The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-terror Attack on the Korea Hydro & Nuclear Power Co., Ltd.

Kyung-bok Lee[1] and Jong-in Lim[1]
[1]Graduate School of Information Security, Korea University
Seoul, Republic of Korea
[e-mail: isnare@korea.ac.kr, jilim@korea.ac.kr]
*Corresponding author: Jong-in Lim

Received August 14, 2015; revised October 6, 2015; revised November 3, 2015; revised December 4, 2015; accepted December 20, 2015; published February 29, 2016

Abstract

Due to an increasing number of cyberattacks globally, cybersecurity has become a crucial part of national security in many countries. In particular, the Digital Pearl Harbor has become a real and aggressive security threat, and is considered to be a global issue that can introduce instability to the dynamics of international security. Against this context, the cyberattacks that targeted nuclear power plants (NPPs) in the Republic of Korea triggered concerns regarding the potential effects of cyber terror on critical infrastructure protection (CIP), making it a new security threat to society.

Thus, in an attempt to establish measures that strengthen CIP from a cybersecurity perspective, we perform a case study on the cyber-terror attacks that targeted the Korea Hydro & Nuclear Power Co., Ltd. In order to fully appreciate the actual effects of cyber threats on critical infrastructure (CI), and to determine the challenges faced when responding to these threats, we examine factual relationships between the cyberattacks and their responses, and we perform analyses of the characteristics of the cyberattack under consideration. Moreover, we examine the significance of the event considering international norms, while applying the Tallinn Manual. Based on our analyses, we discuss implications for the cybersecurity of CI in South Korea, after which we propose a framework for strengthening cybersecurity in order to protect CI. Then, we discuss the direction of national policies.

Keywords: critical infrastructure protection; national cybersecurity; cyber terror; cyberattack; case study

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2015-H8501-15-1003) supervised by the IITP (Institute for Information & Communications Technology Promotion).

http://dx.doi.org/10.3837/tiis.2016.02.023 **ISSN : 1976-7277**

1. Introduction

Cyberattacks on critical infrastructure (CI) have long been a concern from a national security perspective since the emergence of Stuxnet [1]. Since 2011, the Council on Foreign Relations, which is a think tank that specializes in U.S. foreign policy and international affairs, has continuously classified "a highly disruptive cyberattack on the U.S. CI" as a Tier I contingency [2]. This prioritization shows that the cybersecurity of CIs is already considered to be a pressing national security issue.

For this study, we focus on the December 2014 cyber-terror attacks on the Korea Hydro & Nuclear Power Co., Ltd. (KHNP), which operates nuclear power plants (NPPs) in the Republic of Korea (ROK). This "KHNP cyber-terror attack" emerged as a national security threat and triggered a response from the ROK society, which up until then had been sensitive to security incidents. Fortunately, this cyberattack did not result in the loss of human life or the destruction of facilities. However, it showed that there is a need to pay close attention to such incidents because it highlighted the inadequacies of the existing cybersecurity system for CI, as well as the fact that previously identified security problems had not yet been resolved. In addition, it is necessary to analyze and review such cyberattacks in order to prevent the occurrence of similar incidents in future. In particular, this cyberattack should be studied because there are significant implications from various perspectives such as information security, national defense, national security, and international security.

The case of the hacking of Sony Pictures Entertainment (hereafter referred to as the "Sony hack") occurred around the same time (December 2014), and is believed to have been carried out by the same attacker (North Korea). This case was considered to be an international security issue, according to the strong response of the U.S. However, compared with the Sony hack, the KHNP cyber-terror attack has not yet been discussed in a similar manner, considering its relative importance. The main reason for this is that the details of the KHNP cyber-terror attack were unknown, and the subsequent response to it was inadequate.

Accordingly, we carried out a case study on the KHNP cyber-terror attack to better understand the actual cyber threats to the CI of the ROK. Moreover, in order to respond to the cyber threats in the CI sector, we attempted to identify the challenges that are being faced. By performing this case study, we demonstrated how potential cyber threats may be used by attackers to disrupt the CI. We also explored various practical countermeasures to such cyber threats.

The remainder of this paper is structured as follows. In Section 2, we present the steps involved in our research. Section 3 focuses on recent global trends regarding national cybersecurity. In Section 4, by performing a case study, we provide detailed descriptions on the KHNP cyber-terror attack, including its significance, facts, characteristics, and attack attribution. In Section 5, we show the results of the application of the Tallinn Manual [3] to the KHNP cyber-terror attack, while in Section 6, we discuss implications arising from our case study on the incident. In Section 7, we propose suggestions regarding cybersecurity of national critical infrastructure, which are based on the implications discussed. Finally, we discuss the results obtained and conclude the paper.

2. Research Flow

This study aims to identify potential cyber threats to CI, understand the challenges faced in the implementation of the current cybersecurity posture of the ROK's CI, and propose solutions for the reinforcement of cybersecurity systems having national CIP. To do this, we carried out research according to the following procedures.

We examined recent national cybersecurity trends from an international perspective. Then we performed a qualitative case study that relied on formalized media releases provided by the press and government because there was insufficient quantitative data about the incident. By performing a thorough analysis of the progress, characteristics, and responses to the incident, we provided descriptive accounts of the attack and its responses. These narratives were further supplemented by analysis of social circumstances that were related to the event. In addition, we analyzed the KHNP cyber-terror attack in terms of international norms using Tallinn Manual, which is one of the first international norms established for cyberspace.

This approach is similar to some aspects of the general risk-management process. Therefore, the flow of the above-mentioned research procedures is shown schematically in **Fig. 1**, and is in accordance with the risk-management process of ISO/IEC 27005:2011 [4], which is a representative standard for the IT risk-management domain.

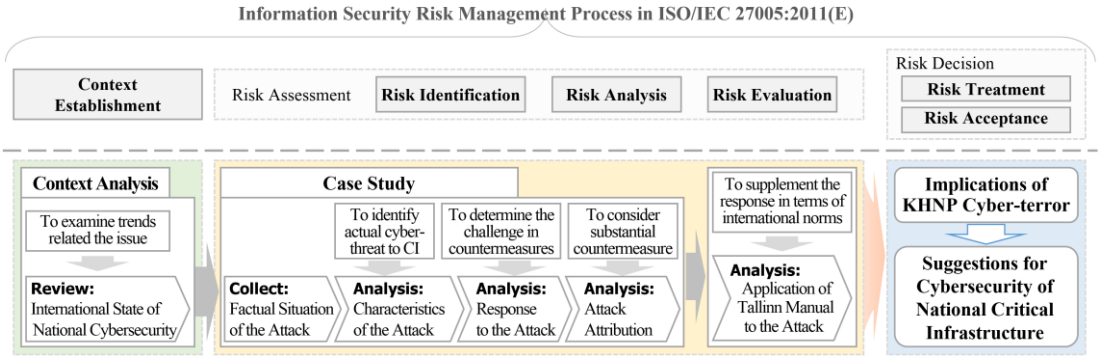

Fig. 1. Research Procedures

3. State of National Cybersecurity from an International Perspective

3.1 Intensified Cyber Threat and Progress of National/International Response

Because of the large number of cyberattacks that have been carried out since 2000, cybersecurity is considered to be an important issue in the maintenance of an information-based society. However, the dangers of cyberattacks have increased in proportion to the importance of cybersecurity. Since 2010, the discovery of malware threats, such as Stuxnet, that are widely believed to have been developed by state-sponsored hackers, has led to the beginning of discussions on how nations may be behind of cyberattacks. After the Sony hack in 2014, the U.S. announced tough sanctions against North Korea (hereafter referred to as "NK"), and countermeasures against cyberattacks became a major concern at the national level. With the increasing use of hacktivism, which involves the use of hacking as a means of social activism, as well as the increased number of cyberattacks against governments, the issue has become a national security threat. Recently, following cyberattacks such as the hack on France TV5 Monde by the Islamic State organization, cyberattacks are considered to be more

of a threat to international security.

With the increasing severity of cyber threats, many states and international organizations have begun to take responsive measures. Cybersecurity-related cooperation between international organizations has also started to materialize, as shown in **Table 1**.

Table 1. Recent National/International Responses to Cyber Threats

Subject	Responsive Measures
UN	Adopted recommendations for international cybersecurity through the UN Group of Governmental Experts (UN-GGE) in 2013.
NATO	• Specified that cyberattacks had become a threat to its allies, in accordance with the *Lisbon Summit Declaration* in 2010. • Agreed that cyberattacks on one or more members should be considered an attack on all allies, in accordance with the *Wales Summit Declaration* in 2014, and based on the provisions for "collective defence" in *NATO Article 5*.
EU	In the process of implementing the *Directive on Network and Information Security* to help establish its members' cybersecurity systems, as per the *Cybersecurity Strategy of the European Union* (2013).
EU & NATO	Discussed the potential for cooperation in response to Russia's hybrid warfare, which includes cyberattacks.
U.S.	Since the *2015 State of the Union* address by President Barack Obama stating that cybersecurity is a major agenda item, national cybersecurity has been reinforced at the federal level. • *Executive Order 13687* places sanctions on NK in response to the cyberattacks attributed to NK. • *Executive Order 13691* encourages and promotes cybersecurity threat information sharing within the private sector and between the private sector and government. • *Executive Order 13694* defines a cyberattack as a national emergency, and proposes severe punishment for hackers and their accomplices.
U.K.	• Has strengthened the government's cybersecurity and countermeasures against cyberattacks according to the *UK Cyber Security Strategy* (2011). • Has developed additional capacities to effectively counter cyberattacks by forming the Joint Cyber Reserve and the CERT-UK.

3.2 Re-emergence of the Importance of Critical Infrastructure Protection

When handling recent cyber threats, the most prominent issue has been the cybersecurity in the CI systems. This had already been recognized as a major military-related issue 20 years ago after the Oklahoma City Bombing in 1995, and was considered a national security agenda item following publication of the *Critical Foundations: Protecting America's Infrastructures* by the U.S. Presidential Commission on CIP in 1997 [5]. However, in 2000, some experts expressed the view that the threat of the Digital Pearl Harbor had been overstated, and was not a real issue [6]. Therefore, discussions on the matter did not progress any further.

However, as malware such as Stuxnet and Dragonfly, which were capable of causing physical damage, were detected worldwide, the cybersecurity of the CI resurfaced as a security issue among advanced countries. The U.S. issued *Executive Order 13636* to improve and reinforce the CI's cybersecurity, and *Presidential Policy Directive 21* to address the role of government agencies in order to ensure the effective implementation of this order. With the establishment of the *Cybersecurity Framework*, which is intended to decrease cyber threats to the CI, and the *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, which is a new CIP plan, the U.S. began to reorganize its cybersecurity system for CI. The UK is establishing a "cybersecurity hub" for threat-information sharing with CI's operators, and it has also formed a joint communiqué that regulates joint training and information sharing pertaining to the CI's cyber threats.

International discussions about the issue have also become more substantial. At the *Hague Communiqué*, which was adopted by the *Nuclear Security Summit 2014*, world leaders agreed that systems/networks of NPPs needed protection in order to address the growing threat of cyberattacks.

3.3 Threat to International Security: NK's Repeated Cyberattacks

With the continuous emphasis by Kim Jung-un on cyber warfare as one of the three major means of warfare, recent military threats by NK have been extended to cyberspace. The Heritage Foundation, which is an influential think tank in terms of policy decisions adopted by the U.S., has analyzed NK's cyber-warfare capabilities, and it has reported that they are a real threat to the vital interests of the U.S. [7].

Cyber warfare is used by NK as its main military force and strategic weapon [8], and it appears to have been recently adopted as a means of resolving economic sanctions [9]. NK has also taken advantage of its isolated condition by becoming a "cyber-hired gun, paid to conduct attacks or provide plausible deniability for other "cyber have nots" from other states to terrorist or criminal organizations[1] [10]." This is somewhat problematic, as NK appears to be interested only in displaying its confidence in its capabilities to launch cyberattacks, and not in following international norms [9].

In order to resolve NK's cyber threat, the U.S. has already switched from its strategic policy of tolerance to a more uncompromising policy, as per *Executive Order 13694*. However, it is doubtful that the international economic sanctions on NK will produce the intended economic and political consequences [9]. Cyberattacks may not cause much damage to NK because of its closed social systems and low level of cyber-infrastructure [11][12]. Therefore, there is a need for discussions among the international community to determine how to address NK's cyber threat.

4. Case study of KHNP Cyber-terror Attack

4.1 Significance of KHNP Cyber-terror Attack

The KHNP cyber-terror attack was an attack against the CI of the ROK, and it was assumed that NK was the source of the attack. Further, it stimulated discussions about the need to re-examine the CI's cybersecurity and make improvements to the national cybersecurity system in the ROK. The incident was characterized by keywords that are common when referring to recent international cybersecurity issues, such as "cyberattack by nation," "counteractions at the level of national security," "cybersecurity in CIP," and "NK's cyber threat." As it is a representative example of recent cyber threats, we need to analyze the problems and solutions of this attack.

Given the characteristics of the KHNP cyber-terror attack, the responsibilities and responses of nations should be discussed at an international level. In this study, we conducted a case study to determine the significance of the KHNP cyber-terror attack, based on these implications.

[1] This means that NK has become an agent who carries out cyberattacks or cyber terrorism for monetary gain, on behalf of other nations, terrorists, or criminal organizations that want to conduct attacks or terrors, but which do not have the capability. In addition, it means that NK provides plausible deniability to other nations, terrorists, or criminal organizations that do not have plausible deniability in cyberspace. Because NK is one of the most tightly controlled and closed societies in the world, there is some degree of plausible deniability regarding their cyberattacks.

4.2 What happened to KHNP?

On December 17, 2014, the online media reported an incident [13] in which an attacker, who was allegedly a part of NK's hacker groups, sent phishing emails to KHNP employees with malware that had the potential to destroy data, after which threats were made to the ROK government that leaked data regarding NPPs would be publicized via the internet.

The incident was first acknowledged at about 2 pm on December 9, 2014, when the phishing email was discovered in the email inboxes of employees at Wolsong NPP. Upon discovering questionable "Hangul" document files with malware, KHNP targeted the malware in cooperation with AhnLab. Although some computers were damaged in the process,[2] the operations of NPP were not compromised, and the incident was therefore initially treated as an uncomplicated cyberattack that was not made public. However, the details were revealed on December 15, 2014 when the attacker publicly posted personal information of all of the KHNP employees, as well as data related to NPPs on an online blog, after which the online media was tipped off. By August 3, 2015, there had been nine incidents involving data leakage and their corresponding threats, making the incident a serious cyber threat to the ROK society.

As it became public knowledge that the first phishing email was sent only to KHNP employees, and that the discovered malware did not result in information theft, it was assumed that the data publicized by the attacker must have been leaked through other channels prior to the incident. An announcement of interim findings made by the Government Combined Investigation Unit on Personal Information Crime (GCIU-PIC) [14] then revealed that the preliminary cyberattacks had been carried out on KHNP's partners and retirees, and that the data leaks had actually taken place prior to September 2014.

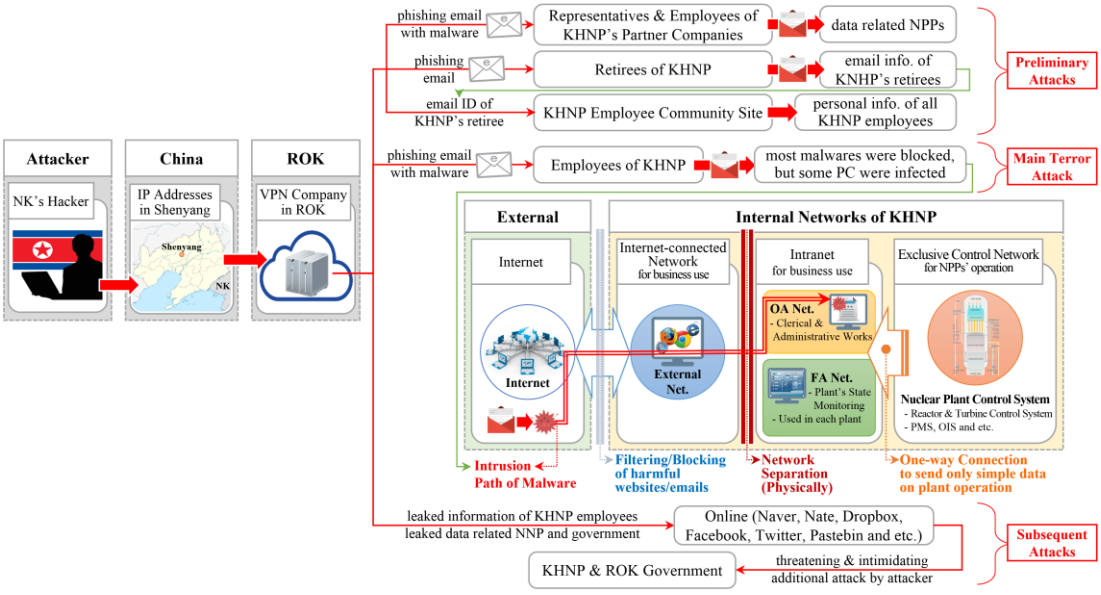

Fig. 2. Details of KHNP Cyber-terror Attack

[2] Eight KHNP computers were infected with malware. Of these PCs, five hard-disks were initialized and four PCs (three on an intranet and one connected to an external network) were damaged.

4.3 Characteristics of KHNP Cyber-terror Attack

4.3.1 Nature of the Cyberattack

The KHNP cyber-terror attack was marked by several complex characteristics. It was considered to be a "social attack" which is a combination of a "social engineering attack" and a "psychological cyberattack" [15]. Given the attack's mode of operation, it was also an "advanced persistent threat (APT) attack" that involved complex and sophisticated code [16]. Because NK was eventually determined to have been both directly and indirectly implicated in the attack, it can also be considered as a "state-sponsored cyberattack" [17][18]. Finally, because it had the potential to cause substantial damage to CI, the event may be categorized as a "cyber-terror attack" [19].

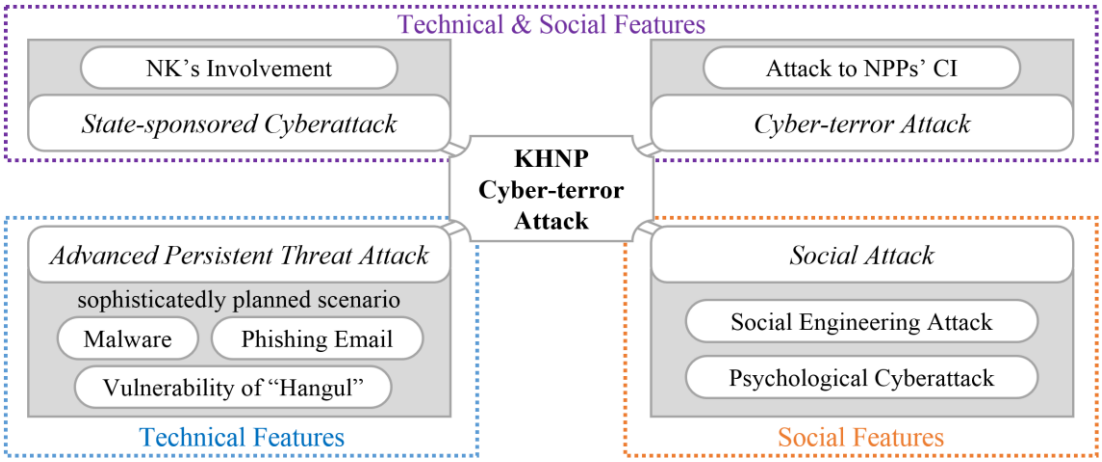

Fig. 3. Characteristics of KHNP Cyber-terror Attack

4.3.2 Features from a Technical Perspective

From a technological perspective, the attacker used three methods: 1) malware, 2) exploitation of Hangul's vulnerability, and 3) phishing emails.

1) **Malware:** The attacker used different malwares to realize their goal. In the preliminary attacks aimed at data collection, malwares with the ability to leak data were used, while in the cyber-terror attack, malware with the ability to destroy data was used. This implies that the attacker did not attack randomly, but instead sent the malware to specific targets for specific purposes. It was revealed that the latter malware was capable of destroying data in the same manner as a time bomb. In other words, it was set to cause the malfunction of systems/networks up to a certain point in time, after which it would destroy the systems' master boot records (MBRs). The attacker's intention thus appears to be clear.
2) **Vulnerability of Hangul:** Hangul's vulnerability was exploited during the installation and execution of the malware. Hangul is an essential Korean word processor that is widely used by the government of the ROK, and the cyberattack was regarded as a customized attack targeting the ROK. Because Hangul's vulnerability has been exploited several times in cyberattacks carried out by NK, it was considered to be useful information in determining the attacker's identity.
3) **Phishing Emails:** Several different malwares were circulated and data were collected through the use of phishing emails. During the preliminary attacks, phishing emails with a false message requesting password changes were sent out, and the email passwords of

some KHNP retirees were thus leaked. Furthermore, during the attack, phishing emails that were disguised as ordinary business emails spread the malware to computers of KHNP employees and KHNP's partners. Phishing emails make it difficult for an ordinary person to recognize their hidden dangers and the ability to detect these emails is limited, the attacker may therefore have used phishing emails.

In addition, the attack routes involved China and the ROK. The IP addresses of the phishing emails were based in Shenyang, China. During the attacks, the attacker accessed Naver.com and Twitter.com, and posted threatening messages using the IP addresses of Shenyang area through a Korean VPN company. These characteristics indirectly revealed the attacker's intention to hide their location and conceal the cyberattack.

Table 2. Technical and Social Evidence of NK's Involvement in KHNP Cyber-terror Attack

View	Evidence	Logical Basis
Technical	Resemblance of malware	The malware was very similar to "Kimsuky" malware [20]. • Kimsuky malware is known to be used by NK's hackers. • The inner shellcode's operation, command architecture, and remote access code of the malware were similar.
	Similarity of SW vulnerability and timing	In the preliminary attacks, the malware used zero-day bug of Hangul. • This vulnerability has been used in Kimsuky malware since May 2014. • As the vulnerability patch was issued in November 2014, it is unlikely that others would have developed malware using the same vulnerability within the short period of six months.
	IP address similarity	IP addresses used for the attack were found to include the range of IP addresses from Shenyang, China. • Shenyang's IP address range was supposedly used by NK's hackers. • The IP range had the same 9 digits as the one used by Kimsuky malware.
	IP addresses used by NK	As determined by the VPN Company in ROK, the details of the attacker's IP access include North Korean IP addresses. • NK's 24 IP addresses and 5 IP addresses which have been allocated to a communications company affiliated with NK's Ministry of Post.
	Parallelism of attack method	The malware destroyed HDDs' MBR by overwriting special characters. • This technique was also used in the 3/20 cyberattack in 2013 and the Sony hack in 2014 [21].
Social	"John," the name used by the attacker	The attacker used the name "John" on Twitter (ID: john_kdfifj1029) and Facebook (name: Jenia John). In addition, the Hangul file used in the attack was finally modified by "John." • The user ID of the North Korean computer used in the 3/20 cyberattack was also "John." • "John" is often the name associated with the email accounts used in NK's targeted attacks.
	Specific vocabulary	The attacker used certain Korean words, such as "u-ttul-ga-yo," "a-nin-bo-sal," "yo-rok," "hu-gwa," and "han-ji" (meanings are "how is this," "pretending to not know," "summary," "results" and "place to not hide" respectively). • These words are used mostly by North Koreans and Korean-Chinese persons, and are rarely used in the ROK.
	Attacker's messages and their characteristics	While the attacker appeared to desire nuclear disarmament on a superficial level, threatening messages were posted toward the ROK government, which provoked fear and anxiety because of the use of words containing negative connotations. • The attacker may have carried out such behavior for the purpose of causing social unrest. • Considering the possible benefits that the attacker may have gained after the success of the attack, we can speculate that the attacker may have been from NK.
	Similarities in psychological behavior	As was the case with the phrase "Who Am I?" that appeared during the cyberattack, the attacker indirectly repeated the question of his identity. • This behavior is similar to the psychological warfare techniques employed in the 3/20 cyberattack and the 6/25 cyberattack in 2013. • The behavior appears to be similar to the cyber-psychological warfare that NK is known to pursue against its southern counterpart.

4.3.3 Features from a Social Perspective

At the macroscopic level, the KHNP cyber-terror attack was a serious cyberattack that affected national security, and at the microscopic level, it was a threat to the privacy of KHNP employees. Thus, the KHNP cyber-terror attack is very significant from a social perspective. Because China and NK were both believed to have been involved in the attack, it should be addressed as an international societal issue.

It is notable that the KHNP cyber-terror attack involved an attack technique having social characteristics, namely social-engineering and psychological cyberattacks. First, the attacker conducted a social-engineering attack using phishing emails, through which they identified targets and stole data needed for a future attack. In other words, the social-engineering attack played an essential role, and is an important component of such attacks.

Second, the attacker threatened the ROK society using psychological cyberattacks employing the media and the social media. After the failure of the initial email attack, which also remained unpublicized, the attacker tried to make the society aware of the cyberattack by using press reports. Moreover, there was a continued attempt to disrupt the society by consistently releasing leaked data that was believed to have been important, and by issuing additional threats via the press and Twitter. These psychological attacks may be considered as forms of cyber provocation and deceptive strategies. The attacker also pretended to oppose the building of NPPs, thereby superficially piggybacking on a socially sensitive issue to mask the real intention. This tactic may therefore also be considered as a form of psychological attack.

4.4 Attack Attribution

Because the attacker used the name, "No Nuclear Power Plant Group," it was initially assumed that the guilty party was an environmental activist group. The GCIU-PIC subsequently discovered evidence that the attacker had a connection to NK, and indicated that NK was behind the attack [14]. To arrive at this conclusion, there were five pieces of evidence from a technical perspective, as well as four pieces of evidence from a social perspective, as shown in **Table 2**.

Regarding the results of the interim investigation carried out by the GCIU-PIC, NK regarded the result as ridiculous, and asserted that they had not committed the attack [22]. However, given the aforementioned evidence, as well as NK's recent actions that openly show its intention to undertake cyberwar [23], it was concluded that NK was closely linked to the event.

5. Application of Tallinn Manual to KHNP Cyber-terror Attack

5.1 Tallinn Manual

To efficiently resolve conflicts in cyberspace, it is necessary to thoroughly analyze certain specifics and the nature of the conflict. Because cyberspace is not defined by physical national borders, the analysis requires an international perspective. We analyzed the significance of the KHNP cyber-terror attack on international norms using the Tallinn Manual [3].

The Tallinn Manual is meaningful in that it confirmed that the existing international laws are applicable to cyberspace. As in the Tallinn Manual, we may consider the recommendations of the UN-GGE [24], as another approach to dealing with cybersecurity from the perspective of international security. There is some significance to the UN-GGE's recommendations in that it comprises the first international agreement on cybersecurity for international security,

and confirms the applicability of existing international norms for cyberspace, as is the case with the Tallinn Manual. However, the UN-GGE's recommendations indicates the need for more rigorous discussions on the application of the norms, as it states that "Common understandings on how such norms shall apply to State behavior and the use of ICTs by States requires further study [24]." In comparison, the Tallinn Manual incorporates all the different opinions on cyber-related issues that have not been agreed upon by experts. Therefore, it enables a more flexible analysis of cyberattacks from the perspective of international norms.

Considering the current need to discuss the establishment of international norms on cybersecurity, it is appropriate to flexibly apply the Tallinn Manual instead of the UN-GGE's limited recommendations when considering any possible response to the KHNP cyber-terror attack. Moreover, while the Tallinn Manual is a reference that is not legally binding, its fundamental logic is identical to that of the UN-GGE's report and it encompasses all related legal issues, thus, its significance should not be disregarded [25].

5.2 Application of Rules

The Tallinn Manual is important in that it confirms that *jus ad bellum* and *jus in bello* may be applied to cyber warfare [25]. It may therefore be necessary to consider Rules 11, 13, and 30 of the Tallinn Manual when examining the nature of the KHNP cyber-terror attack.

5.2.1 "An Attack" based on the Law of Armed Conflict

According to Rule 30, the KHNP cyber-terror attack was a cyber "attack" that was based on the law of armed conflict. As the means of carrying out the attack, the malware was capable of interrupting the control systems of NPPs, and this function of the malware represents "effects that are caused," which is the crux of the notion in defining a cyberattack. Although the malware was blocked and did not cause much damage, it is believed that it could have interrupted the operations of control systems because the control network had been already infected by other malware. Thus, the event may be regarded as a "cyberattack."

Furthermore, according to the Tallinn Manual, the definition of a cyberattack includes (1) "interference with functionality that necessitates data restoration, while not requiring physical replacement of components or reinstallation of operating system," (2) "a cyber operation does not actually result in the intended destructive effect," and (3) "an attack that is successfully intercepted and does not result in actual harm." Therefore, our conclusion may therefore be deemed reasonable.

5.2.2 "Use of Force" from the Perspective of International Law

According to Rule 11, the KHNP cyber-terror attack may be regarded as the "use of force." In international law, the "scale and effects" matter when determining whether particular actions amount to a use of force. Because the KHNP cyber-terror attack did not cause serious damage, such as human casualties or the loss or destruction of property, it is difficult to designate the event as one that exhibited the use of force.

Then, we evaluated the KHNP cyber-terror attack using the Schmitt Criteria [26][27], which is an approach that was proposed in the Tallinn Manual in order to characterize cyber operation as the use of force. We also considered actual measurements that were proposed by James B. Michael et al. (2003) [28]. **Table 3** shows an evaluation of the KHNP cyber-terror attack. By combining these assessments, the evaluation score of the KHNP cyber-terror attack was 5.25, which is located in the mid-range of the scale, and is not sufficient for the event to be considered a use of force. We therefore assumed that it may be difficult to describe the event as a use of force.

Here, we examine some additional criteria that were suggested by the Tallinn Manual. First, in terms of the prevailing political environment, the ROK is a divided nation that is opposed to NK, and is constantly subject to NK's military threats. Thus, although the cyberattack and its end result were not kinetic, they should be viewed as a serious threat. Second, it may be advisable to consider the attack as a use of force as NK is presumed to have been the attacker, and in recent times, international society has responded to its cyberattacks. Third, given the record of cyberattacks by the presumed attacker, this event may be considered to be a part of NK's prolonged and continued cyberattacks. Therefore, it may be necessary to discuss whether or not the attack can be categorized as the use of force. Fourth, with respect to the nature of the target, the attack targeted NPP facilities and it was therefore serious and dangerous. Considering all of the above, the KHNP cyber-terror attack may be regarded as the use of force, even if its "scale and effects" are not sufficient to individually meet the criteria.

Table 3. Application of Schmitt Criteria to KHNP Cyber-terror Attack

Factor	Level (Rating)[3]	Reason
Severity	Low-high (3)	There was no physical damage, but the CI was targeted.
Immediacy	Medium-medium (5)	The effect was negligible, but the event happened quickly.
Directness	High-low (7)	There was causal connection between the start (e-mail attack) and the result (destruction and leakage of data) of the event.
Invasiveness	High-medium (8)	High level of protective measures had been implemented in KHNP
Measurability	Medium-medium (5)	The effect of the attack was insubstantial but measurable.
Military Character	Low-medium (2)	The event is only indirectly related to military intentions.
State Involvement	Medium-high (6)	There exists only circumstantial evidence to show NK's involvement.
Presumptive Legality	Medium-high (6)	The event targeted NPPs, against which attacks are prohibited.

5.2.3 "An Armed Attack" from the Perspective of International Law

According to Rule 13, the KHNP cyber-terror attack may be considered to have been an "armed attack," which would give the right of self-defense to the targeted nation. When interpreting cyber armed attacks, the Tallinn Manual places great importance on whether or not the results of the attack are similar to kinetic armed attack. Because the damage from this attack was not physical and the effect was negligible, it is unlikely to be interpreted as an armed attack.

However, in the Tallinn Manual, some experts defined an armed attack as a "cyber operation directed against major components of a State's CI that causes severe, albeit not destructive, effects," as per "the extent of the ensuing effects." Thus, there is a small possibility that the KHNP cyber-terror attack may be considered as an armed attack. Moreover, because the attacker's intention and the effects of the attack are clear, and that "all reasonably foreseeable consequences" and "whether the effects in question must have been intended," it may be considered as grounds for defining the event as an armed attack.

Given that experts do not agree on whether or not the physical damage caused by Stuxnet

[3] Each factor was evaluated in three stages (high: fully reflected, medium: reasonably reflected, low: insufficiently reflected), and each stage was evaluated qualitatively (high: existence of the specific item being considered, medium: relative consideration, low: low consideration), on a nine-point scale. The mean value of the numeric-ratings was calculated and used to determine whether the event could be categorized as a use of force.

met the criteria for an armed attack [3], it may not be meaningful to pursue discussions regarding the classification of the KHNP cyber-terror attack as an armed attack. However, because there is no clear international agreement on the definition of a cyber armed attack, it is possible that the KHNP cyber-terror attack may be considered as an armed attack.

5.2.4 "State Responsibility" as per International Law

Furthermore, it is necessary to consider Rules 5, 6, and 8, which describe national responsibilities according to international law. First, because the KHNP cyber-terror attack may be considered "a cyberattack" and "the use of force" according to international norms, it may be possible to assign international legal responsibility to NK for breaching an international obligation as per Rule 6. Because the association between the attacker and NK is merely presumed, and up to the present, there has been no reported direct relationship of this nature, it may be difficult to assign responsibility for the attack to NK. However, given NK's closed nature and the U.S.'s sanctions after the Sony hack in 2014, it may be reasonable to demand that NK bears responsibility.

Second, according to Rule 5, it may be possible to demand that China also accepts some of the responsibility. Had China been aware of NK's use of the infrastructure in China, while failing to address the situation, this may also be considered as a violation by China of international law [29]. Because it is unlikely that China, which is a carefully controlled socialist nation, had no knowledge of another nation's activities within its own territories, such a demand may be reasonable. While Rule 8 states that the fact that an attack routed through a state cannot be sufficient evidence for attributing the attack to that state, some experts have proposed that if the states fail to take reasonable measures to prevent the transit, then the state should bear responsibility. Considering these experts' opinions, it may then be possible to hold China indirectly responsible.

6. Implications from Case Study

6.1 Substantive Awareness of Cyber Threats against NPPs

The KHNP cyber-terror attack is significant because it provided the government of the ROK with an opportunity to actually acknowledge cyber threats to the CI, such as NPPs, which are vital to the nation.

There had been several previously issued warnings regarding the cybersecurity system of KHNP. In 2012, the Board of Audit and Inspection (BAI) highlighted many problems, such as the presence of 88 arbitrary connections between the exclusive control network of the NPPs and the intranet, the lack of control over USBs on the control network, the detection of 148 different bits of malware in the exclusive control network, and the neglect of 118 identified vulnerabilities [30]. The internal audits performed by KHNP in 2013 [31] and 2014 [32] revealed similar problems, such as unregistered storage media, neglected USBs that were for business use, and inadequate information security in place by its partners.

While most of these problems could have been solved utilizing simple measures, the low security awareness of KHNP, the closeness of organizations related to NPPs, an inadequate budget, and insufficient regulatory control prevented them from being resolved, and they were incorrectly reported as having been resolved. According to reports from inspections of the National Intelligence Service (NIS), the internal security of KHNP and the security management of its subcontractors received almost perfect assessments during the period

2013-2014 [33].[4] In other words, even though the ROK's NPPs were vulnerable to potential cyber threats, they were not considered to be problematic because the government and KHNP were not aware of the seriousness of those problems.

Because of the KHNP cyber-terror attack, pre-existing cybersecurity problems regarding NPPs were again reviewed. The ROK government and society became acutely aware of the need to strengthen the cybersecurity system of the overall CI, and discussions for more effective programs are ongoing.

6.2 Effectiveness of Existing Cybersecurity System

As the society directed its attention to the cybersecurity of NPPs, the effectiveness of existing cybersecurity systems became the most discussed issue in the press media and academia in South Korea. Although KHNP had a high-level cybersecurity system as per the CIP, as a result of this incident, several questions were raised as to whether the cybersecurity system of KHNP was being properly maintained.

6.2.1 Poor Security of Network Separation

The first question is: Was the network separation secure? KHNP had made claims that external cyberattacks would be virtually impossible because the intranet and Internet were physically separated, and that the control network of the NPPs was completely isolated.

However, during this incident, malware was transmitted to computers on the intranet, and according to an internal audit done in 2015 1Q, there were 77 cases that violated the network-separation policy [35]. These facts proved that KHNP's claim was not reliable. The effectiveness of KHNP's network-separation system is particularly questionable as KHNP claimed to have corrected the network-separation violation detected in the 2012 audit highlighted by the BAI.

6.2.2 Uncontrolled Use of External Storage Devices

The second question is: Were external storage devices properly controlled? After it was realized that Stuxnet had accessed NPPs' control systems via the use of USBs, enforcing restrictions on the use of external storage devices became an essential step for CIP.

However, through an on-the-spot survey, malware that was unrelated to the KHNP cyber-terror attack was discovered on many USBs drives utilized on NPPs' control networks, and old malware, such as Conficker, was discovered in control systems. This discovery showed that the use of external storage devices was being poorly managed. Given that these security issues had already been noted in the BAI's 2012 audit and KHNP's 2014 self-audit, we can assume that while KHNP was aware of the problem, it did not make the necessary effort to resolve the issue.

6.2.3 Need for Comprehensive Approach (Technical - Administrative)

The two issues mentioned above are only some of the problems identified with KHNP's cybersecurity system. A proper analysis of the effectiveness of KHNP's cybersecurity system requires a more comprehensive approach that addresses both technical and administrative security perspectives.

[4] Evaluation scores of KHNP's internal security were measured as 100 in both 2013 and 2014 by NIS's inspection. Given that the average scores in public enterprises are 95.56 in 2013 and 88.89 in 2014, KHNP's internal security was considered to be at a very high level. In addtion, the security management systems employed by scores of KHNP's subcontractors received scores of 90.48 (2013) and 100 (2014), while the averages are 84.37 (2013) and 84.07 (2014).

Technical protection requires general inspections and revisions of security systems and their operation, focusing on the problems identified, such as the use of anti-virus software for detecting and preventing malware, email-protection systems for blocking malicious email and preventing information leakage, document-management systems for preventing information leakage, and process interception systems for intercepting malware processes.

In terms of administrative security, a comprehensive review of cybersecurity policies, organizations, manpower, budget, and cybersecurity-related education is required in order to resolve existing problems such as the absence of a dedicated cybersecurity unit, lack of human resources and budget, and low levels of expertise [35].

6.3 Identification of Problems Faced when Countering Cyberattacks on CI

As the responses by KHNP and the government were carried out publically, previously undiscovered problems regarding responses to cyberattacks on the CI were revealed.

6.3.1 Problem 1 - Unclear Role of Government Agencies

Because the departments involved did not have clearly assigned roles, there was some degree of confusion during the initial response, and agencies that were tasked with resolving cybersecurity issues were not able to carry out their functions.

During the early stages of the incident, the police requested search-and-seizure warrants from prosecutors. However, the prosecution rejected their demands, delaying the investigation by about one week. Similarly, NIS, which was tasked with examining the CI's cybersecurity, could not perform an examination because of the refusal by KHNP. The Korea Internet and Security Agency, which is the agency responsible for information security, did not act at all as its jurisdiction was limited to the private sector.

6.3.2 Problem 2 - Limitations of National Cybersecurity Control Tower

The national cybersecurity response system was established in response to the *National Cyber Security Comprehensive Countermeasures* (2013), where the Blue House was assigned responsibility for the control tower, NIS was assigned the role of managing practical affairs, and each Ministry and office concerned was assigned duties related to their respective sectors.

However, the limitations of this system were subsequently revealed. While the control tower should have begun the response from the onset, the central government only began to perform serious countermeasures on December 22, 2014, which was two weeks after the event took place. Even then, it appeared that the control tower lacked the capabilities to perform its functions. Its responsibilities were carried out by the Cyber Crisis Response Team of the Office of National Security under the Blue House, which comprised only five persons, and this is not adequate considering the scale of the nation-wide project. The team did not have the adequate capacity to share information and work together with the different departments and organizations involved in the process of implementing countermeasures.

As the regulatory agency that is responsible for the safety aspect of NPPs, the Nuclear Safety and Security Commission (NSSC) had an ambiguous position in this response system. Given that expertise in relevant fields is crucial when coping with any incident, the NSSC should have provided more rigorous support to the control tower. According to the *Enforcement Decree/Rule* of the *Act on Measures for the Protection of Nuclear Facilities, ETC. and Prevention of Radiation Disasters*, which was revised in December 2013, the NSSC's responsibilities extended to "cybersecurity regarding the operation and control system of NPPs." Therefore, the NSSC should have been more active in its response to the event. However, its activities were limited to supporting the Ministry of Trade, Industry, and

Energy (MOTIE) and the NIS.

6.3.3 Problem 3 - Absence of Manuals Related to Cyber-crises

The NSSC and MOTIE prepared a manual for managing crises pertaining to the security of NPPs. However, this manual addressed only two issues, "radioactive leakages" and the "discontinuation of operation of NPPs in the event of a walkout." Thus, no systematic responses could be made to an incident such as the KHNP cyber-terror attack.

In other words, it may be assumed that the two aforementioned problems resulted from the absence of manuals specifying the countermeasures for cyber-terror-related incidents. In particular, the parliamentary audit in 2013 revealed that none of the 23 NPPs in the ROK had formulated a cybersecurity plan that included a manual for responding to cyberattacks [36]. Following that inspection, cybersecurity implementation plans for the NPPs were scheduled to be completed by December 2014, but the results have not yet been confirmed since the response to this latest event.

6.3.4 Problem 4 - Problems with KHNP Response

Several problems were identified in the response by KHNP to this incident. First, its preventative measures had failed. There were already signs of a malware invasion in the control network, albeit not involving the malware used for the KHNP cyber-terror attack. Second, its responses were delayed. KHNP's initial response on December 9, 2014 progressed quickly, but slowed thereafter. KHNP requested a formal investigation 10 days after the incident, and it was not able to quickly identify the nature of the leaked data or the loopholes that caused their leak, hence prolonging the response to the incident. Third, KHNP reacted idly and did not appear to have taken the matter seriously. It continuously claimed that the released data were not important, and that there was no risk of danger to the targeted NPPs because its networks were isolated.

6.4 Confirmation of the Need for Substantial Cooperation

The KHNP cyber-terror attack indicated the need for diversified cooperation when responding to cyberattacks on CI.

6.4.1 Need for Effective International Cooperation

First, substantial international cooperation regarding cybersecurity is deemed to be necessary. During the investigation, Chinese IP addresses were identified, and the GCIU-PIC asked the Chinese government for judicial assistance. The Chinese Ministry of Foreign Affairs responded positively, and China's Ministry of Public Security informed the ROK's Supreme Prosecutors' Office that the incident had been handed over to the Cybersecurity Defense Division on December 30, 2014. Thus, it had initially appeared that there would be hope of tracking down the attacker. However, since then, China has stopped corresponding.

This result had been expected. Although the relationship between China and NK has recently become estranged, it was expected that China would have stood by its long-standing friendship with NK, and that NK would focus on its relationship with China. China's response therefore appears to be a public gesture motivated by its "strategic cooperative partner relationship" with the ROK, and it may therefore be necessary to build an international system of cooperation to ensure substantial mutual aid beyond this kind of superficial cooperation.

6.4.2 Need for Public-Private Cooperation

This event suggests that public-private cooperation is necessary for information sharing and to receive expert support from the perspective of the CIP. Soon after the incident, there were

requests for an immediate investigation and an analysis on the state of cybersecurity in the overall CI, but KHNP was unable to mount an effective internal response. Of all the KHNP employees (19,693 persons), there were only 53 cybersecurity personnel (0.26%), and of these, only nine employees (0.046%) were dedicated to cybersecurity-related tasks; the other 44 employees either had other simultaneous responsibilities (35 persons) or belonged to external companies (9 persons) [35]. Thus, in dealing with major cyber threats targeting the national CI, there is a need for a public-private cooperative system that can mobilize outstanding capabilities in the private sector to support the government's preparations for cybersecurity, and to act immediately in the event of an incident.

Because information was leaked through KHNP's subcontractors, there is also a need for a reinforcement of the cybersecurity in this area. A cooperative system that is composed of CI administrators, the control system's vendors, and cooperating companies should be equipped with proper cybersecurity.

Table 4. Implications from Case Study on KHNP Cyber-terror Attack

Implication	Details
Substantive Awareness of Cyber Threats against NPPs	• The incident provided the ROK government with an opportunity to actually acknowledge cyber threats to the CI. • The ROK government became acutely aware of the need to strengthen the cybersecurity system of the overall CI.
Effectiveness of Existing Cybersecurity System	Arising from this incident, several questions were raised as to whether the cybersecurity system of KHNP was being properly managed, including: • Were external storage devices properly controlled? • Was network separation secure?
Identification of Problems Faced when Countering Cyberattacks on CI	Previously undiscovered problems regarding responses to cyberattacks were highlighted. These include: • The uncertain role of government agencies • The limitations of national cybersecurity control tower • The absence of counteraction manuals • Some problems in KHNP's responses
Confirmation of the Need for Substantial Cooperation	Diversified cooperation may be needed to respond against cyberattacks to CI: • Substantial international cooperation regarding cybersecurity • Public-private cooperation in information sharing and expert support from the perspective of CIP • Cooperative system among subcontractors

7. Suggestions for Strengthening Cybersecurity in National CIP

7.1 Improvement in Cybersecurity Awareness among All Concerned with CI

The importance of the human factor has already been highlighted in many previous studies concerning CIP [37]. However, the fundamental problems that were observed in the wake of this attack stemmed from the lack of an awareness of cybersecurity in general. In particular, KHNP had a vague cybersecurity awareness in that the assumption was made that it would have been secure from cyber threats, and it was therefore slow to respond to actual cyber threats. Thus, the importance of strengthening security awareness should again be emphasized among those persons/organizations responsible for CI.

Fostering a security awareness should be more helpful when resolving security problems other than technical/administrative security measures. In other words, the success of security measures ultimately depends on the actions and awareness of the stakeholders [38]. Besides, security awareness is a relatively low-cost protection mechanism with the potential for a high return-on-investment [39]. Therefore, cybersecurity awareness should be improved to

strengthen the cybersecurity of CI.

7.1.1 Focus on Improving Cybersecurity Awareness for CI

KHNP exhibited an unclear confidence in the security of its control network, and it was overconfident in its security measures employed, such as the network-separation policy. For this reason, to promote an understanding of its importance regarding all cyber threats that target CI, and to prepare personnel to actively respond to such threats, the security awareness should constantly be reinforced, and it should not be taken for granted that current systems/networks in CI are secure from emerging cyber threats.

Cybersecurity should be recognized as an important part of the operations in CI, to achieve an appropriate security level. In addition, a sound cybersecurity culture should be promoted by integrating it as a part of the organizational culture. The will of the leader should also be considered when improving the cybersecurity awareness for CI because it is necessary to prepare the foundations for raising the security awareness, and to provide the internal motivation for members to comply with the cybersecurity policy.

To realize these improvements in the cybersecurity awareness for CI, it should be understood that "cybersecurity" is an essential requirement at the same level as "safety" in CIP.

7.1.2 Measures and Subjects

Although a basic approach to creating and developing security awareness, one-way communication should be directed from authorities to a large population of single individuals using expert knowledge, as member participation is also important to change security awareness [40]. In other words, in order to enhance cybersecurity awareness, continuous training and education should be provided to all members. Continuous training and education will transfer the knowledge on the cyber threats and risks that exist in CI environments. Also they will share information on violations of security policy and their consequences, and enhance the responsibilities of members.

Furthermore, an individual's capacities for security are strengthened according to the appropriate policies and plans for cybersecurity, and they should therefore be made to observe regulations via incentives/punishments, as well as to improve their security awareness.

These measures should be applied not only to operators of CI such as KHNP, but also to all related parties. All related parties include the central government, which is responsible for establishing a national policy on CI, and various governmental organizations and public enterprises that are responsible for regulations and practical affairs. It also include the private sector as control system vendors and partner enterprises.

7.2 Establishment of National Cybersecurity Strategies for CIP

In order to solve the aforementioned problems, executive programs for CI cybersecurity should be continuously and systematically pursued, and should be based on continuous, long-term plans.

To this end, there is a need for the establishment of a national cybersecurity strategy for CIP, which determines the directions for national policies regarding CIP, and which provides concrete details and executive plans of various measures for protecting CI. This strategy should include all CIP activities, and should encourage cooperation and participation from the private sector. In addition, an adequate budget should be secured for the effective pursuit of activities proposed by the strategic action plan. Based on the suggestions above, topics included in the strategic action should be addressed in a national cybersecurity strategy for CIP

as follows.

7.2.1 Direction of Legal Modifications

First, the "direction of modifications to laws/regulations related to CIP" should be established. Before and after the incident, relevant bills were proposed, but they applied only to specific countermeasures, such as the collection of information and the establishment of a certain organization. Thus, comprehensive legal foundations for the cybersecurity of CIs could not be established.

Accordingly, with respect to the *Act on the Protection of Information and Communications Infrastructure*, the goal of revising the laws should be established through the strategy, and the legal systems should be improved following reasonable justification and systematic procedures.

7.2.2 Guidelines for Cybersecurity of CI

Moreover, the "establishment of administrative guidelines for CI's cybersecurity" should be planned strategically and proposed. The current guidelines are based on different individual aims, and the contents are incoherent. Consequently, the management and application of the guidelines are difficult. Administrative guidelines should be inclusively planned and proposed through the specification of strategic action plans in the strategy, so that various guidelines are related to each other and are implemented efficiently.

The KHNP cyber-terror attack revealed the need for specific guidelines, including response manuals for a cyber crisis, such as the cyberattack on the NPPs' facilities, security guidelines that define the practical and required level of information security for CI, and cybersecurity management guidelines for the operation of information security systems.

7.2.3 Education, Cooperation, and R&D

In addition, the national cybersecurity strategy should incorporate education systems for cybersecurity personnel in the CI sector, plans to establish various types of cooperative systems, and R&D roadmaps for developing cybersecurity technologies that are specific to CI.

7.3 Establishment of Diversified Cooperation for Cybersecurity

To adequately respond to cyber threats to CI, diversified cooperation is necessary, and continuous efforts should be made to establish substantial collaboration.

7.3.1 Focus of International Cooperation

Beyond only establishing cooperative relations, international cooperatives should work strategically with a strong focus on improving the unsatisfactory level of current cooperation. As was the case with to the *Seoul Conference on CyberSpace* (2013), the ROK should take the lead in establishing cybersecurity norms in international society, and in laying down the foundations for substantial cooperation.

International cooperation for preemptive defense should also be made a priority, as it is with nuclear problems, and the international society should come together to develop cyber-deterrence capabilities or increase information sharing regarding cyber threats through the Forum of Incident Response and Security Teams. Further, concrete cooperative mechanisms regarding cyber issues should be developed alongside developed countries that have already established such cooperative systems.

7.3.2 Establishment of Regional Cybersecurity Cooperation

Cooperative systems should be formed in regions such as Northeast Asia or Asia-Pacific. Northeast Asia is more frequently targeted for cyberattacks than other regions, and is highly vulnerable to potential security threats. Currently, cooperation between countries within this region focuses on technological cooperation at a low level, such as information sharing, discussion of standards, and joint training [41]. Thus, discussions concerning more substantial cooperation, such as confidence-building measures for cybersecurity, should be conducted on a regional level.

Moreover, to avoid the scrutiny of international society, NK is moving its hacking base, which is disguised as an IT company, to countries in Southeast Asia such Malaysia and Cambodia [42]. Given this situation, cooperative systems that can enhance the inadequate cyber apparatuses of those countries should be established, and foundations for efficiently countering cyberattacks that occur in those countries should be prepared.

7.3.3 Domestic and International Military Cooperation and its Coordination

On both domestic and international levels, we should discuss cooperation in terms of national defense. According to international norms, a cyberattack such as the KHNP cyber-terror attack, may merit some military counteraction. Thus, international military cooperation should be discussed to handle cyberattacks. Specifically, China does not have any protocol for military cooperation regarding cybersecurity, and they have appeared to be active in cooperating with the ROK in the areas of politics and technology, as of 2013 [41]. Thus, cooperation for cybersecurity should be discussed through appropriate channels for military cooperation, as with the *Seoul Defense Dialogue*.

Cooperation among private, public, and military sectors should be discussed domestically as a basis for international military cooperation. A serious cyberattack requires emergency support from the military in non-military areas, such as in the formulation of counteractions to terror/crises and social stability, as well as defense in militarized areas. Further, the cybersecurity capacity in the private sector is more specialized and at a higher level of expertise than in the military and public sectors. Thus, in response to catastrophic cyber-crises targeting CI, government should take the lead in establishing cooperative systems that can efficiently utilize the functions of the military and the capacity of the private sector, mediate the roles of each sector, and support communication between them.

7.3.4 Development of Government-Industry-Academic Cooperative System

In terms of CIP and information security, government-industry-academic cooperation is required because cyberattacks may be resolved by understanding cybersecurity technology and using it effectively. Accordingly, to achieve R&D in the area of cybersecurity technology that is required at the national level, government should support industrial, academic, and research institutions in the field of information security.

Government should also strengthen the cybersecurity capabilities of partners that manufacture, manage, and repair systems/networks of CI. In addition government should establish cooperative systems for supply chain cybersecurity, where cooperating companies may participate in the enforcement of the CI's cybersecurity, such as the prevention, preparation, response, and recovery against cyberattacks, including performing weakness/vulnerability analyses and cybersecurity R&D. The cybersecurity industry sector should also assist other organizations regarding the detection and response to cyber threats.

7.4 Systematic Implementation of Cybersecurity Technology R&D for CIP

In order to significantly strengthen the cybersecurity of CI, cybersecurity technology is required. Government and operators of CI should identify essential cybersecurity technology needed for CIP, set up a roadmap to pursue its R&D, and carry out the R&D accordingly.

7.4.1 Specialized Cybersecurity Technologies for Control Environment in CI

The development of cybersecurity technologies that are specific to the control environment of CI should be given priority. While some security technologies have already been developed for control systems, even basic security technologies such as encryption cannot be applied to systems in a control environment. Thus, cybersecurity technologies that can be applied to the overall control system should be researched strategically.

By carrying out extensive testing, they should also be developed into stable technologies that do not interrupt the operations of CI. This R&D requires an understanding of each individual control system as well as expertise in information security, and therefore should involve cooperation between control system vendors and security companies.

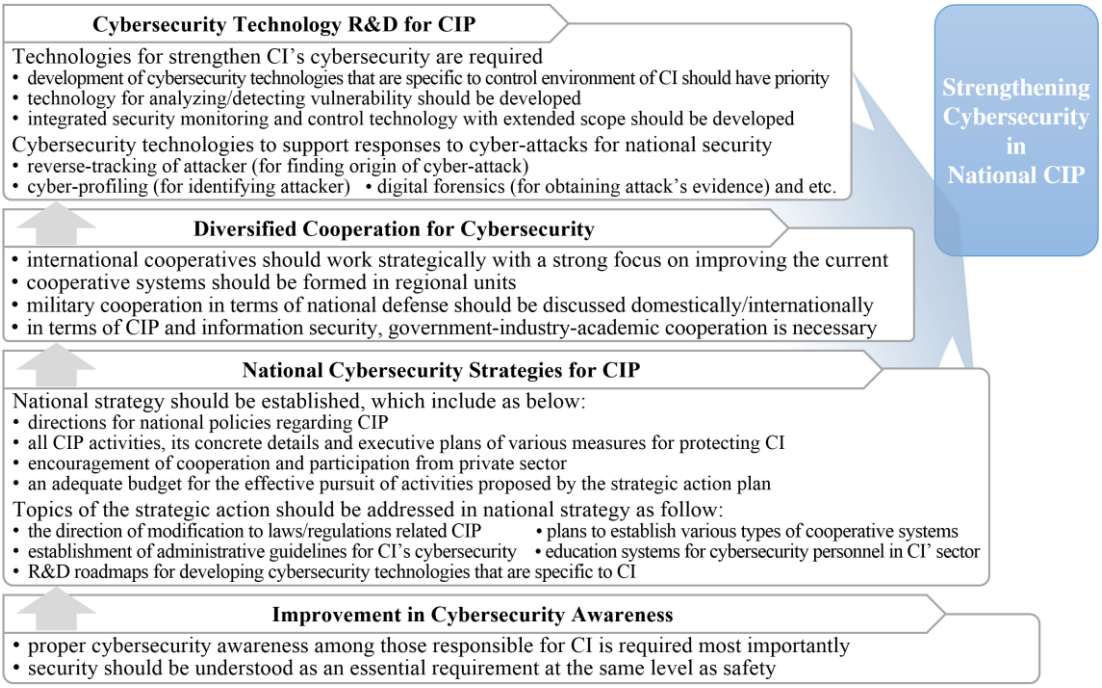

Fig. 4. Suggestions to Strengthening Cybersecurity in National CIP

7.4.2 Advanced Technologies for Threat Analysis and Security Monitoring & Control

To reduce the possibility of latent cyber threats in CI, technologies for the analysis and detection of vulnerabilities should be developed. The APT attack, such as the one used in the KHNP cyber-terror attack, is a cyber threat that is difficult to prevent, detect, or counter, even when existing cybersecurity systems are well implemented. Thus, to prevent cyberattacks in advance, there is a need to develop analytic technologies for vulnerabilities that can cause cyber threats.

Moreover, there needs to be developed integrated security monitoring and control

technology (SMCT) with an extended scope. Because most SMCTs focus on inbound traffic to block cyberattacks/invasions from external sources, it is difficult to detect information leakage, as in the case of the KHNP cyber-terror attack. Thus, there is a need for SMCT that covers outbound traffic. Furthermore, the basic monitoring functions of systems/processes should be extended in terms of cybersecurity so as to develop SMCT that allows the immediate identification of unusual control system behaviors that may be caused by cyber threats.

7.4.3 Cybersecurity Technologies for National Security

Cybersecurity technologies, such as the reverse tracking of attackers (to determine the origin of cyberattacks), cyber profiling (to identify an attacker), and digital forensics (to acquire evidence pertaining to an attack) are needed to support responses to cyberattacks for national security. Therefore, the government, which is responsible for national cybersecurity, should take the lead in fostering these R&D with military, information security industries, and academia.

7.4.4 Technologies to Solve Problems identified in KHNP Cyber-terror Attack

In addition, there is a need to develop technological and administrative measures that can fundamentally remove Hangul's vulnerability, which was used for the KHNP cyber-terror attack. Improved security systems should also be developed, as well as fixing problems in pre-existing security systems, such as network separation and external storage device control.

8. Conclusion

After the sixth release of data on March 12, 2015, it appeared that the KHNP cyber-terror attack had been temporarily resolved. However, on July 8, 2015, about four months later, the attacker made yet another release of data through the social media, and has been threatening the ROK government. We do not anticipate a simple end to this cyberattack, but believe that it will continue, given the source of the attack and given that the political situation in the Korean peninsula remains hostile. Therefore, there is a need for discussions on subsequent responses to this situation. Given this context, in this study, we performed a case study on the KHNP cyber-terror attack, and we sought answers to the following questions: What is the significance of the KHNP cyber-terror attack as an example of a cyberattack? What are the problems related to the cybersecurity of the CI of the ROK? What needs to be done to solve these problems?

From the case study, we obtained the following results. First, the KHNP cyber-terror attack is significant in that it occurred during a period over which there had been warnings concerning cyber threats to the CI, and it therefore alerted the nation. It also provided the opportunity to strengthen the cybersecurity of the CI of the ROK. It is also important in that it revealed previously identified cybersecurity weaknesses in the CI that had remained unresolved, as well as actual problems that could not be adequately addressed using cybersecurity measures. This served to provide a reminder to relevant agencies of the need for countermeasures that would result in practical results. Second, the KHNP cyber-terror attack is significant in that according to international norms, it may be interpreted as a cyber "attack" (a prohibited act), the "use of force" (a violation of the international norms), and an act that may be considered as an "armed attack" (grants the target the right to self-defense). There is therefore a need for international cooperation in formulating a response. Third, cybersecurity awareness is the most essential step in strengthening the cybersecurity of CI, and a national strategy should be formulated as a first step in this regard. Through this strategy,

improvements to the relevant legal systems, administrative guidelines, diversified cooperative systems, and cybersecurity R&D should be systematically pursued.

In this paper, we presented a case study that identifies cybersecurity threats against CI, as well as actual problems being faced when dealing with the threats. We proposed comprehensive countermeasures that can improve the cybersecurity of CI, and its scholastic significance thus lies in its practicality. However, this paper is limited in that it only proposes macroscopic countermeasures, so additional studies should be conducted to complement the proposed countermeasures.

References

[1] Nicolas Falliere, Liam O Murchu and Eric Chien, "White Paper of Symantec Security Response," *W32.Stuxnet Dossier*, version 1.4, February, 2011. Article (CrossRef Link)
[2] Center for Preventive Action of Council on Foreign Relations (CPA-CFR), *Preventive Priorities Survey*, 2011~2015. Article (CrossRef Link)
[3] Michael N. Schmitt, "Tallinn Manual on the International Law Applicable to Cyber Warfare," *Cambridge University Press*, New York, March, 2013.
[4] ISO/IEC JTC 1 SC 27, *ISO/IEC 27005:2011(E) Information technology - Security techniques - Information security risk management*, Second Edition, June 1, 2011.
[5] Myriam Dunn Cavelty, "Cyber-Terror - Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate," *Journal of Information Technology and Politics*, vol. 4, issue 1, pp. 19-36, October, 2008. Article (CrossRef Link)
[6] Michael Stohl, "Cyber terrorism: A Clear and Present Danger, The Sum of All Fears, Breaking Point or Patriot Games?," *Crime, Law and Social Change*, vol. 46, issue 4-5, pp. 223-238, December, 2006. Article (CrossRef Link)
[7] Dakota L. Wood, "2015 Index of U.S. Military Strength: Assessing America's Ability to Provide for the Common Defense," *The Heritage Foundation*, Washington DC, 2015. Article (CrossRef Link)
[8] Jong In Lim, You-joong Kwon, GyeHyun Jang and Seung-Jo Baek, "North Korea's Cyber War Capability and South Korea's National Counterstrategy," *The Quarterly Journal of Defense Policy Studies*, vol. 29, no. 4, pp. 9-45, Winter, 2013. Article (CrossRef Link)
[9] Nir Kshetri, "Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses," *East Asia*, vol. 31, issue 3, pp. 183-201, September, 2014. Article (CrossRef Link)
[10] Rhea Siers, "North Korea: The Cyber Wild Card," *Journal of Law and Cyber Warfare*, vol. 4, issue 1, pp. 1-12, Winter, 2014. Article (CrossRef Link)
[11] Richard A. Clarke and Robert Knake, "Cyber War: The Next Threat to National Security and What to Do About It," *HarperCollins*, New York, 2010.
[12] Joseph Menn, "Exclusive: U.S. Tried Stuxnet-style Campaign Against North Korea but Failed - sources," *Reuters*, May 29, 2015. Article (CrossRef Link)
[13] Kyung-Ae Kim, "[Exclusive] KHNP, 10,799 Employees' Personal Information leaked!," *BoanNews*, December 17, 2014. Article (CrossRef Link)
[14] "Government Combined Investigation Unit on Personal Information Crime of ROK," *Interim Investigation Report of the KHNP Cyber-terror*, March 17, 2015.
[15] Katharina Krombholz, Heidelinde Hobel, Markus Huber and Edgar Weippl, "Advanced Social Engineering Attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113-122, June, 2015. Article (CrossRef Link)
[16] Aditya K. Sood and Richard J. Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," *IEEE Security and Privacy*, vol. 11, issue 1, pp. 54-61, Jan.-Feb., 2013. Article (CrossRef Link)
[17] Chris W. Johnson, "Anti-social Networking: Crowdsourcing and the Cyber Defence of National Critical Infrastructures," *Ergonomics*, vol. 57, issue 3, pp. 419-433, 2014. Article (CrossRef Link)

[18] Kenneth Geers, Darien Kindlund, Ned Moran and Rob Rachwald, "WORLD WAR C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks," *FireEye's Annual and Regional Threat Reports*, September 30, 2013. Article (CrossRef Link)
[19] Rabiah Ahmad and Zahri Yunos, "A Dynamic Cyber Terrorism Framework," *International Journal of Computer Science and Information Security*, vol. 10, no. 2, pp. 149-158, February, 2012. Article (CrossRef Link)
[20] Dmitry Tarakanov, "The "Kimsuky" Operation: A North Korean APT?," *Securelist*, September 11, 2013. Article (CrossRef Link)
[21] Trend Micro, "MBR Wiper Attacks Strike Korean Power Plant," *TrendLabs Security Intelligence Blog*, December 23, 2014. Article (CrossRef Link)
[22] Jungje Ri, "Slanderous <NK Hacking> Rumor Full of Absurd <Evidence>," *Uriminzokkiri*, March 17, 2015. Article (CrossRef Link)
[23] Ilchul Chae, "Cyber Terrorism is Absolutely Not Tolerated," *Rodong-Sinmun*, June 9, 2015. Article (CrossRef Link)
[24] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations General Assembly A/68/98, June 24, 2013.
[25] Nohyoung Park and Myunghyun Chung, "Basic Concepts of Cyber Warfare in International Law: Focusing on the Tallinn Manual," *The Korean Journal of International Law*, vol. 59, no. 2, pp. 65-93, June, 2014. Article (CrossRef Link)
[26] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law*, vol. 37, pp. 885-937, 1998-1999. Article (CrossRef Link)
[27] Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review*, vol. 56, issue 3, pp. 569-605, November, 2011. Article (CrossRef Link)
[28] James B. Michael, Thomas C. Wingfield and Duminda Wijesekera, "Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System," in *Proc. of the 27th Annual International Computer Software and Applications Conference*, pp. 622-626, November 3-6, 2003. Article (CrossRef Link)
[29] Min-Jung Paik, "Application of Tallinn Manual to KHNP Cyber-terror," *Northeast Asia Strategic Analysis*, pp. 1-4, May 12, 2015.
[30] Board of Audit and Inspection of ROK, *Audit and Inspection Report - Crisis Management of National Critical Infrastructure (Focusing on Nuclear Safety, Drinking Water and Oil·Gas)*, December, 2012.
[31] Standing Auditor of KHNP, *2013 Annual Audit Report*, March, 2014.
[32] Standing Auditor of KHNP, *2014 Annual Audit Report*, March, 2015.
[33] Tae Kyung Ha, "Ha Tae Kyung, <KHNP Nuclear Power Plants Security Status> Confirmation of Overall Insufficiency," *Press Release*, November 2, 2014.
[34] Standing Auditor of KHNP, *Request for Penalty as per Audit Result - Inspection of Information Management and Use of Internet Network*, March, 2015.
[35] Won Sik Choi, "Inquiry Material to Nuclear Safety and Security Commission," *2014 Parliamentary Audit - Science, ICT, Future Planning, Broadcasting and Communications Committee*, October 8, 2014.
[36] KHNP, *2013 Parliamentary Audit - Correction·Handling Requirements and Action Plan*, July, 2014.
[37] Antony Bridges, "Industrial Control Systems: The Human Threat," in Christopher Laing, Atta Badii and Paul Vickers, *Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection*, IGI Global, Pennsylvania, pp. 82-104, December, 2012. Article (CrossRef Link)
[38] John D'Arcy and Anat Hovav, "Deterring Internal Information Systems Misuse," *Communications of the ACM*, vol. 50, no. 10, pp. 113-117, October, 2007. Article (CrossRef Link)

[39] Michael E. Whitman, "Enemy at the Gate: Threats to Information Security," *Communications of the ACM*, vol. 46, no. 8, pp. 91-95, August, 2003. Article (CrossRef Link)
[40] Eirik Albrechtsen and Jan Hovden, "Improving Information Security Awareness and Behaviour Through Dialogue, Participation and Collective Reflection. An Intervention Study," *Computers and Security*, vol. 29, issue 4, pp. 432-445, June, 2010. Article (CrossRef Link)
[41] Geun-hye Kim, Kyung-bok Lee and Jong-in Lim, "CBMs for Cyberspace Beyond the Traditional Security Environment: Focusing on Features for CBMs for Cyberspace in Northeast Asia," *Korean Journal of Defense Analysis*, vol. 27, no. 1, pp. 87-106, March, 2015. Article (CrossRef Link)
[42] Injung Kim, "Status and Outlook of North Korea's Cyber Terror," in *Proc. of the 2015 Joint Conference Between Institute for National Security Strategy and National Security Research Institute: North Korea's Cyber-terrorism Threats and Countermeasures*, pp. 25-46, March 31, 2015. Article (CrossRef Link)

Kyung-bok Lee is a Ph.D. candidate in the Graduate School of Information Security and a researcher at the Center for Information Security Technologies (CIST) and Cyber Defense Research Center (CDRC) at Korea University. He received his M.E. in Information Security Policy from Korea University. His primary research area is the National Policy on Cybersecurity including Privacy, Security of Converging Technologies and Cyber Warfare and Social Network Analysis

Jong-in Lim is a professor of the Graduate School of the Information Security/Department of the Cyber Defense in Korea University. He received B.S., M.S., and Ph.D. degrees in the Department of Mathematics at Korea University. He is a former Special Advisor to the President for National Security, Republic of Korea. His primary research area is National Cybersecurity, Information Security Policy, Cyber Warfare, Security of Converging Technologies, Privacy and Cryptography.