The Korean Journal of Defense Analysis
Vol. 30, No. 3, September 2018, 437－454

The Countermeasure Strategy Based on Big Data against North Korean Cyber-attacks

Yong-joon Lee, Hyuk-jin Kwon, Jae-il Lee, and Dong-kyoo Shin*

DSI; KIDA; KISA; Sejong University, Seoul, Republic of Korea

North Korea is enhancing its cyber-attack capability, as an asymmetric weapon, and the threat of North Korean cyber-attacks is continually increasing, as seen in the example of the cyber-attacks against South Korea within four months of a nuclear experiment. The analysis of the trends and characteristics of North Korean cyber-attacks in the last decade showed that the attacks had been intellectualized, complex, and objective–oriented, so there is a need for a national countermeasure that is more systematic than previous actions. More importantly, a nationwide cyber-attack prediction system that collects information about North Korean cyber-attacks should be established to detect and take actions against cyber-attacks in the early stages. Early prediction and prevention are possible with such a system, so it is necessary to prepare for a big data-based integrative analysis system. To do this, domestic and foreign cyber security teams must collect the cyber-attack information and malicious codes North Korea has produced. The collected information should be shared according to international standards, and thus we can predict North Korean cyber-attack strategies using the large amount of collected information. Based on the predictions, we can change our countermeasure strategy from that of a reactive one to a preemptive one by preparing response measures against North Korean cyber-attacks.

Keywords: North Korean Cyber-attacks, Countermeasure Strategy Based on Big Data against Cyber-attacks, Cyber-attack Information-sharing

Introduction

North Korea is continuously delivering cyber-attacks using cyber weapons, which are a form of asymmetrical weapons. They have about 1,700 highly specialized hacker troops that have gone through an intense training process. Moreover, South Korea has a high

* E-mail: shindk@sejong.ac.kr (corresponding author)

ISSN 1016-3271 print, ISSN 1941-4641 online

http://www.kida.re.kr/kjda

dependency on its information system to perform most of its daily tasks. Therefore, the North Korean cyber-attacks targeting the Korean information system are predicted to be more sophisticated.

Information-sharing among the private, military, and administrative sectors, as well as the cooperative system with overseas institutions are necessary to deal with the increasing threats from North Korean cyber-attacks. Moreover, upon international cooperation and information-sharing, responding to cyber-attacks based on big data is essential in preparing preemptive measures against North Korean cyber-attacks.

Thus, in this study, we analyzed the strategies and capability of North Korean cyber-attacks, recent cases of North Korean cyber-attacks, the characteristics of North Korean cyber-attacks, and the capability and limitations of South Korea to deal with the cyber-attacks. Also, we propose a big data-based countermeasure strategy against cyber-attacks and analyze the expected effect of the strategy. Lastly, the conclusion is suggested.

Strategies of North Korean Cyber-attacks and Their Capabilities

The Strategy of North Korean Cyber-attacks

North Korea has been recognizing cyberspace as a battlefield with high strategic importance, and actively using cyber warfare in a strategic asymmetrical capacity. Cyber warfare capacity is one of the three biggest asymmetric warfare capacities, along with nuclear and guerrilla capabilities.[1]

The reason for North Korea to use cyber warfare capacity as a strategic weapon is that cyber-attacks have a high cost-effectiveness, can be easily utilized, and can quickly spread to show a great ripple effect. Also, cyber-attacks do not require physical penetration and have anonymity, so it is difficult to impose sanctions and retaliations against such attacks.[2]

The aim of the North Korean cyber-attack strategy includes social unrest, disturbance of military actions in case of emergency, paralyzed national functions, ideological propaganda, and foreign money earnings to secure income. More precisely, the primary aim is to preoccupy informative superiority against South Korea and to attack the intelligence network when there is a total war to delay the intervention of U.S. troops. Then, they are aiming to secondarily neutralize the South Korean weapon system and munitions support by attacking the C4I system, and quickly exterminating the South Korean troops with mass fire.[3] U.S. experts have been assessing that the main goal of North Korean cyber-attacks is to interpret the South Korea–U.S. military alliance.[4]

North Korea completed its unique concept and strategy of cyber information warfare in the late 1990s, and has developed various tactics, including cyber-attack tactics, psychological tactics, and economic information acquisition tactics.[5] It is believed that North Korea has imitated the acupuncture strategy, which is included in Chinese military doctrine, and benchmarked Chinese cyber warfare strategies.[6]

North Korean cyber warfare tactics are apparently classified into the following:

surprise attack tactics, camouflage tactics, deception tactics, informative tactics, psychological tactics, concealment tactics, and destruction tactics. Considering the cases of North Korean cyber-attacks, they have developed various strategies and tactics, and they seem to have already established the rules of cyber-engagement.[7] The North Korean rules of engagement have recently been modified to not perform cyber-attacks within North Korean territory. North Korean cyber-attacks are performed by cyber troops in safe houses located in China. It is said that hundreds of troops deliver attacks on one target using proxy servers to conceal the origin of the attack, and when the operation is complete, they return to North Korea.[8]

Such cyber-attack tactics maximizes the possibility of concealing the fact that the attackers are from North Korea, through the maintenance of confidentiality and covering up the origin of the attack. They are taking advantage of the nature of cyber-attacks usually taking a few months to identify the causes of attacks to make it difficult to specify the attackers.

North Korea's Cyber-attack Capacity

The capacity of North Korea's cyber-attacks is significant in that it has been regarded as one of the most aggressive in utilizing cyberspace, along with China and Russia.[9] The U.S. Department of Defense conducted a simulation experiment on this issue, and the result showed that North Korean cyber troops are capable of paralyzing the control post of the U.S. Pacific Command, and damage the mainland's electrical grid. The United States has recently expressed its concern over North Korea's cyber-attack capability. U.S. experts noted that the North Korean cyber-attack capability was insufficient when they delivered DDoS attacks on July 7, 2009. However, their evaluation was raised beginning with the cyber-attack on March 20, 2013, and now many experts agree that North Korea's cyber-attack capacity has reached a considerably high level.[10]

North Korea showed a high interest in the cyber troops already under Kim Jong Il's rule and supported them. Now, Kim Jong-un, the Chairman of the Central Military Commission, is directly controlling cyber and electronic warfare. In North Korea, cyber warfare management is a nationwide task as part of a national military strategy under direct control of the Labor Party and the Central Military Commission, which are the highest authorities in North Korea.[11] The government's budget is also focused on the preparation of cyber warfare where they are putting an enormous amount of support into high-performance computers, internet training networks, and advanced facilities.[12]

North Korea has a department of cyber operations and relevant organizations under the influence of the People's Army and Korean Worker's Party to perform cyber-attacks, cyber psychological warfare, and cyber spy communication. There are also departments such as the People's Army General Command Post, the General Secretariat under the direct control of the National Defense Committee, the Labor Party's United Front Department, and the Exclusive Cyber Team under the Labor Party Department No. 225. The General Command Post is taking charge of cyber psychological warfare, such as collecting military intelligence, hacking, disturbing and neutralizing military command

and communications and spreading false information against South Korea. The General Secretariat under the National Defense Committee is commanding the cyber warfare against South Korea and is in charge of delivering cyber-attacks based on the overseas bases, such as collecting South Korean strategic information, delivering cyber-attacks against the South Korean public network, and dispatching special agents abroad. The Labor Party's United Front Department is in charge of conducting cyber psychological attacks against the South Korean people. The Exclusive Cyber Team under the Labor Party Department No. 225 is in charge of making spy commands and communications using cyber technology. Likewise, North Korea is running a systematic operations structure.[13] In particular, Kim Jong-un, the chairman of the North Korean labor party, ordered the establishment of a cyber strategic command at a 4th labor competition, November 11, 2013. The goals of the cyber strategic command are disarming cyber strategic resources of South Korea, the United States, and Japan and executing unexpected attacks on the national infrastructures via cyber-attacks, cyber warfare, and disturbance of GPS signals by obtaining secrets and organizing a cyber special force team (EMP).

In terms of the scale of the North Korean cyber military force, the intelligence reported to the National Assembly in November 2013 by Nam Jae-jun, the Director of the National Intelligence Service, is believed to have the public's confidence. In the report, the National Intelligence Service said that North Korea had 1,700 specialized hackers in seven hacker departments, and their support to hacking involved about 4,200 personnel in 13 organizations to develop cyber weapons.[14]

North Korea is training about 100 cyber troops at Mirim College each year. Considering the previous cases of cyber-attacks, it seems that North Korea has a number of hackers who can threaten South Korea.[15]

The North Korean cyber weapon system has the capability of delivering various types of attacks, using electronic, psychological, and logical weapon systems. The electronic weapon system involves EMP[16] to neutralize electronic devices, and GPS jammers to disturb the GPS signals. The psychological weapon system utilizes social engineering technology, spear phishing[17], and pro-North Korean applications. The logical weapon system involves various cyber-attack techniques, such as DDoS attacks[18], APT attacks[19], botnet operations, and malicious code development. In addition, they have a more advanced attacking technology, such as attack bypassing to prevent backtracking, encryption, and trace deletion.

The U.S. Strategic Commander Cecil Haney noted about the North Korean cyber warfare capacity that there is a need for immediate counteractions against North Korean cyber-attacks.[20] The U.S. government and the Heritage Foundation estimated that the North Korean cyber-attack capacity had reached a dangerous level, although the threat was relatively lower than that of China, Russia, and Iran.[21] Technolytics Institute graded the cyber-attack capacities of each country, where China received a score of 4.2, Russia 4.0, Iran 3.4, and North Korea 2.8, out of 5.[22]

Cases of North Korean Cyber-attacks

North Korean cyber-attacks against major institutions in South Korea have been raging since 2009. In July 2009, the North Korean attack paralyzed 47 institutions' websites in South Korea and the United States, including the Blue House and the White House, and destroyed 1,488 PCs.[23] In March 2011, they used a more advanced technique to deliver DDoS attacks on 40 websites including the Blue House and Naver, and destroyed the hard disk drives in 820 PCs.[24] In April 2011, they penetrated the laptop of a maintenance engineer to attack the network of Nonghyup to delete the financial data from 273 servers, causing disorder that translated to 20 days of financial paralysis.[25] In June 2013, they hacked into *Joongang Ilbo*, a press company, to falsify the main page of its website and destroyed 74 server computers, including the newspaper production server, with the attacks via a server maintenance engineer's laptop.[26] In 2013, they delivered multiple simultaneous attacks twice in March and June. The March attack spread malicious codes to press companies, including KBS, MBC, and YTN, and financial companies, including Nonghyup and Shinhan, and destroyed 48,000 computing devices. In June, they conducted DDoS attacks and destroyed the servers at 68 institutions, including broadcasting companies, newspaper companies, and the Blue House.[27,28] In November 2014, Sony Pictures was attacked after releasing a trailer of a comedy movie "The Interview," which was about the assassination of Kim Jong-un, and the attack deleted and leaked the data from 3,200 PCs and 830 server computers. The FBI announced that North Korea had originated the attack, and mentioned the possibility of imposing ten hours of sanctions against North Korea as a countermeasure.[29] In December 2014, North Korea hacked into the Korea Hydro & Nuclear Power to destroy five PCs at Kori and Wolsong Nuclear Power Plants, and leaked 84 pieces of data including the nuclear power plant blueprint.[30] In October 2015, North Korea was suspected of attacking Seoul Metro, a subway company operating subway lines 1–4 in Seoul, to hack into two server computers and spread malicious codes to 58 PCs.[31] In September 2016, there was an attack on the vaccine server of the Ministry of National Defense, and the exclusive server for the internal network of the Cyber Warfare Command. This attack damaged 2,500 military internet PCs and 700 intranet PCs.[32]

According to a 2016 intelligence agency report, about 40,000 hacking attacks either from North Korea or foreign countries occurred per hour on average, which equaled over 1 million attacks per day. The main targets of the external attacks were mainly the websites of governmental or public institutions. The origins of hacking were mainly distributed among three Northeast provinces of China, including Shenyang, Qingdao, and Yanji. There were also IP addresses from the United States and Southeast Asia, where North Korean gambling websites have recently been operating illegally.[33] The major global security companies, including Symantec, McAfee, and Kaspersky Lab have recently announced that North Korea is the *de facto* power of hacker groups such as Dark Seoul, Operation Troy, and Operation Kimsuky.

We analyzed eight years of North Korean cyber-attacks from 2009 to 2016 in terms of the attack target, purpose, technique, preparation period, and the relation of attacks to

North Korean nuclear experiments.

The analysis of the attack target showed that they were mainly attacking press companies, financial companies, and governmental institutions, which could lead to social confusion. The 7.7 DDoS attack (2009) targets were financial companies and governmental institutions. The 3.20 attack (2013) targeted financial and broadcasting companies. The 6.25 cyber-attack (2013) targeted the press and governmental institutions.

The purpose of the attack has changed from DDoS attacks to cause disorders in major national services to APT attacks to hijack or destroy national confidential information. The DDoS attacks, such as the 7.7 DDoS attack (2013) and 3.4 DDoS attack (2011), changed to APT attacks, such as the 3.20 cyber-attack (2013), 6.25 cyber-attack (2013), KHNP hacking (2014), Seoul Metro hacking (2015), and national defense network hacking (2016). DDoS attacks were prevalent between 2009 and 2011, but the circumstances changed to concentrate on APT attacks from 2013 to 2016.

The technique of attack was mainly to hack into multi-use facilities, such as web-hard services and computational resource management servers located in private companies, which involve a number of users, to spread malicious codes. Web-hard services was the main path of attack for the 7.7 DDoS attack (2009) and 3.4 DDoS attack (2011), and the computational resource management servers located in private companies was the major path of attack for the 3.20 cyber-attack (2013), 6.25 cyber-attack (2013), and national defense network hacking (2016).

It was suggested that the preparation period for the North Korean cyber-attacks was at least three months, and at most seven months. It was found that the Nonghyup hacking (2011) took seven months, and the 3.20 cyber-attack (2013) took three months of preparation.

Due to the paralysis of major media and financial companies, which are closely related to people's lives, people ended up experiencing inconvenience and fear. There were also qualitative losses, including an increased distrust toward government action. The quantitative loss caused by the 3.20 cyber terror could be calculated using two methods: direct/indirect loss (damage amount) and derivative loss (damage amount). The direct/indirect loss was calculated using the cost price method, and the derivative loss could be calculated through the quantitative analysis of the decreased prices of stocks due to the weakening of public trust. A total of 74 billion KRW was recorded as direct or indirect losses, which involved direct loss, such as the profit loss and rehabilitation expenses, and indirect loss, such as the loss of production efficiency. A total of 731.1 billion KRW of derivative loss was recorded, including reduced stock values. Therefore, the total loss due to the 3.20 cyber terror was estimated to be 805.1 billion KRW.[34] Considering that the 7.7 DDoS attack in 2009 marked a 54.4 billion KRW loss, the 3.20 attack caused about 14.8 times greater damage, and such findings suggest that the damage caused by the North Korean cyber terror had sharply increased.

In terms of the correlation between North Korean nuclear experiments and cyber-attacks, it was found that they conduct cyber-attacks within one to four months of nuclear experiments. The second nuclear experiment was performed in May 2009, followed by

the 7.7 DDoS attack (July 2009), and the third nuclear experiment was performed in February 2013, followed by the 3.20 cyber-attack (March 2013). The national defense network hacking (December 2016) followed the fifth nuclear experiment (September 2016). Considering these cases, it is believed that North Korean cyber-attacks often follow after a nuclear experiment.

Characteristics of North Korean Cyber-attacks

The characteristics of North Korean cyber-attacks could be analyzed into the following: evolution of attacks, online/offline parallelism, difficulty in tracing the origin of the attack, and the paralleled cyber strategy against the private sector.

First, the attack target and range, as well as the damage are becoming more significant, involving the targets of national defense systems, public institutions, media, broadcasting, financial sector, telecommunications, infrastructure, and conglomerates. In terms of the methods, simple attacks, such as DDoS and website falsification developed into APT attacks which could deliver high-level damage over an extended period. The purpose of spreading malicious codes used to be for the collection of personal information, but became more critical, such as the destruction of data or hard disk drives.[35] Based on such information, it is believed that the cyber warfare capacity of North Korea is becoming greater, and as their information about South Korea has been widely collected, more precise attacks become feasible.

Second, North Korean cyber-attacks are not only occurring in terms of logical aspects, but also in physical aspects. When network penetration is unfavorable, North Korea is trying to use socio–technical methods, such as winning over Korean citizens or the employees of an overseas branch of a Korean company. They are using these people to spread software with hidden malicious codes to perform cooperative actions, such as attacks on supply chains. Such a strategy is used because online penetration has become difficult due to South Korea's actions against North Korean cyber-attacks, including network separation and the cloud environment. North Korea is trying to use internal collaborators or subcontract employees, who are capable of connecting to the intranet, to sneak into the network.

Third, backtracking and hitting back has become more difficult, as it is difficult to recognize the origin of attacks. North Korea is utilizing various concealing and bypassing techniques to prevent cyber-attack detection and backtracking. In addition, they are delivering cyber-attacks via China, which makes it even more difficult to retaliate against the attack, due to issues related to jurisdiction and diplomatic matters, although it is possible to identify the origin.

Fourth, they are combining military–strategic attacks with cyber fraud and psychological attacks on the private sector. They are committing financial fraud using leaked personal information through infected computers with malicious codes, to obtain foreign currency and collect basic information for other cyber-attacks.[36] Also, they are making use of psychological cyber strategies to bring over the personnel for the cyber-

attacks.

Likewise, North Korea has a systematic weapon system and attack strategy to conduct cyber-attacks at various ranges and levels. The number of North Korean attacks on South Korean infrastructure is expected to increase in the future. There is an increasing possibility of delivering multiple simultaneous pinpoint strikes, after finding out the vulnerabilities of the control networks and financial networks of major infrastructures, such as traffic and electric grids. Hence, there is an increasing threat of simultaneously paralyzing the traffic, communication, finance, and electric networks to cause damage as serious as physical attacks.

Limitations of South Korean Countermeasures against Cyber-attacks

Focusing on Handling Incidents Caused by North Korean Cyber-attacks

Currently, the South Korean countermeasure strategy against North Korean cyber-attacks is minimizing damages when an incident takes place due to North Korean cyber-attacks by quickly handling the incident. Each national cyber-security team barely managed to prevent the spread of negative results caused by sporadic and continuous North Korean cyber-attacks by primarily identifying and blocking the attacks quickly. For example, they distribute vaccines and block the origin of malicious codes. This reactive strategy has fundamental limits to coping with the continuously changing strategies of North Korean cyber-attacks. For example, because North Korea focused on large-scale DDoS attacks in 2011, South Korea focused on blocking excessive traffic on the Internet network to deal with the DDoS attack. To disarm South Korea's strategy, North Korea has focused on new APT attacks since 2013. So, the limitations of South Korea's strategy of defending against DDoS attacks were exposed, and since then, South Korea has changed its cyber-attack response system by tightening security for internal staff and outsourcing personnel. Like this example, coping reactively to changes in North Korean cyber-attacks is only a temporary solution.

Hence, it is necessary to change the current cyber-attack response system to one of prevention and preemptive measures by detecting changes in North Korean cyber-attacks preemptively. To do this, a virtuous cycle structure is needed to collect information about North Korean cyber-attacks from domestic and foreign countries as much as possible, detect fundamental changes in their attack vectors via big data analysis, and then reflect on the detected changes in policies about preemptive prevention.

Insufficiency of Systematic Information Gathering of North Korean Cyber-attacks

Recent cyber-attacks from North Korea, including the KHNP hacking (2014) and national defense network hacking (2016) showed the difficulties of nationwide preventive detection. It is difficult to determine if a cyber-attack is targeting the

public, private or military sector, but the countermeasures are based on the jurisdiction in accordance with the legal system, so it is difficult to make multidimensional counteractions. Previous cyber-attacks from North Korea also did not separate the sectors they were targeting, but they conducted simultaneous attacks in every aspect. Therefore, it is difficult to detect or efficiently take action against cyber-attacks only with sector–specific detection activities. In particular, the South Korean backbone networks are mainly operated by private companies, so there is a need for information-sharing within the private sector. Also, when the subject of the cyber-attack is not designated as North Korea, the military and intelligence institutions cannot intervene due to legal restrictions. Therefore, it is necessary to establish a countermeasure system to share information and detect the subject of the attack, and enable cooperative actions among each sector, regardless of their types.

Most of the cyber-attacks occur via foreign networks. In the 7.7 DDoS attack (2009), a total of 46 countries were involved, and in the 3.4 DDoS attack (2011), attacks originated from 70 countries.

Recently, most of the APT–type cyber-attacks conducted by North Korea occurred in foreign countries such as China and Southeast Asia or are delivered via foreign countries. Thus, to share information, an information-sharing system and standardization are needed. Based on the cyber-attack information-sharing system, we can quickly collect information about North Korean cyber-attacks broken out not only by domestic but also by foreign countries, and thus we can detect changes in North Korean cyber-attacks in various ways.

Unpredictable Threats of North Korean Cyber-attacks

South Korea continuously predicts threats of North Korean cyber-attacks and analyzes characteristics of the threats qualitatively. For example, based on the analyzed characteristics, security professionals have predicted that North Korean cyber-attacks will continue by changing the attack method from DDoS to APT or by abusing IT companies or outsourcing personnel as an alternative attack vector due to the difficulty of a direct attack.

However, predictions using cyber-attack–related information through big data analysis are needed rather than warning forecasts. By collecting information, including the type of malicious code, places where cyber-attacks originate, and hacking information from domestic and foreign countries, we need to predict cyber-attacks based on profiling–based quantitative big data analyses. For example, an attack that scans an internal staff's PC information attached in an e-mail which originates from China is predicted. Preemptive prevention is possible only if we predict such scenario–based cyber-attack threats.

Strategies against Cyber-attacks Based on Big Data

Example of Responding to Cyber-attacks Based on Big Data

Developed countries, such as the United States, Britain, or Japan have cross–established various surveillance systems using advanced facilities and sensors to enable cooperation to prevent disasters. For example, they provide a service to analyze the data of typhoons, rainfalls, or earthquakes, to be prepared for national disasters, including the prediction of the possibility of tsunamis or flooding. They integrate water reserves data, weather data, and current rainfall data to take steps to prevent flooding or droughts.[37] Such techniques are also used for risk management and financial fraud prevention, such as the prevention of money laundering and the management of credit risk.[38] There is growing interest and investment in homeland security around the world. The United States is developing technology to predict indicators of terrorism by detecting terrorism trends using analyzed and collected information from social networks, newspapers, magazines, and news reports, for its homeland security. They are trying to resolve security threats, which are defined as fifth–generation warfare involving the addition of political, economic, and sociocultural factors to traditional warfare, through the analysis of the network.

The technique of big data analysis in the field of cyber security is used for large–scale log analysis, the detection of abnormal transactions and actions, and the detection of malicious codes. As a representative case, Sourcefire uses the Hadoop platform to detect the presence of malicious codes by monitoring two million devices.[39] EMC RSA applies the technique to recognize the context or situation through intelligent risk management, to take swift actions.[40] According to EMC RSA, there is no 100 percent perfect means of cyber security, and we should not consider it an extension of past technology and thoughts. They state we need a more creative security method, and it is essential to establish the intelligent security system focused on big data analysis to achieve such a goal.[41]

Establishment of Cyber-attack Analysis System Based on Big Data

The existing cyber-attack analysis system has focused on seeking malicious codes and hacking evidence, so the actions were available only after the damage, which is a big limitation. Thus, there is a need for establishing a countermeasure system to identify the attackers, as well as the malicious codes and hacking evidence through an integrative process of profiling analysis at each stage of the overall life cycles of the cyber-attack information, to generate a rapid response and find the causes of the cyber-attack.

Additionally, the malicious code North Korea spreads becomes very diverse because North Korea continuously uses new and variants of existing malicious code, and thus South Korea must handle the rapidly changing attacks. There are several examples of coping with diversified malicious codes based on big data such as the global security company IBM's information security Intelligence and McAfee's cyber threat Intelligence Exchange. These companies have succeeded in defending the malicious codes by

establishing runtime integrated analysis systems based on big data.

Big data is needed to quickly and accurately understand the vast amount of information about North Korean cyber-attacks. To process such information, state-of-the-art big data processing technologies that can go through a large amount of data quickly and precisely are required. South Korea must build big data analysis systems that can accumulate information about North Korean cyber-attacks by detecting anomalies in the Internet network and generating fingerprints of North Korean cyber-attacks.

Various kinds of artificial intelligence techniques have been introduced in the field of cyber security to address the problems in the conventional methods of detecting network trespassing. In other words, they automatically create knowledge by collecting normal and various abnormal actions and applying various machine learning algorithms to such actions. It can also be seen as a way to determine whether the simultaneously occurring events are normal or abnormal, based on the acquired knowledge.

As described in Figure 1, we construct channels to collect vast amounts of information about North Korean cyber-attacks via self-detection and sharing with private enterprises at the first step, SIEM (Security Information and Event Management). At the second step, we accumulate the collected information and build a big data analysis system to perform real-time analysis for a large amount of in-flow information. At the third step, we predict changes in North Korean cyber-attacks using various statistical analysis methodologies such as machine learning, decision tree analysis, cluster analysis, etc. The performance and quality of the three–step big data analysis system will be gradually improved by cyber security professionals who continuously monitor the system.

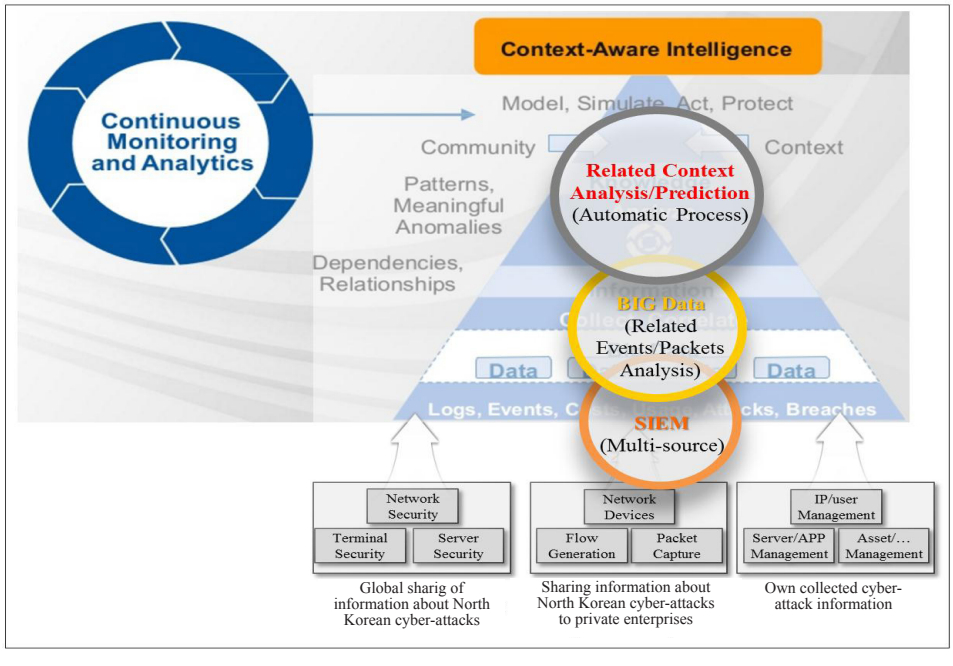

Figure 1. Big Data-based Analysis System for North Korea Cyber-attacks

Recently, the number of examples of big data usage for proving the existence of malicious code spread by North Korean hacking groups or for warning and responding to social issues is increasing.

Using the established analysis system, which is based on a scientific method, can improve the existing decision-making for response strategies which relies on only the experiences and intuition of the analyzer. Also, by sharing cyber-attack related information to institutions which respond to cyber-attacks, the information can be used for prevention and preemptive measures.

Classification of Big Data Information to Prepare for North Korean Cyber-attacks

As shown in Table 1, a total of 20 types of cyber-attack information in five areas should be collected to prepare for North Korean cyber-attacks. The purposes of implementing and spreading malicious codes for infection are mainly collected as the attacker information. By analyzing the collected information, execution of North Korean cyber-attacks can be proven.

Information about cyber-fraud attackers represents the collection of information about North Korean cyber-attacks with the goal of acquiring foreign currencies. Malicious files are the collection of malicious e-mails, malicious codes and the new and variants of malicious applications. We can detect changes in attack vectors North Korea exploits with the malicious files. Information about security vulnerability represents the collection of security vulnerabilities North Korea mainly exploits. By analyzing the security vulnerabilities, we can prevent North Korean cyber-attacks preemptively. The report represents analyses of malicious codes, malicious applications, and incidents by cyber-attacks. We can profile the purposes of North Korean cyber-attacks based on the reports.

Table 1. Classification of Big Data Analyses for North Korean Cyber-attacks

Main Classification	Sub Classification
Attacker information	Spread sites of Malicious Code Pass sites of Malicious Code C&C Information Web Alteration Infected PC Attack IP
Information about attackers of cyber-fraud	Phishing Farming Smishing Information Disclosure Site
Malicious files	Spam E-mail Malicious Code Malicious Apps Web Shell
Security vulnerability	CVE KVE

Sharing North Korean Cyber-attacks

Recently, the U.S. Department of Homeland Security has recognized the need to build an efficient and secure information-sharing system in order to respond to cyber threats and has established STIX (The Structured Threat Information eXpression) standardization for sharing cyber threat information. As shown in Table 2, the STIX cyber threats are comprised of eight components; Indicator, Incident, TTP, ThreatActor, Campaign, ExploitTarget, and COA. South Korea also needs to use STIX to share information about North Korean cyber-attacks executed both inside and outside of the country. Through this, it is possible to establish a standardized system which collects information about North Korean cyber-attacks not only from domestically but from foreign countries.

Table 2. Eight Components of the Standardized STIX Sharing North Korean Cyber-attacks

Main Classification	Sub Classification
Observable	Structures related to all events can be observed in cyber space: STIX-based components Example: file–related information (name, hash, size, remove histories, and etc.), registry key, service list, IP address, receipt logs
Indicator	Structures related to threat metric: the collection of observable data related to threat metric Example: hacked domain, forged e-mail, file hash related to a trojan
Incident	Structures related to incidents: indicators which are proven to be results of cyber-attacks Example: Information related to damage and attack based on the six–way rules such as time and damaged system
Tactics, Techniques and Procedure (TTP)	Structures related to attack methods: Attack methods including strategies, techniques, and procedures behind the incidents Example: (Strategy) Credit card information leak, (Technique) Sending a targeting e-mail where malicious codes such as a key logger are attached. (Procedure) Set up attack targets → Write social technologic e-mails or documents → Build C & C domains → Send the attack e-mails
ExploitTarget Course of Action (COA)	Structures related to vulnerability: vulnerabilities in SW and system for executing TTP of ThreatActor, network, and configurations Example: vulnerability Structures related to response: recovering ‘ExploitTarget,’ responding to ‘Incident,’ etc.

Expected Effect of Using Big Data against North Korean Cyber-attacks

Enhancing North Korean Cyber-attack Information Collection Ability

Recent cyber-attacks from North Korea are targeting not only governmental offices, but also private companies, with the purpose of taking and destroying military, industrial, and private secrets. When there is a cyber-attack, a swift cooperative confrontation based on information-sharing is required. A quick and effective confrontation could prevent the damage spread in the early stages. The methods of cyber-attacks are changing day by day, so countermeasures are difficult. Thus, there is an increasing need for real-time information-sharing. Also, the participation of private companies should be continuously expanded for an overall analysis of cyber threats and violations, in addition to the standardization of information-sharing. A widely applicable standard, which is not restricted to a specific organization, should be proposed to share the cyber threat information. There is a need for information-sharing and big data analysis in terms of hacking–attempt domains, IP, C&C, infected IP, spread and pass sites of malicious codes and malicious code samples, to deal with North Korean cyber-attacks. To do this, it is necessary to establish a big data-based cyber-attack information-sharing system and utilize standards that can share information such as STIX. Through this, it is possible to systematically collect vast amounts of information about North Korean cyber-attacks in real time. It is expected that the technical infrastructure can be implemented through a cyber-attack information-sharing system and standardization, and the attack information is shared quickly between the relevant organizations, so that an immediate response is possible in case of an incident.

Predicting Threats of North Korean Cyber-attacks

Instead of making intelligence–based cyber-attack predictions, it is possible to make statistical predictions based on quantified information by collecting information such as types of malicious codes, sources of hacking, hacking information, etc., from domestic and foreign countries. Based on the statistical prediction, it is possible to preemptively detect changes in North Korean cyber-attacks using various statistical analysis methodologies such as machine learning, cluster analysis, etc. From the detected changes, we can confirm that the North Korean cyber strategy is changing. By analyzing the North Korean strategy and predicting cyber-attacks in a scenario–based way, it is possible to respond to cyber-attacks preemptively. This is the same as the method that concentrates resources to respond to specific crimes when the pattern of the crime is predicted. Thus, minimizing potential threats or even preemptive responses is possible by predicting North Korean cyber-attacks.

Change into Preemptive Measures against North Korean Cyber-attacks

The main measure against North Korean cyber-attacks is minimizing damages after the incidents caused by the attacks. Additionally, education for increasing security awareness and advice for applying security patches and security applications are conducted as preemptive activities. However, it is possible to predict the strategies of North Korean cyber-attacks and individual tactics in a scenario–based way by using big data. Thus, strategy can change from a focus on incident response to preemptive measures against North Korean cyber-attacks after establishing such infrastructures for prediction. It is expected that the infrastructures would have the effect of preventing North Korean cyber-attacks because they concentrate resources on the predicted points where North Korean cyber-attacks will change.

Enhancing International Cooperation via Standardization of Cyber-attack Information Sharing

We expect that international cooperation will become more active by establishing a cyber-attack information-sharing system and by using STIX, an information-sharing standard, to enhance international cooperation. Since the North Korean cyber-attacks are committed in a foreign country or delivered via foreign servers, the international community should devise various efforts to foster international cooperation. In particular, enhanced overseas information collecting and sharing is necessary to deal with APT attacks, which are the recent patterns of North Korean cyber-attacks.

Enhanced detection of malicious codes and monitoring of DDoS attacks are necessary to allow preemptive detection, through connection analysis of cyber-attack indicators including spread sites, threat codes and infected PC information. It is important to conduct a joint investigation of CERT and infringement of each country, to allow for counteractions against the attacks from foreign countries targeting South Korea. Over 80 percent of the total hacking cases require information-sharing with the United States, China, and Japan, so it is especially necessary. Therefore, we should extend the information collection channels through the activities of the Asia Pacific Computer Emergency Response Team (APCERT)[42] and the Forum of Incident Response and Security Teams (FIRST),[43] and enhance the cooperative system against emergencies through informative and human interchange with neighboring countries, including China and Japan. It is necessary to perform joint actions and measures, as well as information-sharing between international CERTs in terms of major infringement issues, including vulnerabilities and malicious codes.

Conclusion

There is an increasing threat of North Korean cyber-attacks that North Korea is enhancing as a form of asymmetric weapon. North Korea has about 1,700 highly trained hacker troops, and there is a continuous provocation against the dependency of South Korean IT advancement. The analysis of the trends and characteristics of North Korean cyber-attacks within the past decade show that the attacks have been intellectualized, complex, and objective–oriented, so there is a need for a national countermeasure that is more systematic than the previous actions. To do this, North Korean malicious codes and cyber threats should be collected widely in company with domestic and foreign cyber security teams. Thus, an internationally standardized system is essential to sharing cyber threats such as malicious codes and cyber-attack information. Above all, in order to identify and respond to North Korean cyber-attacks in the early stages, it is necessary to establish a cyber-attack response system that predicts cyber-attacks early by collecting information about North Korean cyber-attacks and analyzing it based on big data. As a result, it is possible to change our countermeasure strategy from one focusing on responding to North Korean cyber-attacks at an early stage to preemptive measures by predicting North Korean cyber-attacks preemptively.

Notes

1. Jong-in Kim, Yu-joong Kwon, Gyu-hyun Jang, and Seung-jo Baek, "North Korea's Cyber War Capability and South Korea`s National Counterstrategy," *The Quarterly Journal of Defense Policy Studies* 29, no. 4 (2013). [in Korean]
2. Sang-ho Lee, "The Reality of Cyber Warfare and Future Cyber-attack Countermeasures: Lessons and Countermeasures of the 7.7 Cyber-attacks," *The Spirit of the Times*, no. 44, 2009, 246–65. [in Korean]
3. "North Korea's Final Battle is Cyber Warfare," *Jaju Minbo*, May 20, 2013. [in Korean]
4. Richard A. Clarke and Robert K. Knake, *Cyber War : The Next Threat to National Security and What to Do About It* (New York, NY: Harper, 2010).
5. "North Korean Cyber Tactics Imitated the Chinese Acupuncture Tactics," *JoongAng Daily*, July 10, 2009. [in Korean]
6. The acupuncture strategy refers to the paralysis of the overall system by capturing the vulnerabilities and acupuncture points of the opponent's information system to pursue maximized effectiveness. "North Korean Complex Provocation Warning! Do You Know the EMP Electric Warhead?," *New Daily*, March 26, 2013. [in Korean]
7. "What are the Cyber War Tactics Implemented by North Korea in the 6.25 Hacking," *Dailysecurity*, June 6, 2013. [in Korean]
8. "North Korean Cyber Troop Defector, Refers to the 3.20," *Electronic Times*, May 14, 2013.
9. Sung-pyo Hong, "North Korean's Cyber-attack Method, Advanced and Intelligent," *Unified Korea*, no. 328, April 2011, 34–35.
10. Jung-ku Kim, "The National Crisis System for the Preparation of Cyber Terrorism is Urgent," *BCP&ERM*, July 9, 2008.
11. Tyler Jense and Samuel Lies, "Open-source Analysis of the Cyber Warfare Capability of North Korea," Proceedings of the 14th Annual Information Security, 2013.
12. Heung-kwang Kim, "North Korean Cyber Terror Information Warfare Capacity and a Proposal of Cyber Security Measures," *Industrial Technology Spill Response Conference*, 2010.

13. "2013 National Intelligence Service's Parliamentary Inspection Report," *The National Intelligence Service*, 2013.
14. Kwan Choi and Min-chi Kim, "A Comparative Analysis of the National Defensive System against Cyber Terrorism for National Security and Public Safety: Focus on the South Korea, America, and France," *The Journal of Police Policies* 29, no. 2 (August 2015): 1–36. [in Korean]
15. Dakota L. Wood, "Index of U.S. Military Strength Assessing America's Ability to Provide for the Common Defense," *Heritage Foundation*, 2015, 28–34.
16. EMP (Electromagnetic Pulse effect): It is the effect of electron emission due to the EMP. All the electronic devices within the influence of electromagnetic pulse are destroyed.
17. Spear Phishing: Named after spear fishing. Unlike common fishing targeting unspecified masses, it is a varietal fishing type targeting a specific individual or group using the previously acquired information with the purpose of personal information capture or fraud.
18. DDoS (Distributed Denial of Service): A technique to disable normal services by neutralizing the traffic path or service device with massive traffic.
19. APT (Advanced Persistent Threat): A hacking technique to intelligently and continuously sneak into the internal system to seize and destroy the information, aiming at a specific target with a clear purpose.
20. Sung-won Baek, "U.S. Strategic Commander North Korean Cyber Capacity Development, Urgent Response Needed," *Voice of America*, January 16, 2015.
21. "Obama Ranks N. Korea Cyber Capabilities as Not So Good," *WIRES*, February 18, 2015; and Dakota L. Wood, "2015 Index of U.S. Military Strength, Assessing America's Ability to Provide for the Common Defense," *Heritage Foundation*, January 2015.
22. Tecnolytics, "World War III: A Cyber War has Begun," August 2007.
23. Korea Information & Security Agency (KISA), "7.7 DDoS Attack," *Internet & Security Focus*, February 2013.
24. "3.4 DDoS Attack, Upgrade Version of 7.7 DDoS Attack (Ahnlab)," *News Hankuk*, March 7, 2011. [in Korean]
25. "Prosecutors' Office, Nonghyup Hacking Prepared by General Secretariat for 7 Months," *Dong-A Ilbo*, May 4, 2011. [in Korean]
26. "Joongang Ilbo's Website Hacking," *Boan News*, June 9, 2011. [in Korean]
27. "Malicious Code Penetration Against Network of KBS, etc. North Korea's Deed," *New Daily*, March 20, 2013. [in Korean]
28. "6.25 Cyber Terror Local Press Company 1 Mercilessly Hacked, Suspicions on North Korea," *Etoday*, June 25, 2013. [in Korean]
29. "North Korean Internet Overall Shutdown for 10 Hours, Possibly U.S. Cyber Revenge," *The Hankyoreh*, December 12, 2014. [in Korean]
30. "KHNP Hacking, North Korean Hacker Organization Deed," *Maeil Business Newspaper*, March 17, 2015. [in Korean]
31. "Seoul Metro Computer Server Hacking Suspicion on North Korea," *YTN*, October 5, 2015. [in Korean]
32. "Intelligence Authority, National Defense Network Hacking Suspicion on North Korea," *YTN*, December 7, 2016. [in Korean]
33. "Hacking Attacks Aimed at South Korea 360 Million a Year," *New Daily*, June 24, 2015.
34. Lee Yong-joon, Kwon Hyuk-jin, Lee Jaeil, and Shin Dong-kyoo, "Development of Countermeasures against North Korean Cyberterrorism through Research Case Studies," *The Korean Journal of Defense Analysis* 27, no. 1 (March 2015): 71–86.
35. "North Korean Cyber Warfare Capacity World's 3rd Place Threatening IT Powerhouse," *NK Vision*, May 9, 2013.
36. "North Korean Cyber Warfare Capacity Comparable to U.S. CIA," *Yeongnam Ilbo*, August 5, 2011.
37. J. Manyika et al., "Big Data: The Next Frontier for Innovation, Competition, and Productivity," *McKinsey Global Institute*, May 2011.

38. J. Feiman, "Hype Cycle for Application Security, 2012," *Gartner Group*, July 2012.
39. N. MacDonald, "Information Security is Becoming a Big Data Analytics Problem," *Gartner Group*, March 2012.
40. S. Curry et al., "Big Data Fuels Intelligence-Driven Security," *RSA Security Brief*, January 2013.
41. M. Nicolett and K. M. Kavanagh, "Critical Capabilities for Security Information and Event Management," *Gartner Group*, May 2012.
42. APCERT (APCERT, Asia–Pacific Computer Emergency Response Team): An international organization established in 2003 to improve international cooperation against infringements within the Asia–Pacific region, based on the representative internet response team (CERT) of each country.
43. FIRST (Forum of Incident Response and Security Teams): An international organization established in 1989 with 41 countries and 190 institutions to deal with international internet infringement.

Notes on Contributors

Yong-joon Lee (Ph.D., Soongsil University) is a senior researcher at the Defense Security Institute (DSI), where he has researched the insider threat program since 2016. He worked at the Korea Internet & Security Agency (KISA), where he researched cyber security from 2010 to 2015. His research interests have been focused on issues of cyber incidents detection.

Hyuk-jin Kwon (Ph.D., SungKyunKwan University) is a research fellow at the Korea Institute for Defense Analyses, where he has researched Information system assessment and information system development since 1991. He is a author and co-author of a number of scholarly articles. His most recent papers are: *Defense Information System Management Perspective Evaluation Models for Risk Management* (2013), *Evaluation System for IT Project and the Design for Post Evaluation System in Defense Area* (2013) and *The Analysis Study for Cyber Combat Types and Patterns in the Near Future* (2013). His research interests include cyber security and performance for information systems.

Jae-il Lee received B.S. and M.S. degrees in Computer Science and Statistics from Seoul National University, Seoul, Korea. He received his Ph.D. in Computer Science from Yonsei University, Seoul, Korea. He is a vice president of the Korea Internet & Security Agency (KISA), and the head of KrCERT/CC, and responsible for national internet incident responses for the private sector. His research interests have been focused on issues of establishing a internet and information security policy framework, reforming the legal environment, encouraging the private sector to utilize the internet as much as possible while protecting their own and/or public assets and data by validating every single step, and promoting it to the international level.

Dong-kyoo Shin received a B.S. in Computer Science from Seoul National University, Korea, in 1986, an M.S. in Computer Science from Illinois Institute of Technology, Chicago, Illinois, in 1992, and a Ph.D. in Computer Science from Texas A&M University, College Station, Texas, in 1997. He is currently a Professor in the Department of Computer Science & Engineering at Sejong University in Korea. From 1986 to 1991, he worked at Korea Institute of Defense Analyses, where he developed database application software. From 1997 to 1998, he worked in the Multimedia Research Institute of Hyundai Electronics Co., Korea as a Principal Researcher. His research interests include information security, digital right management for multimedia, home network middleware and ubiquitous computing.