in Korea

Regarding improvement of management for cyber terror in Korea many people are saying about establishment of control tower. Actually, a bill for having National Intelligence Service as a controller tower was submitted to the 18th National Congress and as of now, similar regulations are on the table. Following is the suggestion on directions of improving management system for cyber terror;

1. Clarification of concept of cyber terror

There is a necessity of clearly defining difference between cyber terror and regular infringement of personal information. Regulations related to information protection in Korea do not make a clear classification and thus,

confusion in duties and responsibilities of related organizations is resulted. Also, as it is highly difficult to divide cyber terror and regular infringement of personal information there is a high possibility of doubt in private sectors caused by national authority.

2. Indication of responsible organization in law and making solutions for its management

National Intelligence Service is in charge of implementing core function in managing cyber terror based on order of President 'National Cyber Security Management Regulation.' There is a problem of designating role of National Intelligence Service by Order of President instead of regulations when determining problems of infringement of national rights taking place in the process of handling cyber risk.

Therefore, after having a detailed social discussion, it is necessary to define roles and duties of responsible organizations by law. Along this with, under the control of responsible organization, practical policy solutions shall be implemented to nurture professional manpower for cyber security. If responsible body for cyber terror is established legally and institutionally, there is a possibility of having a very strong authority, as known as big brother as all both public and private informations are concentrated. As this is the case, systematic control for this is required. We might consider having an audit and report to assembly but details shall be defined in law clearly [5].

3. Establishment of professional system and national digital evidence laboratory

As management of cyber crime is focused on investigation after accident, there is a limit to prevention and effective management at the initial stage. Also, existing investigation basis on determination of personal experience, information, and intuition of individual investigator without any proper methodology. Although investigating organizations have a big data on crime but it is not easy to utilize these data and thus, analysis on crime is not made properly. Therefore, it is necessary to develop "professional system" to be used in investigation by analyzing a large amount of data to prevent cyber crime. For this, not only scientific investigational method such as profiling and data mining done across academic fields such as psychologist, criminologist, and jurist but also experiences of investigators shall also be combined to develop a comprehensive system. Currently, research on physical and biological evidence is done by National Forensic Service but no research on digital evidence is available. This means that no research center for managing national cyber terror exists. There should be a responsible organization for analyzing and researching different digital evidences including hacking and malignant code.

4. Nurturing of cyber terror professionals

Recently, number of discussion on cyber crime and terror in international organizations such as UN, OECD, ITU, and INTERPOL has increased. Therefore, cyber terror investigation is based on international cooperation and it is not easy to have a quick investigation if professionalism on technologies such as hacking and DDoS and foreign language skills are not good enough. Therefore, to nurture professional investigator for cyber terror, lot of efforts shall be made to train a specialist through middle to long term professional training such as global education. If necessary, graduate school course shall be made in universities to have systematic and comprehensive education. It is also important to raise professional for international cyber crime who can participate in decision making on behalf of Korea police.

5. Establishment of non-destructing computer environment - Cloud

Cloud is a technology that enables use of other computers connected by internet instead of having self computer for processing necessary data. It can also be defined as distributed processing by using virtual machine [6].

Actually, cloud is not a new type of computer. When computer first appeared with a high price, it utilized Dummy Terminal, which is for processing input and output data and this data was sent to big computer in IT center for further processing. This is a very similar method to today's cloud system. The 'virtual' in the definition of cloud means dividing one computer server into small servers to enable processing of many tasks at once. If used properly, effective use of server is allowed and can have efficacy of utilizing various computer servers at a low cost.

These technologies are called cloud IaaS, Paas, and HaaS. This technology allows convenient use by turning computer server and different hardware into software.

This operates computer server two to three times to enable automatic operation of back up computer when one computer goes out of order. It is referred to as virtual machine and it can be considered as a completely independent computer that operates inside the computer. Adopting this can have an efficacy of having many computers at a cost of using one computer. As many virtual computer servers can be made from one computer server one can have separate operation from server computer for routine operation and back up computer server that runs automatically in a emergent situation.

Building 'non-destructing computer environment' with this technology will be the right solution for managing cyber terror. This means having computer server group by functions such as server computer, database server, etc. Also, cloud virtual machine with various hardware cloud is made and 'console controller' for managing the whole computer environment is built. This computer environment allows automatic turning and recovery of data. This environment enables automatic turning to backup system by 'console controller' when cyber attack takes place and thus prevents total down of system regardless of any cyber terror. If computer environment is established by using this cloud virtual machine, installation of software required for data processing in the computer as well as regular updates are not required.

6. Nurturing of white hackers

Ministry of Science, ITC, and Future Plan has announced a plan of designating young hackers with high grades in global and Korean hacking prevention competition as staff of cyber headquarter and police cyber investigation in November. This is the post process to 'K-ICT strategy' reported in last March and a part of comprehensive security solution of private, public, and military to deal with external hacking threat.

Military cyber headquarter has selected 60 special manpower for information protection last year and police also hired 14 staff for security work for the first time. Those people either completed 'next generation security leader' training course by KITRI or have experiences in club activities for information protection.

Even today, unseen hacking war among hackers of different nationalities is taking place in cyber space. Hackers have enhanced into an organization leading cyber space over crime level and carrying out invisible cyber attack to national organizations. Cyber attack is a scary existence harming relationship between countries or public benefits, more than just showing off their abilities and being.

In IT field, white hackers with outstanding security knowledge and professionals are considered as high quality manpower in other countries. Early August of last year, Korea 'DEFKOR' team has won the world's renowned hacking protecting competition called DEFCON CTF which first started from 1993. This is the achievement made by next generation security leader nurturing program called BoB implemented by Ministry of Science, ICT, and Future Planning from 2012 in cooperation with industry, academy, and institutes.

KISA and KITRI are implementing training to 2000 information security professionals every year and even made security-GYM, a practical training center for cyber security. An active review on policy of university entrance without exam for junior hackers (designation of special university for information protection) shall be examined.

Whenever there is an issue related to hacking like hacking of Korea Hydro and Nuclear Power and National Intelligence Service, lot of attention is made to the hackers. However, social service or recognition of those hackers need lot more improvement.

Nevertheless, market for internet of things is expanding and anxiety over information security is increasing as well but as we only focus on security solution security problem keeps taking place. Therefore, active investment in raising skills of hackers who play 'spear and shield' roles is required. Government should make an environment for white hackers to show their abilities freely. There should be a active supporting of high-quality programs such as BoB in the future. To improve information protection into future growth motivation, we should nurture professionals for information protection as well as white hackers through training programs.

Cyber war may be something that is more scary than traditional war or nuclear war where gun and cannon shooting takes place. It means that main national facilities-electricity, communication, transportation, financial network, oil pipe, gas pipe, and water system-can be destroyed all at once without any prior notice.

Ⅴ. Conclusion

With recent aggressive threatening from North Korea, South Korea has become the center of world news. Other countries are considering Korea to be in a dangerous situation for its high possibility of having a war. However, we are living in a routine without worries. Many people going to cherry blossom and road suffering from heavy traffic, nothing has changed from before.

Under this circumstance, 3.20 cyber terror that happened few weeks ago shocked our society. This kind of cyber terror happens often. Looking at 7.7 DDoS and 3.4 DDos, Korea was proud to be the leading IT company but these incidents tell us that our security concerns, social recognition, as well as individual security are at risk [7].

In fact, damage and attack size of cyber terror is growing to the national size. Not only targeting at a certain companies or individuals but number of cyber terror targeting government bodies or unspecific people is increasing. This is because compared to traditional weapon, input cost is very cheap but ripple effect and shock are much stronger, affecting not only certain groups but also each individuals.

'Anti-terror measurement for protection of nation and public safety' passed last month is one of the renowned measurement passed regardless of objection from opposition party. The opposition party went against this through filibuster for 192 hours but this finally passed National Congress due to lack of oppositions.

Korean government is taking post actions after passage of anti-terror measurement. Legislation of enforcement ordinance and regulations is due by 6th of next month. This regulation will be executed from June 4th after legislation.

Whenever there is any security issues such as hacking of Korea Hydro and Nuclear Power and National Intelligence Service happens, lot of attention is made to those hackers. However, social recognition or management of those hackers need lot more improvement. Especially, as market of internet of things is increasing, there is an increased anxiety on information security. But as we only rely on security solutions, this problems are keep happening. Therefore, active investment on nurturing hackers who play the role of 'spear and shield' shall be made. Government should put more efforts to allow white hackers to show their abilities. We should have a policy for supporting high-quality programs such as BoB. To make information protection industry into future growth engine, it is necessary to nurture professionals for information protection and white hackers through special programs.

Politicians should make related regulations as soon as possible to remove factors that prevent swift management of cyber attack due to lack of legislation. Government should pay lot more financial investment to nurturing professional manpower than now. Protecting life and asset of nation is responsibility and duty of our government. We all should recognize that controlling cyber attack is a part of national defense.

REFERENCES

[1] Haeseong Yoon, Seokgu Kang, Youngwoo Park, Minho Kim, Hyungyoung Kwon, Doseung Kim, and Kibeom Kim, Research on establishment of cyber security system, Korean Institute of Criminology 10-07, year 2010, p.67.

[2] Doseumg Kim, 'Legal work for managing cyber risk: around status and implication of cyber risk management in America' Korea Communication Policy No. 21 Volume 17, Korea Information Society Development Institute, 2009.

[3] Kibeom Kim, Yoonsik Jang, 'Investigation of Cyber Crime', Korean National Police University, 2012.

[4] Haeseong Yoon et al, 'Research on trend of cyber terror and its management'. Korean Institute of Criminology, 2012.

[5] Recent paralyzing of data processing network and improvement of managing measurement of cyber terror, issues and discussions of National Assembly Research Service, 2013. 04. 18.

[6] One of solutions to solving cyber terror, cloud, Digital Times, 2013. 04. 17.

[7] Effective solution to cyber terror, Financial News, 2013. 04. 16.

Authors

Jong-Ryeol Park received the Ph.D. degress in Laws and Civil Law from Chosun University, Korea, in 2001, 2006 respectively. Dr. Park joined National Communication Ombudsman District Prosecutors' Office in Gwangju in 2009 and was a member of Metropolitan Police Agency Administrative Disposition of a Driver's Licence Review Committee in Gwangju in 2010. Also he was Policy Advisers in Gwangju.Jeonnam Regional Military Manpower Administration. He is currently a professor in the Dept. of Police & Law at Kwangju Women's University. He is interested in Civil Special Act and Registration of Real Estate Act.

Sang-Ouk Noe received the Ph.D. degress in Police Studies from Wonkwang University, Korea, in 2015. Voluntarily resigned from human resources department of Posco Gwangyang steel mill in 2008 and worked as professor for industry-academy cooperation in Gangneung Wonju National University and Cheonnam National University, trying to promote employment and field practices. Since 2015, I have been working as an assistant professor in Police Law Department of Joongbu University.

Furthermore, I was designated as a professional member of Korea Industry Commercialization Association in 2014.