211-0007
378 Tenjinchou Kamimaruko Nakaharaku
Kawasakishi Kangawhken Japan

ISSN: 2423-8775

International journal of military affairs

2016 1(2)

<Index>

J-INSTITUTE

2016 1(2) 1-7 Submission: 2016/11/10, Peer review: 2016/11/20, Accepted: 2016/11/25, Published: 2016/12/30

International journal of military affairs

Publication state: Japan
ISSN: 2423-8775

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

Corresponding author
E-mail: manjong74@naver.com

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

http://dx.doi.org/10.22471/militaryaffairs.2016.1.2.01

Recommendations for the Development of COUNTERTERRORISM Policy in KOREA: Evaluation on Anti-Terrorism Act

Lee Man-jong

Howon University, Gunsan, Republic of Korea

Abstract

As Korea is the only divided nation in the world, it can be said that Korea has been maintaining a little negative attitude toward terrorism while considering the military preparedness against North Korea and prevention of war provocation. However, with the 9/11, the government and all citizens made it possible for the nation to recognize that there was not a safe country for terrorism. Moreover, since the French terrorist attacks, countries have been more alert to terrorist groups like the Islamic States(IS) In Korea, the controversy over the enactment of the Anti-Terror Law has been raised, but some people have raised public opinion that anti-terrorism measures should be prepared as soon as we are not a safe zone of terrorism. In the 19th National Assembly, a bill called "Anti-Terrorism Act for the Protection of the People and Public Safety" was initiated in the 19th National Assembly, and the enactment of the Anti-Terrorism Act was concluded with the enactment of Law No. 14071 on March 3, On March 3, 2016, the Anti-Terrorism Act for National Protection and Public Safety was enacted and promulgated, followed by the State Planning Office and the National Intelligence Service, which enacted the Law on Terrorism for National Protection and Public Safety The enforcement decree was enacted on June 4, 2016.

The enactment of the "Anti-Terrorism Act", which has been controversial in the meantime, has great significance in terms of securing the legitimacy of counterterrorism administration and establishing and enforcing related laws that directly and uniformly regulate terrorism. However, there are a few things to consider in terms of complementary aspects. Since the Law on the Prevention of Terrorism for Public Protection and Public Security, which was promulgated on March 3, 2016, was accompanied by political and social controversy during the legislative process, it is expected that there will be a lot of controversy in the future operation of law and enforcement ordinance have. It is also pointed out some legislative problems as it fails to legislate all of the important issues contained in existing legislative initiatives.

The Act on the Prevention of Terrorism for the Protection of the Public and the Public Security, known as Anti-Terrorism Act, is a law to prevent terrorism as it is, and it is true that such a law is necessary because the Republic of Korea is on the list of designated target by IS. However, it is hard to say that the controversy has subsided. Moreover, it has growing concern on three parts of the law: (i)the authority of the National Intelligence Service expanded excessively in the name of counterterrorism; (ii)military operations against civilians which are restricted in case of exercise of National Emergency Right on Constitution; and (iii)overly comprehensive and unclear definition of authority and organization of Center for Counterterrorism.

From this point of view, this article is intended to analyze the changes caused by the enactment of Anti-Terror Law and the direction of future counterterrorism policy development.

[Keywords] ***Anti-Terrorism Act, Counterterrorism Policy, Counterterrorism Human Rights Officer, Reimbursement, Compensation***

1. Introduction

As Korea is the only divided nation in the world, it can be said that Korea has been maintaining a little negative attitude toward terrorism while considering the military preparedness against North Korea and prevention of war provocation. However, after 9/11, the government and all citizens made it possible for the nation to recognize that there was not a safe country for terrorism. Unlike ordinary criminal offenses, terrorism is a serious crime, which can determine the State's existence through cruelty and unpredictability. Therefore, since 9/11, various discussions on terrorism have been made, and in particular, discussions on legislation on terrorism have become a key issue. According to the discussions on the legislation, the legislation of the anti-terrorism law was initiated and accordingly, a lot of efforts were made for legislation. However, the law has not been enacted due to differences of opinion on enactment laws[1].

But since the French terrorist attacks, countries have been more alert to terrorist groups like the Islamic States(IS) In Korea, the controversy over the enactment of the Anti-Terror Law has been raised, but some people have raised public opinion that anti-terrorism measures should be prepared as soon as we are not a safe zone of terrorism. In the 19th National Assembly, a bill called "Anti-Terrorism Act for the Protection of the People and Public Safety" was initiated in the 19th National Assembly, and the enactment of the Anti-Terrorism Act was concluded with the enactment of Law No. 14071 on March 3, On March 3, 2016, the Anti-Terrorism Act for National Protection and Public Safety was enacted and promulgated, followed by the State Planning Office and the National Intelligence Service, which enacted the Law on Terrorism for National Protection and Public Safety The enforcement decree was enacted on June 4, 2016[2].

The enactment of the "Anti-Terrorism Act", which has been controversial in the meantime, has great significance in terms of securing the legitimacy of counterterrorism administration and establishing and enforcing related laws that directly and uniformly regulate terrorism. However, there are a few things to consider in terms of complementary aspects. Since the Law on the Prevention of Terrorism for Public Protection and Public Security, so called Anti-Terrorism Act, which was promulgated on March 3, 2016, was accompanied by political and social controversy during the legislative process, it is expected that there will be a lot of controversy in the future operation of law and enforcement ordinance have. It is also pointed out legislative problems as it fails to legislate all of the important issues contained in existing legislative initiatives[2].

This is because, from the time of the legislation, the claim that the legislation is essential for national security and national security and the control methods for the possibility of abuse of human rights and the abuse of authority of national intelligence agencies prior to the enactment of the law should be given priority, and the anti-terrorism law passed the plenary session[3].

In other words, the Act on the Prevention of Terrorism for the Protection of the Public and the Public Security, known as Anti-Terrorism Act, is a law to prevent terrorism as it is, and it is true that such a law is necessary because the Republic of Korea is on the list of designated target by IS. However, it is hard to say that the controversy has subsided. Moreover, it has growing concern on three parts of the law: (i)the authority of the National Intelligence Service expanded excessively in the name of counterterrorism; (ii)military operations against civilians which are restricted in case of exercise of National Emergency Right on Constitution; and (iii) overly comprehensive and unclear definition of authority and organization of Center for Counterterrorism[2].

In particular, our Constitution strictly regulates the requirement in exercising the power of the State in emergency in order to guarantee basic rights of the people. Therefore, all laws and regulations cannot escape the boundaries and limitations of the Constitution, and these principles apply in the controversy related to the current Anti-Terrorism Act and the Enforcement Decree.

From this point of view, this article is intended to analyze the changes caused by the enactment of the Anti - Terror Law and the direction of future counterterrorism policy development.

2. Basic Grounds of Anti-Terrorism Act

On March 3, 2016, the "Anti-Terrorism Act for the Protection of the People and Public Safety" was enacted and promulgated. The Enforcement Decree of the Anti-Terrorism Act(hereinafter referred to as the "Enforcement Decree") for public protection and public safety was enacted on June 4, 2016.

The Enforcement Decree of the Anti-Terrorism Act for the Protection of the People and the Public Safety is intended to protect national security, public safety and its citizens' lives and properties.

The Enforcement Decree establishes the National Anti-Terrorism Committee (hereinafter referred to as the "Anti-Terrorism Committee"), in which 19 chief of the relevant organizations including the head of the State Coordination Department, the Ministry of National Defense, the Minister of Foreign Affairs. Also, there is a 'counterterrorism center' to coordinate. In addition, in order to carry out prevention of terrorism and its response professionally, it is necessary to operate a "dedicated organization" that utilizes the currently operated organization, and to establish human rights protection center for preventing human rights violations and protecting human rights through counterterrorism activities.

3. Analysis on Contents of Anti-Terrorism Act

The first plan is to impose an obligation to share information with the terrorist organization, which is the primary source of terror information. The second plan is to impose an obligation to share information with the counter-terrorism.

3.1. National anti-terrorism committee and counterterrorism center

In the composition and operation of the National Anti-Terrorism Committee(Articles 3 to 5), the National Anti-Terrorism Committee, such as the Minister of Strategy and Finance and the Minister of Foreign Affairs, or upon a request by a majority of the members of the committee. The secretary shall be appointed as the head of the counter-terrorism center(Article 3) in accordance with Article 6 of the Law[2].

Article 6 of the Enforcement Decree allows the Counter-Terrorism Center to deal with matters necessary for the smooth conduct of the national anti-terrorism activities and the office work necessary for the operation of the Committee, and to request the cooperation of the heads of the relevant agencies for the necessary cooperation and support. The Counterterrorism Center acts as a control tower for counter-terrorism tasks in accordance with the Anti-Terrorism Act for National Protection and Public Security. It is an affiliate of the Prime Minister's Office of State Coordination[4].

3.2. Counterterrorism human rights officer

In addition, Article 7 to Article 10 of the Enforcement Decree provides the matters related to the Counterterrorism Human Rights Officer, which is a member of the Committee in order to prevent human rights violations that might occur in the course of counterterrorism activities. The Counterterrorism Human Rights Protection Officer(hereinafter referred to as the "Human Rights Protection Officer") shall be appointed by the chairperson of the council committee, so that the term of office may be renewed in two years and shall not be invoked against the doctor except in cases of criminal cases The qualification is determined by a lawyer who has worked for more than 10 years, a person who has expertise in the field of human rights, and has worked for more than 10 years as an associate professor[2].

The role of the Human Rights Protection

Officer is to provide human rights protection Advice and recommendations related to anti-terrorism policies and systems proposed by the Countermeasures Committee, and to deal with civil complaints related to human rights violations through counter-terrorism activities. In other words, the Counterterrorism Human Rights Protection Officer advises and recommends the improvement of the human rights of the counter-terrorism policies and systems related to the counterparts proposed by the Counter-Terrorism Committee(Chairman, Prime Minister), And other activities to protect human rights are human rights education for related institutions, for example. If there is a reasonable reason to admit that there is an act of violation of human rights during the performance of the duties, it may be recommended to the head of the concerned agency after reporting to the chairperson[3].

Although it is clear that it is only an advisory role without compulsory authority or inquiry, it is the only person who is legally given authority to check and prevent human rights violations in the process of counterterrorism activities by the government.

3.3. A dedicated organization for counterterrorism

Article 11 to 21 of the Enforcement Decree establishes a "professional organization" composed of joint institutions for the prevention and countermeasures against terrorism, or established by heads of related organizations. In the case of terrorism response system, if terrorist attacks occur or there is a high possibility of occurrence, the heads of related organizations in five sectors (Minister of Foreign Affairs: Foreign Affairs Countermeasures Headquarters, Minister of National Defense: Military Terrorism Countermeasures Headquarters, The headquarters of the countermeasures headquarters will set up and operate the countermeasures against terrorism, and the head of the headquarters of the countermeasures headquarters will be the headquarters of the countermeasures against terrorism. And the organization of all the related organizations that are dispatched to the field such as rescue teams.

In order to prevent and respond to terrorism, the regional agencies are allowed to hold regional terrorism councils and airport / port terrorism councils. If the terrorist attacks are likely to occur or are likely to occur, the chiefs of related agencies should establish and operate a terrorist incident countermeasure headquarters based on the types of terrorist incidents, such as the countermeasures against terrorism and the countermeasures against terrorism. Terrorism response support headquarters, terrorism recovery support headquarters, counterterrorism special teams, and terrorist response teams.

In other words, if the head of the relevant organization is necessary to prevent and respond to terrorism in addition to the 'professional organization', the subordinate organization that performs counter-terrorism work can be designated and operated as a dedicated organization. In particular, in order to organically cooperate and coordinate the prevention of terrorism among municipalities, municipalities, special autonomous regions, provinces and special autonomous regions, and the related institutions, and to implement deliberations and decisions of the countermeasures committee. Director of the relevant department of the National Intelligence Service is responsible for this performance.

In order to carry out the operation against the terrorist attacks, the Minister of National Defense, the Minister of National Security and the Director of the Police shall establish and operate a "counterterrorism special team." In order to promptly rescue and rescue a terrorist incident, Minister Suh and the city and provincial governors have set up and operated a "counterterrorism rescue team."

Also, in order to manage the information related to terrorism, the National Intelligence Service establishes and operates an ‘Integration Center for Terror Information’ consisting of public officials. In addition, when terrorist incidents occur at home or abroad, or when terrorist intelligence is obtained or reports of terrorism are filed, the NIS director can organize and operate a counterterrorism joint investigation team with related agencies.

3.4. Procedures for response to terrorism

Articles 22 to 24 of the Enforcement Decree provide procedures for dealing with terrorism. The head of the Center for Counterterrorism, when there is a significant level of terrorist threat, is required to issue a terror alert after deliberation by the Task Force on Counterterrorism Measures, and the head of the related organization shall strengthen the control, preservation and security of the incident site. The Head of the Terrorism Countermeasures Headquarters has established an on-site command center in order to respond to the terrorist incident, maintain the situation propagation and response system, and systematically implement the measures.

3.5. Safety management measures to prevent terrorism

Articles 25 to 28 of the Enforcement Ordinance provide safety management measures for preventing terrorism. The head of the concerned organization shall establish safety management measures for the terrorism prevention measures of the national important facilities and multi-purpose and multi-use facilities and the manufacturing, handling and storage facilities of the terrorist use means, and check the appropriateness evaluation of the countermeasures established. In addition, the head of the relevant organization shall consult with the head of the counterterrorism center to establish and implement sector-specific safety management measures in accordance with the characteristics of the state's important events. If necessary, the countermeasures against terrorism and safety measures are taken to be organized and operated.

3.6. Reimbursement for prevention of terrorism

Article 29 to 34 of the Enforcement Decree provides for reward for prevention of terrorism. The head of the organization concerned has made it possible to prevent terrorism in advance or to report a person who has participated in or supported terrorism, or to give a reward to a person who has been apprehended after deliberation by a reward committee. In order to deliberate on the payment of rewards, the reward committee will be composed and operated by the head of the counter terrorism center. The reward committee will review whether the reward will be paid and how much the amount of reward will be paid. The rewards are paid in the range of 100 million won in consideration of the accuracy of the declaration contents and the credibility of the evidence.

3.7. Support for terrorist damage

Recently, the issue of terrorism has always been a hot topic in the international community and has become a premise and target of discussion in all areas of state relations. In particular, the September 11 terrorist attacks in the United States, which have occurred in 2001, have developed into a form of war. New terrorism, such as India's Mumbai terrorist attack in 2008, will cause terrorist countries to be hit and confused politically and economically as possible as it can[5].

Articles 35 to 44 of the Enforcement Decree provide support for terrorist damage. The state or municipal government is able to support the recovery cost of medical treatment and property damage caused by terrorism. In addition, for those who have suffered from the death of a person who died of terrorist attack and for those who have suffered from physical disability or long-term treatment, a special survival benefit, special disability benefit, or special severance benefit is provided.

4. Conclusion

Since the collapse of the Communist countries in the 1990s, terrorism has attracted attention as a major international issue that threatens international peace, including human rights and poverty. Terrorist environment and the environment surrounding Korea are gradually diversified in accordance with changes in domestic and overseas security environment. In other words, international terrorism is a frequent trend all over the world, and there are concerns about the possibility of domestic terrorism due to the increase of international marriage, migrant workers, and North Korean Refugees in Korea, and the threat of terrorism, as an asymmetric warfare, by North Korea[1].

As of June 4, 2016, the National Intelligence Service(NIS), which is a public information organization, is responsible for (i)collecting personal information(including sensitive information such as thoughts, beliefs, and health), site of location, and use of communication (ii)monitoring and inquiry on information of immigration and financial transaction, (iii)suspension of financial transaction. The NIS is also given the right to investigate and track down terrorist threats. The Anti-Terrorism Act has made it possible for the NIS to directly exercise its powers held by investigative agencies such as the prosecution, police, etc., following legal procedures such as a court warrant and written request[6].

The dramatic conclusion of the issue of the enactment of the Anti-Terrorism Act in 15 years is fortunate in the face of growing threats to terrorism both domestically and internationally. However, there is a concern that the 19th National Assembly was in a hurry to pass, and it is concerned that remaining contents in the act lacks key points. In the course of future operations, additional controversy may arise in details such as initiative of information and invasion of privacy. It is necessary to ask how much terrorism prevention law has actual efficiency and value to prevent terrorism. We know that even if there is 'law', we cannot prevent all illegal activities. Even if there is a punishment for robbery, it is the same as the strength does not disappear. The Anti-Terrorism Act also provides a degree of legal protection against terrorism, but it cannot be a safety barrier to all acts.

In order to protect the life, body and national security of the people in an emergency situation called terrorism, it is a national obligation to prepare and prepare for countermeasures against terrorism in advance. Of course, in order to prevent terrorism, it is necessary to build an integrated information system. In the past, the United States has separated and controlled many intelligence agencies, but now it maintains an integrated framework for effective terrorist surveillance. However, if the efforts of these countries cannot guarantee their effectiveness with unnecessary controversy, it will be difficult to achieve the original purpose. In other words, the Korean government's efforts to counteract terrorism are indispensable measures for the security of the nation and the public, but it would be difficult to ensure the effectiveness without guaranteeing national consensus on the functional and systematic efficiency and constitutional limitations related to human rights[7].

In the perspectives of the fact that the Anti-Terrorism Act violates the basic rights of the people, it is needed to consider the cases of the United States and the United Kingdom, which enacted the law in the past, have been used to violate the rights of their citizens. Thus, it is expected that the controversy over the national security and violation of basic rights will continue. What is important in the direction of future development in counterterrorism policy is 'tolerance' of the law guaranteeing basic rights and dignity of the people in the Constitution. As seen in the case of former National Security Agency (NSA) agent Edward Snowden, who disclosed the NSA's indiscriminate collection of personal information, it is a matter of social normative debate on the relationship between security and human rights, rather than how appropriate and proper the power was exercised.

In the future, it will be necessary to improve and strengthen the legal system so that the Anti - Terrorism Act can be effectively applied to prevent terrorism. However, due to the existence of strong counter-terrorism laws, hundreds of terrorist simulations are detected in a year to prevent terrorism in advance. We should do our best to prevent terrorism by comparing and developing terrorism related laws and experience cases of these countries. The study of relevant legal systems and empirical cases in countries that have enacted and enforced the Anti-Terrorism Act prior to us can help us a great deal.

The Anti-Terrorism Act should have procedures and contents that meet the constitutional standards, not the authority to end and end the intelligence agency. The most important thing in the national counterterrorism policy is how harmoniously two values of human rights and security can be operated. The Anti-Terror Act has been passed, but future challenges remain. No matter how good a law or system is, it does not make any sense if we cannot get the people's understanding and bring the power of the people together. In the process of legislating and revising the detailed legislation in the future, it is necessary to minimize the infringement of the basic rights of the people. State power should be used to minimize the violation of the people's freedom.

5. References

5.1. Journal articles

[1] Park HH & Kim JH. A Study on the Act on Anti-Terrorism for the Protection of Citizens and Public Security. *Korean Journal of Police Science*, 18(3), 69-98 (2008).

[2] Hyung HK & Kim SH. Issues and Challenges in the Enforcement Decree in the Anti-Terrorism for Protection of the People and Public Safety. *Journal of Issues & Discussions*, 1180, 1-4 (2014).

[5] Lee MJ. A Study on Concerning Anti-terrorism Legislation Major Issues and Complementary Review. *Korean Journal of Police Science*, 9(1), 139-162 (2010).

5.2. Additional references

[3] http://www.newsis.com/ (2016).
[4] http://news.kmib.co.kr/ (2016).
[6] http://www.asiatoday.co.kr/ (2016).
[7] http://www.munhwa.com/ (2016).

Author
Lee Man-jong / Howon University Professor
B.A. Chosun University
M.A. Chosun University
Ph.D. Chosun University

Research field
- A Study on the Prospect and Countermeasures of Terrorist Organization in the Middle East, Korean Terrorism Studies Review, 8(2) (2015).
- State Compensation Should Correspond to the Refugee Problem in South Korea, Korean Terrorism Studies Review, 9(1) (2016).

Major career
- 2008~present. Korean Association for Terrorism Studies, Chairperson
- 2016~present. Institute of Counterterrorism and Peacemaking, Chairperson

2016 1(2) 8-14 Submission: 2016/11/10, Peer review: 2016/11/20, Accepted: 2016/11/25, Published: 2016/12/30

International journal of military affairs

Publication state: Japan
ISSN: 2423-8775

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

Corresponding author
E-mail: huayl@cku.ac.kr

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

http://dx.doi.org/10.22471/militaryaffairs.2016.1.2.08

A Study on KOREA-CHINA Fishing Dispute and Marine SECURITY Strengthening Plan

Shin Hyun-joo[1]

Catholic Kwandong University, Gangneung, Republic of Korea

Lim Ying-hua[2*]

Catholic Kwandong University, Gangneung, Republic of Korea

Abstract

In the Korean waters, illegal fishing activities by Chinese fishing vessels are increasing rapidly and becoming violent. For example, due to the severe resistance to the recent crackdown, Korean Coast Guard was settled down and the high-speed boat was sunk. Marine security issues such as marine environment and maintenance of ocean order are becoming a national problem. In this regard, Korean Coast Guard revised its manual on use of weapons and shifted its position toward stronger response. However, it is necessary to prevent the controversy of international disputes by explicitly stipulating its role and authority in the relevant laws and regulations. Korean Coast Guard have cracked illegal fishing vessels in China and processed them according to domestic legal process. Since these disputes are international in character, they cannot be expected to be actively responded to because they can become diplomatic problems.

This study examined the actual situation of illegal fishing in China and domestic and overseas laws, and suggests the enhancement of responsiveness and social interest of the seaside through the improvement of the legal system.

South Korea and China have promised to cooperate in order to maintain fishing order and protect fishery resources in the West Sea in 2014. In the "2015 Working Group Meeting on Penetration of Fisheries in Korea and China", it was decided to strengthen the cooperative control of the two countries on unauthorized Chinese fishing vessels with the common awareness that strong crackdown and punishment are necessary for the eradication of illegal fishing.

Disputes over maritime sovereignty in Korea and China, as well as globally, are at stake. In each country, fisheries resources and energy security are emerging as important issues for national security as well as for economic development. Therefore, a national maritime sovereignty protection strategy is needed to effectively secure the maritime security of the Republic of Korea. First, it is necessary to strengthen responsiveness through the maintenance of related laws and efforts to reduce disputes under international law. Second, it is required to enhance the conservation of fishery resources and raise social interest to maintain good fishing relations. In addition, it is necessary to build an efficient marine management system between government ministries and strengthen multi-dimensional maritime security cooperation with neighboring countries.

[Keywords] ***Korean Coast Guard, Maritime Police, Illegal Fishing, Chinese Fishing Boat, EEZ, Maritime Security***

1. Introduction

Countries around the world are competing to expand their sovereignty[1]. As the United Nations Convention on the Law of the Sea came into force in 1994, the rights and obligations of the coastal states to the oceans have been strengthened. As a result, countries around the world have declared the exclusive economic zone (EEZ) and are increasing the strength of maritime jurisdiction and development[2]. Disputes between neighboring countries are intensifying in connection with securing marine resources.

Despite domestic and international laws and agreements, the illegal fishing of Chinese fishing vessels within the EEZ of Korea is becoming increasingly collective and violent rather than eradicated. The problem is that the Korean maritime police officer is killed by a violent resistance to cracking down on illegal fishing, and an accident such as the sinking of high-speed assimilation occurs, and the level of resistance is increasing such as intentional demonstration of power or acts of violence using weapons. In the meantime, Korean maritime police have cracked illegal fishing vessels in China and processed them according to domestic legal process. Since these disputes are international in character, they cannot be expected to be actively responded to because they can become diplomatic problems.

Nonetheless, recently, the Korean government announced the manual for weapons in November 2016. It has decided to take tough action against illegal fishing and acts of violence in China that have undermined the sovereignty of the Republic of Korea and have lost its power. However, there is still international dispute, which is a challenge for improving maritime police activities for maritime security in Korea. Therefore, this study examines the domestic and foreign laws for the illegal fishing practices of the Chinese fishing vessels and their crackdowns, and suggests ways to improve the security of the maritime security of the Republic of Korea.

2. The Actual Conditions of Illegal Fishing of Chines Fishing Vessels

2.1. Definition of illegal fishing of Chinese fishing vessels

2.1.1. Definition and cause of illegal fishing

Illegal fishing can be defined as fishing activity that does not comply with the regulations set by the law. Illegal fishing of a foreign language ship can be defined as a foreign ship engaging in fishing engaged in the maritime jurisdiction of Korea which is prohibited from fishing in accordance with domestic law or international law[3]. These include unauthorized fishing activities, breach of permits, breach of fishing zone, breach of fishing gear, and use of illegal fishing gear[2].

The illegal fishing activities of Chinese fishing vessels are due to the increase of consumption of fishery products in China and the depletion of fisheries and fishery resources due to marine pollution and indiscreet overfishing due to the rapid industrialization process[4]. Therefore, China is operating in the exclusive economic zone or disputed waters of neighboring countries facing the sea area. As a result, conflicts arise with neighboring countries, and competition against marine resources and territories becomes more serious[2].

2.1.2. Type of resistance by illegal fishing vessels

Chinese illegal fishing vessels have been completely armed, including barbed wire and barbed wire on the fishing boat, and hull surrounded by steel plates to block the check of the Korean peninsula. These types of resistance are organized violence, collective behavior, and simple protest[5][6]. The type of organized violence is a situation that crew members carry steel pipes and stand in line and use weapons to show off the power of the multitude under the command of the captain. It is a form of resistance to the end by charging the body of the police officer on board the ship with a weapon, In case of collective action type, if one of illegal fishing vessels is arrested and overpowered, the ship will arbitrarily break down and join with other fishing vessels to conduct collective action. By shutting down the course of vessels and threatening lives of Korean Coast Guards and crew members as a collateral damage, they make the officers give up sending the vessel under escort. Lastly, the type of simple protest is the type that crew members threaten the coast guards with shovels until the guards get on board. If the guards get on the vessel, they abandon resisting to the guards.

2.1.3 Status of regulations on Chinese illegal fishing vessels

When we look at the illegal fishing regulations of Chinese fishing vessels, the majority of captured fishing vessels are 'breach of restriction conditions'. The number of people who have been arrested has increased compared with the previous year, and the amount of security levy is steadily increasing.

Table 1. Status of regulations on Chinese illegal fishing vessels[7].

	Seizure of Vessels				No of arrested people	Amount of margin posed (unit: ten thousand)
	Total	EEZ		Violation of Korean Waters		
		Unauthorized	Violation of fishing conditions			
2009	381	86	272	23	130	553,000
2010	370	91	226	53	56	781,000
2011	534	170	332	32	72	1,458,000
2012	467	106	330	31	173	1,715,000
2013	487	149	304	34	183	2,442,000

2.2. China’s position on Chinese illegal fishing vessels

It is pointed out that “the main cause of the conflict between Korea and China is the Chinese ship” and the main cause is the "unauthorized fishing act" caused by Chinese fishing vessel's invasion of Korean territorial waters[8]. As a solution to this problem, the two governments proposed strengthening cooperation between the two governments, proper handling of fisheries conflicts, strengthening of fisheries management in China, protection of offshore resources, and strengthening training for fishermen. The most important of these is that the fishermen should improve their fisheries quality through education and promotion of fishermen[9].

Chinese Fisheries Department is in charge of the illegal fishing of its own fishing vessels. It sent an official letter to each relevant department instructing them to prohibit fishing, fishermen education and management in violation of the regulations. It also said that it should not be opposed or fugitive when conducting the work in accordance with the conditions of the agreement in relation to the agreement, and when it is checked by a Korean enforcement agency.

Despite the efforts of Chinese government, however, the dispute over illegal fishing on Chinese fishing vessels continues. In October, there was an incident in which the Chinese ship accidentally crashed and sunk the Korean seaport high-speed expressway. The Chinese side said in a press conference, "China is watching the relevant reports and is already checking the situation through the Chinese embassy in Korea and checking the situation with the related departments. On the Korean side, “We will start to deal with the problem calmly and reasonably”, Korean Foreign Ministry spokesman said.

A few days later, the Ministry of Foreign Affairs of China reiterated in a press conference, "The Korean side's position on the incident is unfounded, and as a result of demonstrating the geographical coordinates provided by the Korean side, The Chinese government has already raised strict negotiations with relevant ministries in Korea through diplomatic channels in relation to the case, and the Korean side I need to calmly deal with the problem." They also stressed out that "Cooperation between Korea and China is an important part of bilateral relations, and good fisheries cooperation order is in harmony with the interests of both Koreans"[10].

After that, China has not disclosed its position until now(as of November 15th). However, the Korean Coast Guard secured a message from the Chinese maritime and fishery bureaus on November 16 that the illegal fishing and illegal acts of violence were strictly prohibited on Chinese fishing vessels. It seems that China is making an effort to improve its domestic fishing vessels in response to the strong response of the Korean side.

3. Regulations on Illegal Fishing in Korea

3.1. Domestic and international law on illegal fishing

According to the provisions of national law and international law, waters which are mainly applied to the illegal fishing of foreign fishing vessels can be classified as domestic waters, territorial waters, fishery protection waters, exclusive economic waters and specific prohibited waters. The United Nations Convention on the Law of the Sea (LOSC) It is the basis for the establishment of maritime boundaries and considers illegal fishing practices and the conservation of the marine environment based on this agreement (including the United Nations Fish Stocks Agreement and the FAO Compliance Agreement).

In addition, Korea is regulating fishery activities in EEZ between the two countries through the "Agreement on Korea-China Fisheries" with China. The conclusion of the agreement has made it possible to preserve and manage fish stocks, crack down on illegal fishing, and resolve peaceful settlement of fisheries disputes. According to the agreement, Chinese vessels that wish to operate in Korea's EEZ must be approved by our fisheries authorities. And the type of fish that can be caught, the quota, the operating area and other operating conditions. On the other hand, offending vessels can be boarded and captured, and jurisdiction can be exercised.

As for domestic law, 'ACT ON THE EXERCISE OF SOVEREIGN RIGHTS ON FOREIGNERS' FISHING, ETC. WITHIN THE EXCLUSIVE ECONOMIC ZONE'. It is said that this law is applied to protect the sovereignty of the Republic of Korea and its jurisdiction except exceptive cases determined by agreement with a foreign country. The main contents of this law are fishing in specific prohibited areas, fishing in EEZ without permission, and prohibition of excess amount of fishing. In case of violation, not only fines and confiscations but also legal measures such as seizure of offending vessels can be taken.

In addition, 'FISHERIES ACT' and 'FISHERY RESOURCES PROTECTION ACT' have been granted to judicial police officers to the officers of the naval vessels, officers of the naval vessels and the supervisory staff of the fishery management group to crack down on the permission violations. In addition, according to the TERRITORIAL SEA AND CONTACTUOUS ZONE ACT, foreign vessels are considered to be harming the peace, public order or security of the Republic of Korea if they engage in fishing in territorial waters without permission. Any fishing activity in violation of the above laws will be punished under the procedure of 'CRIMINAL PROCEDURE ACT’.

3.2. The manual on the use of weapon by Korean coast guard at sea

The Headquarter of Maritime Safety at the National Security Agency announced that it will completely reorganize the existing "Gun Usage Guidelines" as a follow-up measure to strengthen crackdown measures against illegal operations, and to revise them as a "Manual for Use of Weapons". In other words, the decision maker of use of weapons at sea depends on the type of firearms: personal firearms will be determined by the officers on crackdown, and crew-served firearms by the field commanders.

Although the high-speed boat was sunk during the recent crackdown on illegal fishing, which was due to the deliberate clashes by Chinese illegal fishing vessels, it pointed out that complete reorganization of the manual on use of weapons is needed. It was because it cannot properly cope with the use of crew-served firearms. As a result, the use of weapons is based on the principle of 'reporting after, action first', and the use of weapons has to be fired on parts of the body or hull where the damage of use of weapons can be minimized after warnings and warning shots. It also expanded the requirements for the use of weapons, including the use of crew-served firearms in case of deliberate clashes. In the meantime, it also clarified the respect of legal rights and reasonable treatment in compliance with legitimate law enforcement based on the respect on human rights and humanitarian spirit. In addition, Korean Coast Guard decided to revise the maritime security law so that police officers' indemnity clause for legitimate use of weapons could be specified[11].

4. Problems of the Dispute Between Korea and China and Measure to Strengthen the Maritime Security

4.1. Reinforcement of response through reform of legal system.

4.1.1. Establishment of clear legal grounds for law enforcement on illegal fishing

Act on the performance of duties by police officers and the "Maritime Security Act", which are the basis of the seafarers' duties and activities, do not accurately reflect the changes in the marine environment. Although it is necessary to have a clear authority regulation on the police function, it is evaluated that it does not. It is, therefore, difficult to actively respond to the illegal fishing of foreign fishing vessels[12]. On the other hand, the revised manuals on use of weapons are not clear in terms of liability, and only a provision that lacks reality is taken into account when considering the special circumstances of maritime. Therefore, it is necessary to strengthen the powers to eliminate the possibility of disputes in international law and to actively carry out the duties of the maritime affairs, and to prepare the legal system such as the clear grounds for the forced disposition. In particular, the principle of necessity and the principle of proportionality should be carefully considered in relation to the use of force.

4.1.2. Reinforcement of equipment for safe law enforcement

Compared to the size of Chinese fishing vessels, there are not enough human resources to cover the coastal area and the working conditions are quite poor. In addition, there are many factors that threaten the officers’ lives, such as Chinese fishing vessels that resist the crackdowns armed with iron pipes. Reinforcement of equipment is necessary for the safety of both fishermen and Korean Coast Guard.

Therefore, it is required to replace the personal safety equipment such as the bumper buoyant vest and uniforms for the oppression at sea directly connected with life. Also, it is necessary to improve equipment such as net gun and grenade launcher for safe crackdown. In addition, for severe punishment, it is necessary to reinforce the investigative equipment such as long distance and infrared camera that can prove illegal activities and to collect evidence[3][13].

4.2. Raising social awareness on marine resources and competitiveness

The offshore order of the coastal countries has been collapsing due to illegal fishing, the resources of fish stocks have been rapidly decreasing, and marine pollution has been intensifying. It is necessary to improve social awareness on the illegal status of Chinese fishing vessels, to inform them of its seriousness and to make them take preventive measures themselves.

Since the accident of the Sewol Ferry, the Korean Coast Guard has been restructuring and has suffered various problems such as the reduction of personnel. However, it is necessary to establish social consensus through the interest and cooperation among the states, citizens and the media as well as the strengthening of law enforcement by the Korean Coast Guard.

5. Conclusion

Both Korea and China have stipulated strict regulations on illegal fishing through agreements. Recently, however, Chinese fishing vessels have invaded Korean waters due to lack of fishery in the sea near China. A more serious problem is that Chinese fishing vessels armed themselves with steel pipes and acted with force to avoid the crackdown on the Korean peninsula.

South Korea and China have promised to cooperate in order to maintain fishing order and protect fishery resources in the West Sea in 2014. In the "2015 Working Group Meeting on Penetration of Fisheries in Korea and China", it was decided to strengthen the cooperative control of the two countries on unauthorized Chinese fishing vessels with the common awareness that strong crackdown and punishment are necessary for the eradication of illegal fishing.

However, the ongoing illegal fishing and Korean-Chinese fishing disputes are not likely to be solved in a short period of time. Not only the efforts taken by both governments, but most importantly, it seems that fishermen themselves need to improve their awareness of compliance with the law.

Disputes over maritime sovereignty in Korea and China, as well as globally, are at stake[6]. In each country, fisheries resources and energy security are emerging as important issues for national security as well as for economic development. Therefore, a national maritime sovereignty protection strategy is needed to effectively secure the maritime security of the Republic of Korea. First, it is necessary to strengthen responsiveness through the maintenance of related laws and efforts to reduce disputes under international law. Second, it is required to enhance the conservation of fishery resources and raise social interest to maintain good fishing relations. In addition, it is necessary to build an efficient marine management system between government ministries and strengthen multi-dimensional maritime security cooperation with neighboring countries.

6. References

6.1. Journal articles

[1] Jung BK & Choi JH & Lim SW. A Study on the Role of Maritime Enforcement Organization as Response of Illegal Fishing. *Journal of Fisheries and Marine Sciences Education*, 26(4), 769-788 (2014).

[2] Roh HR. Illegal Fishing of Chinese Fishing Boat and Countermeasure of Korean Maritime Police. *Korean Police Studies Review*, 9(2), 29-58 (2010).

[3] Roh HR. Illegal Fishing Problems of Chinese Fishermen in the Five Islands the Northern Limit Line of the West Sea. *Journal of Korean Maritime Police Science*, 5(1), 57-80 (2015).

[4] Shin SC. A study on the Countermesures against Illegal Fishing by Chinese Boats. *Maritime Law Review*, 25(3), 215-248 (2013).

[5] Kim JS. The Re Examination on Using Police Equipment for Countermeasure of Illegal Chinese Vessel. *Journal of Korean Maritime Police Science*, 2(1), 3-36 (2012).

[6] Lim CH. A Study on the Law Enforcement of Korea Coast Guard against the Illegal Chinese Fishing Vessels. *Journal of the Korean Society of Marine Environment & Safety*, 20(1), 49-58 (2014).

[8] 詹德斌．海洋權益角力下的中韓漁業糾紛分析．*東北亞論壇*, 10, 63-64 (2013).

[9] Lee KS & Choi JH. Problems with and Effective Countermeasures for South Korea’s Crackdown on the Illegal Chinese Fishing Boats. *Korean Association of Public Safety and Criminal Justice Review*, 64, 167-190 (2016).

[11] 曲維濤．中韓漁業協定執行情況及有關問題研究分析．*漁業信息與戰略*, 3, 175-179 (2015).

[13] Choi K & Kim MC. Development of Maritime Governmental Power for National Security and Public Safety. *The Journal of Police Policies*, 30(1), 269-302 (2016).

6.2. Additional references

[7] Korean Coast Guard. White Paper (2014).
[10] http://www.fmprc.gov.cn/ (2016).
[12] 中華人民共和國農業部, 農業部辦公廳關於 2016 年實施中韓漁業協定有關問題的通知. 中華人民共和國農業部漁業局 (2016).

Lead Author
Shin Hyun-joo / Catholic Kwandong University Professor
B.A. Catholic Kwandong University
M.A. Kwangwoon University
Ph.D. Kwangwoon University

Research field
- The Study on the Current Status of Gambling Addiction and Policy Responses of Late Adolescence Undergraduate, Journal of Korean Association of Addiction Crime, 6(1) (2016).
- A study on Application Strategies and Tasks of the Police Drones, Journal of Public Security Administrations, 13(1) (2016).

Major career
- 2014~present. Korean Association for Criminal Psychology, Chief Manager
- 2016~present. International Society for Military Affairs, Member

Corresponding Author
Lim Ying-hua / Catholic Kwandong University Professor
B.A. Korea National Open University
M.A. Donga University
Ph.D. Kyungsung University

Research field
- Essay on Honorification in Modern Chinese, Korea Journal of Chinese Studies, 48 (2014).
- Chinese Taboo Words and Alternative Type, Korea Journal of Chinese Studies, 51 (2015).

Major career
- 2006~present. Korea Association for Chinese Studies, Member
- 2016~present. International Society for Military Affairs, Member

2016 1(2) 15-20 Submission: 2016/11/10, Peer review: 2016/11/20, Accepted: 2016/11/25, Published: 2016/12/30

International journal of military affairs

Publication state: Japan
ISSN: 2423-8775

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

Corresponding author
E-mail: pws7897@naver.com

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

http://dx.doi.org/10.22471/militaryaffairs.2016.1.2.15

A Study on the Rationale of CYBER TERRORISM Prevention Act in ROK -Where Does the State's Obligation to Prevent Cyber Terror Originate?-

Park Woong-shin

Sungkyunkwan University, Seoul, Republic of Korea

Abstract

In early 2016, the Republic of Korea enacted the "Anti-Terrorism Act for the Protection of the Korean People and Public Safety" and provided the testimony to counter terrorism crimes by international terrorist groups including IS. On the other hand, the legislative response to cyber terrorism, which is more important than the traditional terror crime in terms of the severity and repeatability of the damage, has been insufficient. In this situation, the government of the Republic of Korea deliberated and voted on the "National Cyber Security Bill" in December 2016. Despite the existence of the Anti-Terror Law, there may be criticism that the enactment of a special law for cyber terrorism is unduly violating the fundamental rights of the people. Therefore, it is necessary to first examine whether a separate legislative response is required because cyber terrorism has some difference from traditional terrorism. In this paper, cyber terrorism originated from traditional terrorism, Since the substance is a totally different crime, we need to respond to it separately from terrorist crime, confirming that the legitimacy of the enactment of the special law is guaranteed. In addition, if the necessity is recognized, the special law has the possibility of restricting the freedom of expression in the basic rights of the people, especially in the online space. Therefore, the philosophical basis of the restriction is examined. In this study, It was found in the fundamental purpose of the state and described it as a specific expression of the obligation to protect the basic rights of the state. In addition, the hypothesis that cyber terrorism can be regarded as a new type of risk source proposed by Ulrich Beck also emphasized the necessity of preemptive response before the occurrence of cyber terrorism in response to the risk source. Of course, can not infringe the essential content of the basic rights in the process.

[Keywords] ***Cyber Terrorism, Terrorism, Law of Prevention of Cyber Terrorism, Freedom and Safety, Prevention of Crime***

1. Introduction

In early 2016, the Republic of Korea enacted the “Act On Anti-Terrorism For The Protection Of Citizens And Public Security” and provided the testimony to counter terrorism crimes by international terrorist groups including IS. On the other hand, there was no legislative response to cyber terrorism, which is more important than traditional terrorist crimes in terms of severity and repeatability. In this situation, the government of the Republic of Korea deliberated and voted on the "National Cyber Security Bill" in December 2016. Despite the existence of the Anti-Terror Law, there may be criticism that the enactment of a special law for cyber terrorism is unduly violating the fundamental rights of the people. Therefore, since cyber terrorism has some differences from traditional terrorism, it is necessary to first examine whether a separate legislative response is necessary. In addition, if the necessity is recognized, the special law may limit the freedom of expression in the basic rights of the people, especially in the online space. Therefore, it is necessary to examine the philosophical basis of the restriction, will review the matter.

2. Concept and Characteristics of Cyber Terrorism

It is not easy to distinguish between traditional terror crime and general violent crime[1], just as it is not easy to define terror crime, it is not easy to define the concept of cyber terrorism because of the mixture of real space and cyber space. Generally, cyber terrorism is understood as "direct sabotage or attack on hardware or software, website or information communication infrastructure on cyberspace such as hacking, virus infection, DDOS". If so, what characteristics of cyber terrorism should we consider to limit the basic rights of the people in order to prevent cyber terrorism.

To examine the characteristics of cyber terrorism, one must examine what is different from traditional terrorism. Terrorism is "an act intended to interfere with the exercise of the power of a state, local government or foreign government, to do nothing without duty, or to intimidate the public"[2]. In other words, the conceptual elements of traditional terrorism are: (i) threats to the use or use of violent acts; (ii) political, national and ideological motives as elements of excess subjective constitution; and (iii)separation of victims and the masses as objects of terrorism[3].

However, even if cyber terrorism is derived from traditional terrorism, it is questionable whether it can be viewed as a sub-form of traditional terrorism. First, the traditional forms of terrorism are the core elements of the use or use of violent acts, while cyber terrorism is not a hard infringement, but a malicious infringement of hacking, viruses, malicious codes and so on. Second, while traditional terrorism requires political purpose as an excess subjective component in addition to the intention of crime, cyber terrorism does not require an over - subjective constitutional factor. Therefore, cyber terrorism on the subjective side is different from traditional terrorism. The traditional forms of terrorist crime are not aimed at the illegal acts of violence themselves, but rather by the use of acts of violence to achieve their specific purposes[4]. In addition, those who are directly victimized by such acts of violence, The recipient is clearly distinguished. However, cyber terrorism is often aimed at state-based facilities such as power, telecommunications, and finance. If the infrastructure of the country fails to operate normally due to cyber terrorism, not only direct victims but also the members of the society who enjoy the infrastructure are directly affected. It is different from terrorist crime. Therefore, even if cyber terrorism appears in traditional terrorism, it is not necessary to consider it as a subordinate concept, and it is reasonable to consider it as a separate form of crime.

The next issue to consider is the subject of cyber terrorism. In other words, can it be the subject of cyber terrorism as well as non-state actors such as individuals. There is no reason to deny the state actor's terrorist crime subjectivity in the traditional form of terrorism, so there is no need to deny the subjectivity of the state in cyber terrorism. In recent years, armed conflicts as a form of total war between countries are rare, and there is no reason to exclude the state from the subject of cyber terrorism because there are many dispute resolution methods such as cyber terrorism and low intensity conflict.

Finally, it is necessary to examine the Internet use of terrorist groups. Recent national security is a trend that focuses on comprehensive security threats. The UNODC recognizes[5] the inherent security risks of cyber terrorism and not only moves toward a comprehensive policy approach, but also recognizes cyber terrorism as an inherent security threat, It is approaching as a policy countermeasure rather than as a dogma tick[6]. In other words, the international community including the UNODC sees cyber terrorism as a cyber terrorism, as well as cyber terrorism, which causes cyber terrorism to hurt public goods such as state infrastructure. Therefore, the problem of terrorist criminals such as internet use is not a traditional paradigm of international security-security, domestic-security but a representative example of the approach of both. Therefore, acts such as Internet use of terrorist organizations are sub-types of cyber terrorism It is reasonable to approach.

3. Legal Basis of Cyber Terror Prevention

We examined the concept and characteristics of cyber terrorism and examined the necessity of separate legislation due to the difference from general terror crime. Because cyber terrorism has difficulty in proving the seriousness of the damage and proving the damage, proactive prevention is an important task rather than a posterior response. In terms of the prevention of cyber terrorism, how can the judicial system prevent real and direct infringements against the law? According to the traditional criminal justice system composed of the category of infringement crime, the cyber terrorist act has a logic structure that it can not be penalized without criminal law if there is no special clause because there is no direct infringement against the individual or the state. However, the punishment of a criminal after a terrorist crime has actually occurred can not be more than a retaliation against an actor. Therefore, despite the fact that no actual damage has occurred, it is necessary to consider the grounds for punishing cyber terrorism and further preliminary action. It is also necessary for the state to consider what legal basis it should have in order to curb terrorist crime. If so, we must first derive the evidence from the Constitution. In other words, the law aiming at the prevention of terrorist crime should examine how the Constitution relates to the basic rights of the people, and thus the state that aims to protect the lives and property of the people, It can guarantee the constitutionality of legislation.

3.1. National obligations for crime prevention

3.1.1. The legitimacy of state existence and the duty of crime prevention

One of the characteristics of the September 11 attacks in 2001 was to awaken the desire for fear of life and security of life that was inherent in the abyss since the birth of mankind. Of course, this perception is not caused by 9/11 terror. The history of mankind itself is a history of pursuing its own safety and the maintenance of life. The discussion of "safety of life" is a theme that applies to members of underdeveloped nations or members of Western advanced nations. If so, what is this "safety" and what is the state to do to enjoy this safety.

After the introduction of the notion of sovereignty by the French political philosopher Jean Bodin in the 16th century, the concept of personal safety began to develop in relation to the state, beginning with Thomas Hobbes[7]. As Hobbes saw Europe at the time of the war in disintegration and freedom of religion, the natural state of man was in a state of struggle against all men of the so-called universes, so overcoming these situations of death and disorder is at the top of all powers The Leviathan. That is, all human beings sign a social contract entrusting their rights to Leviathan for survival, and this "safety" is the basis of state power to protect the lives and bodies of individuals threatened in disorder.

John Locke goes further here and assumes the importance of a nation that protects the life and personal safety of an individual, and that country, when securing peace and security in a state where the exercise of power is restricted by law. In the social contract theory, individuals are obliged to transfer their natural right to the state under the premise that the state guarantees the safety of life and body, and the state has the obligation to create an environment in which its members can live safely and peacefully. Therefore, the state is recognized not only as its existence itself, but also the justification of its existence in preventing the life, health and property rights of its members from being infringed by other individuals or organizations and maintaining the order of society[8].

3.1.2. Obligation to protect national fundamental rights and prevent crime

Fundamental rights have the characteristics of ⅰ)the passive defense of state power and ⅱ)the active formation of state order[9]. The duty of the state to protect the lives and property of the people from cyber terrorism is derived from the objective order which is the latter of the fundamental rights. The fundamental right as the basic element of this objective order is to protect the nation from the crime including cyber terrorism, to protect them.

The basic right of the classical sense meant a basic right to protect the passive position of the nation, that is, the life and property rights of the people, from the state, not from the state. In modern society, however, basic rights are required to take an active role, not just passive status. The State must inevitably limit the fundamental rights of third parties to protect the basic rights of the people from cyber terrorism. In this regard, the relationship between the state and the people, and the conflicting values of freedom and security, always means a tension. Therefore, it is best to resolve the tension by establishing clear laws that everyone can understand Method. Considering the various forms of cyber terror crime that can be manifested in various ways, it is the responsibility of the state to abide by the existing system of legal system and to dismantle the maintenance of institutional and legal systems to prevent future crimes.

3.2. The rising of risk society and crimes of terrorism

The German philosopher Georg Wilhelm Friedrich Hegel described in 1821 his “Grundlinien der Philosophie des Rechts” that “criminal law depends on the state of society in that age and its time”. As such, criminal law is influenced by social change. Since the 1970s, ROK society has achieved rapid economic growth, the development of science and technology, and the democratic development that is hard to find anywhere else in the world. However, this compact modernization brought about negative aspects, such as large-scale environmental pollution, large-scale collapse and explosion, industrial accidents, and the emergence of various types of violent crimes that were not seen before in the 1950s. Ulrich Beck has been involved in the development of so-called “neue großrisiken”, a side effect of nuclear, chemical, ecological and genetic engineering technologies, and new types of crime(environmental, economic and terrorist crimes) Society as a Risk society. And ROK society is a representative aspect of the dangerous society proposed by Beck[10].

Due to the economic growth and development of science and technology, our society has reduced the traditional and natural risks compared to the 1950s when the criminal law was enacted. However, this 'objective safety' has increased, but 'subjective anxiety' about the new mass danger perceived by ordinary citizens in the dangerous society and the cruelty of recent violent crimes and hate crimes significantly threatens objective safety. Because of this, the public in our society demands an active role for new threats to the state and the law, especially the criminal law. In this context, the paradigm of the state is the Prevention country(Präventionsstaat), which aims at minimizing the intervention of the penal rights, and at the same time, in the 19th century liberal legal state, to Safety Country(Sicherheitsstaat)[10]. As the national paradigm shifts, the function of the criminal law is required to change the direction to prevent mass danger and to secure safety. The discussion of Risk Criminal Law(Risikostrafrecht) begins here. The dangerous criminal law means that criminal law should actively intervene in order to control these modern risks, since it can not solve the problems of the 21st century that are newly raised with the spiritual tools of the 18th century[11]. In particular, the traditional functions of the criminal law in new types of crimes such as economic crime, environmental crime, terrorist crime and drug crime are no longer limited to maintaining social order. Therefore, And to control the overall social structure by upgrading the strong intervention and the related penalties in the pre-crisis period before the emergence of the crisis (Gefährdung)[10].

Terrorist crimes, including cyber terrorism, can also be discussed on the same line. Terrorist crimes that coincided with the history of mankind existed before discussing the regulation of terrorist crime in modern society. However, in the 1970s and 1980s, due to urbanization and technological development due to changes in social structure, cyber terrorism in modern sense is different from classical terrorism. In addition, since cyber terrorism is more illegal than general criminal offense, there is a need to regulate pre - terrorist acts as well as enforcement actions before the stigma of legal interests becomes real.

4. Considerations for Establishing Cyber Terror Prevention Law

4.1. Comparison of freedom and safety

National liberty can be violated at any time by the State or a third party. Therefore, the State should endeavor to guarantee the freedom of the people based on the purpose of existence and the obligation to protect fundamental rights in the Constitution. There is also the opinion that demanding freedom from the state and safety from others at the same time is an impossible proposition[12]. As John Locke argues, always guarding the duality of state power, state power plays a role in protecting the safety of the people, but paradoxically there is also the danger of threatening the fundamental rights of the people themselves. Freedom from these paradoxes is not a concept of conflicting or conflicting national freedoms and security, but securing personal security when the state power is limited by law and guarantees the survival and well-being of the social community. Therefore, the state power must have clear laws backed up to guarantee the safety of the people.

4.2. Limitations in cyber terror crime prevention

What needs to be considered in responding to cyber terrorism is how to resolve the relationship between freedom and security, such as the two sides of a coin. Through the prevention of cyber terrorism, the state can fulfill its duty to protect basic rights to prevent infringement of the life and property rights of the people from other countries or autographs, but inevitably limits the basic rights of the people inevitably. Therefore, we should consider whether the law aiming at the prevention of cyber terrorism can give some control to the state to prevent it from unduly infringing on people's fundamental rights. If the contents of the law aiming at the prevention of cyber terrorism infringe on the fundamental rights of the people excessively, there is a possibility to violate the principle of proportionality. On the contrary, in order to guarantee the basic rights of the people, Of the total number of deaths, it is not possible to substantially guarantee the obligation to protect the basic rights of the state as a prevention of crime. The Constitution Law stipulates that “all the freedoms and rights of the people may be restricted by law only when necessary for national security, order maintenance or public welfare, and that the essential contents of freedom and rights can not be infringed even when restricted”. In this way, it is recognized that the rule of law also restricts the basic rights of the people to unlimited, but in certain cases. Therefore, even if the basic rights of the people are restricted due to national security, order maintenance, public welfare, etc., the basic rights can be restricted only within the purpose, method and limit set by the Constitution Law.

5. Epilogue

In this paper, we examine whether the law is necessary and what grounds it is, in spite of the Anti - Terrorism Act in accordance with the National Cyber Security Act. Cyber terrorism originates from traditional terrorism, but in reality it is a totally different crime. Therefore, it is necessary to deal with terrorism separately from crime. If so, prevention of cyber terrorism is also important, which may inevitably limit the basic rights of the people. In this study, we found that the basis of the restriction was found in the fundamental purpose of the state for the prevention of crime, which is expressed specifically by the obligation to protect the basic rights of the state. In addition, the hypothesis that cyber terrorism can be regarded as a new type of risk source proposed by Ulrich Beck also emphasized the necessity of preemptive response before the occurrence of cyber terrorism in response to the risk source. Of course, can not infringe the essential content of the basic rights in the process.

6. References

6.1. Journal articles

[3] Park WS & Yoon HS. A Study of Terror Concept. *Korean Terrorism Studies Review*, 6(2), 44-71 (2013).

[5] Yoon HS. Cyberterrorism: Trends and Reponses. *Korean Institute of Criminology*, 12, 3-303 (2012).

[7] Jeong MS. Recht Auf Sicherheit: Grundlage und Massstab. *Journal of Law and Politics Research*, 7(1), 217-239 (2007).

[10] Kim JY. Reaktion Des Straf Und Strafprozessrechts Gegen Den Gesellschaftlichen Wandel Als Risikogesellschaft. *Korean Journal of Comparative Criminal Law*, 12(2), 251-276 (2010).

[11] Park KM & Lee SD. Countermeasures of the Criminal Law in Accordance with Appearance of Risikogesellschaft. *SungKyunKwan Law Review*, 18(3), 513-533 (2006).

[12] Lee JY. Direction of Improvement of Law and System for Expansion of National Anti-Terrorism System. *Journal of Counter-Terror Policy*, 7, 1-44 (2010).

6.2. Books

[1] Britz MT. Terrorism and Technology: Operationalizing Cyberterrorism and Identifying Concepts in Crime On-line. Carolina Academic (2010).

[4] Alex S & Albert J. Jongman Political Terrorism. Transaction (2005).

[8] Pitschas R. Fortentwicklung Des Polizeirechts und Legitimität Des Staates in: Polzeirecht Heute Schriftenreihe Der Polizei Führungsakademe. Munster (1991).

[9] Chang YS. The Constituibtional Law. Hongmunsa (2011).

6.3. Additional references

[2] Act on Anti-Terrorism for the Protection of Citizens and Public Security Article 1 (2016).

[6] UNODC. The Use of the Internet for Terrorist Purposes (2012).

Author
Park Woong-shin / Sungkyunkwan University Senior Researcher
B.A. Sungkyunkwan University
M.A. Sungkyunkwan University
Ph.D. Sungkyunkwan University

Research field
- A Study on the Problems and Improvement Plans of Personal Information Protection in Changing Environment, The Journal of Legal Studies, 24(3) (2016).
- Research on Countermeasures Against Terrorism in Public Transportation, Counter-Terrorism Research, 39 (2016).

Major career
- 2015~present. Sungkyunnkwan University, Senior Researcher
- 2016~present. International Society for Justice & Law, Editor in Administrator

2016 1(2) 21-26 Submission: 2016/11/10, Peer review: 2016/11/20, Accepted: 2016/11/25, Published: 2016/12/30

International journal of military affairs

Publication state: Japan
ISSN: 2423-8775

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

Corresponding author
E-mail: ksj@sunmoon.ac.kr

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

http://dx.doi.org/10.22471/militaryaffairs.2016.1.2.21

A Study on the Characteristics of IS-Related TERRORISM in Western Europe

Cho Sung-taek[1]

Sunmoon University, Asan, Republic of Korea

Kim Seok-joo[2*]

Sunmoon University, Asan, Republic of Korea

Abstract

The IS expanded its forces in 2014, securing territory, money, and military power in the name of creating an independent state ruled by the Islamic leader Caliph. The IS, which has secured its military power based on the looting economy, is threatening with brutal retaliation and fear of the opposing states or forces. In response, NATO's US and European member states are working together to combat IS.

Terrorism in the Western Europe over the past two years can be evaluated as an intention to expand the power of the IS and retaliation against Anti-IS. From another point of view, recent terrorism in Western Europe is caused by discrimination against Muslims living in Europe. Muslims are alienated as Gentiles in European society, and are easily inclined to IS in this environment.

There has been a series of terrorist attacks in Western Europe for two years, starting in 2015. Terrorist attacks occurred in the daily living space that citizens often visit such as cinemas, football stadiums, cafes, trains, and churches. The fear of terrorism and the fear of civilians are increasing, and the debate over the acceptance of Syrian refugees continues.

The recent terrorist attacks in Western Europe, such as Nurnberg, Munich, and Normandie, were planned terrorist attacks by a 'lonely wolf', which made it difficult for counterterrorism authorities to respond. It is pointed out that recent terrorist attacks require a change in embracing policies for Muslim immigrants residing in Europe. In conclusion, it is also important to attack the base for the purpose of cleansing the IS, but it is necessary to change the policy of active engagement with Muslims.

[Keywords] ***IS, ISIL, Lone Wolf Terrorism, Soft Target, Engagement Policy***

1. Introduction

Terrorism-related attacks have been happening in Western Europe for the last two years. European terrorist experts said that after the Paris terrorist attacks last November, IS is planning a professional terrorism targeting Europe[1]. It is generally argued that terrorism in Western Europe is directly attributed to the ideology of Islam or IS, on the other hand, it is argued that there are other reasons.

Discrimination against Muslims living in Europe is the root cause of terrorism. The terrorist in Brussels, Belgium, is from Molenbee, near Brussels. It notes that 30% of the population is Muslim, and the unemployment rate in the region is 40%[2].

Muslims living in Europe are not enjoying their rights as Europeans and point out that they are discriminated against in Europe. Muslims are alienated as non-Europeans and foreigners, and in this environment they become involved in IS and become terrorists.

2. Theoretical Background

2.1. Formation of IS

IS refers to a state-type armed group aimed at building an Islamic state around Iraq and Syria. It was also called ISIS(Islamic State in Iraq and Syria), ISIL(Islamic State in Iraq and Levant), but it was later called Islamic State(IS). Its goal is to build an Islamic nation in Iraq and the Levant. Levant is named for the Middle East region of the eastern Mediterranean, including Syria, Lebanon, Jordan and Palestine.

2.2. Growth of IS

ISIL started as an Iraqi subordinate organization of al Qaeda in 2003 and has been carrying out various terrorist activities in Iraq. After the Syrian civil war broke out in 2011, it moved its base to Syria. They have been fighting against the government in the Syrian civil war in 2013, but since early 2014, they have been in full swing with other rebels. ISIL, which has acted as an insurgent and has expanded rapidly, has expanded to massive momentum since its occupation of Mosul and neighboring oil fields in Iraq in June 2014, and was renamed "Islamic State (IS)" in ISIL on 29 June[3].

As of October 2014, the number of members in IS organizations is estimated to be between 80,000 and 50,000. Unlike the previous Islamic terrorist groups, it is considered to have abundant man, money, and munitions[4]. The entire IS organization is dressed in black, symbolizing Muhammad, the founder and prophet of Islam, and is using social media primarily to recruit recruits and threaten opponents. More and more young people are joining IS in Europe, Australia, the United States, and the former Soviet Union. There are many children of Islamic immigrant families in Europe with high unemployment rates. IS occupied a military base in Iraq and Syria, and had more combat equipment than Iraqi and Syrian government forces.

2.3. Spread of IS-related terrorism

IS, which declared the establishment of the Caliphate in June 2014, has been focusing on building its territory in Syria and Iraq. However, since October 2015, the IS station has been bombing Turkey and terrorizing Russia. We are expanding our activity area. IS has identified Korea as a target of terrorism by disclosing "The Global Coalition against The Islamic State," which includes 90 countries targeted for terrorism.

According to the National Intelligence Service, IS is distributing 7700 locations of the US Air Force, NATO air force base, and 8,300 civilians from 21 countries through its own hacker organization. In August 2014, IS bombarded British journalists, Japanese, and Jordanians, including the United States journalist, and has been expanding his activities in Asia and Europe, including hosting hostages in a restaurant in the capital city of Dhaka, Bangladesh.

3. IS-Related Terrorism in Western Europe

3.1. Spread of terrorism in Western Europe

In the wake of the year 2015 through 2016, there has been a series of terrorist attacks in Western Europe that threaten daily activities[5]. Terror occurred in the places that citizens often visit, such as cinemas, football stadiums, cafes, trains, and churches. The recent terrorist attacks in Europe were aimed at soft targets[6][7].

The major terrorist incidents in Western Europe are summarized as follows.

January 2015 Charlie Hebdo Terror, 12 killed

February 2015 Copenhagen Terror, 3 killed, 5 injured

Paris Terror in November 2015, 130 dead, 350 injured

. Belgium Brussels Terror in March 2016, 30 people dead, 280 people injured

. Nice Terror in July 2016, 84 dead, 240 injured

. July 2016 Normandie Terror, one killed, one injured

. July 2016 Bayern Terror, 9 killed, 25 injured

3.2. Terrorist attack against the Charlie Hebdo & terrorist attack in Copenhagen

On January 7, 2015, gunfire occurred in the office of Charlie Hebdo, a weekly magazine in Paris, France, by Islamic extremists. Islamic extremist terrorists broke into Charlie Hebdo's office, shooting guns, killing 12 people, including 10 employees and two police officers. Charlie Hebdo, who has been terrorized, has received great resistance from Muslim countries, publishing Muhammad mansions since 2006. Therefore, it was analyzed that this terrorism was a counter terrorism against Muhammad cartoons.

'Charlie Hebdo' is a typical French satirical weekly magazine that has raised much controversy with criticism and provocative attitudes about various sanctuaries. In 2011, he published a special edition called 'Sharīʻah Hebdo' in May, and re-introduced Muhammad's caricature, which says on the cover, "It's 100 thrashing if it's not funny to die." It was threatened by terrorism, and in November of that year, the office was burned down and the Internet site was hacked. In September of 2012, Muhammad, in his suits in a wheelchair with a rabbi headed by a rabbi with a title of 'I can not touch it,' spoke of saying "Do not mock!" This has led to the emergence of French-related facilities in the Arab countries on an emergency alert and the dismissal of more than 20 international schools in France.

After Charlie Hebdo's office gunfire, the French authorities raised the border level to the highest level in Paris, and one of the suspects placed their identities in the escape vehicle on public identities Said Kouachi, Cherif Kouachi and Hamid Mourad. The Kouachi brothers, except for Mourad, who had embroidered since then, took a woman hostage on January 9 at a printing plant near Paris and were shot in the face of military and police forces.

Brother Kouachi, a French-born Algerian French citizen, was not a major surveillance target for France for several months before the terrorist attacks. Cherif was sentenced to three years in prison(18 months probation) on charges of terrorism in 2008 to help send militants to rebels in Iraq. Said was found to have received special training in Yemen in 2011.

US government sources said the Kouachi brothers were listed on two lists managed by US counterterrorism officials, including a potential terrorist database called "TIDE" and a "no-fly" list of the TSC.

Meanwhile, Yemen-based international terrorist group Yemen al Qaeda AQAP claimed that they were behind terrorism on January 14 after Charlie Hebdo Terror.

On February 14 and 15, 2015, three gunshots occurred in Copenhagen, Denmark, resulting in three injuries. Copenhagen terrorism is estimated to be on a continuation of Charlie Hebdo terror. There are many media satirizing Muhammad in Denmark, and the Danish government is actively cooperating with US policy on IS aggression.

'Jyllands-Posten' features 12 cartoons that criticize Islam, including the caricature of Muhammad who carries a turban with a dynamite of Charlie Hebdo. In Islam, it banned the shaping of Muhammad, and it mocked Muslims' antipathy with mocking comics like terrorists. In addition, the Danish government is working closely with the United States, including sending seven F-16 fighters and 140 pilots and ancillary personnel to the US-led "IS Fighting International Allied" raid in October 2014.

The Copenhagen terrorist attack was aimed at Sweden-based Lars Vilks. Vilks is a person who is rebelling against Islamic rights such as Yemen al-Qaida's assassination list in 2007 after he published a newspaper in the newspaper with the body of Muhammad in his head in 2007. In fact, in May 2010, the house was fired, and in December of that year, a chain of car bombings took place in the center of Stockholm in the wake of the Vilks.

In the afternoon of February 14, more than 50 people, including Vilks, university professors, civil activists and journalists, in the cafes of downtown Copenhagen, were carrying out a memorial service for Charlie Hebdo terror. This resulted in the death of one civilian and three police officers. On February 15, a Jewish man who was outside the Jewish synagogue in downtown Copenhagen was killed and two police officers were injured.

3.3. Terrorist attack in Paris

IS committed a simultaneous terrorist attack on November 13, 2015 in Paris, France's heartland. From the night of November 13 to the dawn of March 14, 132 people were killed in the worst simultaneous terrorist attacks, including gunshots and suicide bombings, in six venues, including Paris, theaters and football stadiums in the heart of Europe. On November 14, after the terrorist attacks, IS said in a statement that the attacks were their own.

The French prosecutor's investigation found three teams involved in the terrorist attack, the first team suicide bombing at the Stade de France in a bomb vest, and the second and third teams, including automatic rifles and bomb vests Armed and terrorist attacks at several restaurants and Bataclan theaters, respectively, in central Paris.

The terrorists were divided into three groups and simultaneously caused a total of six terrorist attacks in six locations, including Paris and Saint-Denis, north of Paris. Three suicide bombings took place near the Stade de France in Saint-Denis, where French and German football games were held. French President Hollande, who was watching the game at the time, was evacuated to safety zone after the first half. At that time, another group of people fired their guns at restaurants and cafes in Paris' 10 and 11 districts, killing 40 people. The terrorists broke into the Bataclan Theater in the 11th district of Paris and fired their guns, killing more than 90 people. At that time, 1,500 audiences were watching rock band performances at the theater. They hosted about 60 spectators who could not get out of the theater and confronted the police. Later, Bataclan tried to counter terrorists by putting a counter-terrorist unit in the theater. In this process, three terrorists committed suicide by bombing and one was killed.

On November 14, the day after the incident, IS and Iraq-based Syria claimed that terrorism was their cause. On January 19, 2016, IS published their own magazine "DABIQ" 13, and in the last chapter, they published photos of nine Parisian terrorists and names used in IS under the title "JUST TERROR".

So far, IS foreign terrorism has been a way to instigate lonely wolves through propaganda media or video, but this has been the way that IS has been leading the plan of terrorism from the outside and then running through local members(lonely wolves in France)[8].

In France, there is an increase in the number of Muslim immigrants who are dissatisfied with society because of their job loss in the depression, and there is an analysis that IS has strategically used it. It is also presumed that the French domestic policy, which strictly adheres to the principle of secularism that separates the state from religion, also stimulated Islamic extremism. In 2011, the law prohibits the wearing of burka, a traditional clothing of Islamic women, in public places. In recent years, the Ministry of Education has also forced Muslims to forbid pork meat.

The French government is also a major factor in IS terrorism as well as its leading role in crushing Islamic extremism externally. France launched an air strike to al Qaeda in 2013 at the request of the Mali government, and has been in conflict with Islamic extremists for years in North Africa. And in order to defeat the IS, air raids are underway in Syria since September 2015 following the Iraqi air raids in 2014.

France declared war on IS shortly after the Paris series of terrorist attacks on November 15, 2015, in a major raid on Syria's largest home and heartland, the Raqqah. The UN Security Council has unanimously passed a resolution to repel the IS on November 20, strengthening the international community's response to the IS.

3.4. Terrorist attack in nice

On July 14, 2016, the anniversary of the French Revolution, terrorism arose in a beach town in Nice, France, presumed to be an Islamic extremist. The terrorists drove the massive trucks to the crowd, causing 84 deaths and a catastrophic attack on 100 people. Nice terrorism was recorded as the worst terror in France since the death of IS in Paris in November 2015, when more than 130 people were killed. Mr. Hollande extended the national emergency, which he proclaimed after the Paris series of attacks in November 2015, for three months.

The terrorist was a 31 - year - old Tunisian French man, who shot and rode a 1.8 - kilometer truck, as well as shooting. The terrorist was killed in a shootout with the police at the scene. The killer was a Frenchman who worked as a delivery truck driver in Nice and was reported to have moved to France from Tunisia in 2005.

On July 16, after the incident, IS claimed that they were behind Netis terror through online media. However, no accurate evidence has been found.

According to French prosecutors, the terrorist attacks were carried out by months of preparation and there were five accomplices. It was confirmed that the accomplices had already searched for the place to be terrorized and instructed or informed about detailed terrorist methods.

On the other hand, it has been rarely seen in the existing forms of terrorism that transportation, such as a large truck used in Nice terrorism, was directly used in the killings. The terrorist scene of Nice was different from the existing terrorism. The terrorist attacks targeting Islamic extremist terrorist groups such as IS and Al-Qaeda were mostly airtight areas such as airports, stadiums, cafes, and subways[3].

3.5. Terrorist attack in Bayern

The shocks and anxieties experienced by the German society came about after just three days of indiscriminate terrorism and injuries in public places. On July 19, three days before the München terrorist attack, a 17 - year - old boy suffered a serious injury to four passengers on a train and attacked a citizen on the escape. The killer was a supporter of Pakistan-based IS who came to Germany as a refugee in Afghanistan last June.

On July 22, the boy who committed a terrorist attack in Munchen was found to have been fired at a similar age group with a grudge at the school bullying[9]. He was irrelevant to IS, believed in extreme righteousness, and committed the crime alone.

Bayern, which has suffered terrorism, has recently received more than 63,000 refugees, which has heightened the claims of refugees and terrorists. The next terrorists are those who entered Germany a long time ago or were born in Germany and thus have nothing to do with the refugees.

On July 25, a young man from Syria, at the Ansbach Music Festival, committed suicide bombings and wounded 15 people and wounded himself. The criminal was known to have committed an offense under IS's license. The Bayern authorities said that the 27-year-old Syrian vowed to retaliate against Germany in the name of Allah before the attack.

4. Lone Wolf Terrorism and Muslim Engagement Policy

From 2014 to 2015, IS attacked at least 50 terrorist attacks, 1,100 killed and 1,700 wounded[10]. Europe was no exception, and terror was committed by 'lonely wolves' and organized terrorist organizations[10][11]. Terrorism targeting an unspecified number of civilians is also increasing[12].

After the onset of terrorism, the arrests of extremists in Europe are increasing rapidly. Religious extremist arrests have tripled from 219 in 2013 to 687 in 2015.

IS is moving in an organized way to induce religious tensions within Europe. As this move has taken effect, opposition to Muslims has also been rising across Europe.

Recent terrorism in France and Germany is characterized by 'a blind faith in a teenager who is not a trained combatant,' a target that is difficult to identify, 'a random attack regardless of time and place'.

The Telegraph analyzed that the last two weeks of terrorism were not linked and literally a single, two-person offense without direct support from IS.

Recently, Europol also said that these terrorist organizations did not plan or support direct terrorism, although IS did not.

It is pointed out that a terrorist incident necessitates a change in embracing policy for Muslim immigrants residing in Europe[13]. In conclusion, it is also important to attack the base for the purpose of cleansing the IS, but it is necessary to change the policy of active engagement with Muslims.

5. References

5.1. Journal articles

[2] Hyun HN. The Modern Dhimmi and Slavery in 21st Century Islamism Based on the Origins of ISIS and Salafiya Movement. *Mission and Theology*, 38, 87-122 (2016).

[7] Brandt PT & Sandler T. What do Transnational Terrorists Target? Has it Changed? Are We Safer?. *Journal of Conflict Resolutions*, 54(2), 214-236 (2010).

[8] Kim ES. Islamic State Radicalization and Response Strategy through Paris Terrorism Case Analysis. *Korean Terrorism Studies Review*, 8(4), 27-52 (2015).

[12] Park BR & Ha SG. Countermeasures in Prevention of Soft Target Terrorism. *Korean Terrorism Studies Review*, 9(2), 27-48 (2016).

5.2. Books

[6] Bennett BT. Understanding Assessing and Responding to Terrorism (2007).

[11] Clarke RVG & Grame R. Newman Outsmarting the Terrorists. Westport (2006).

5.3. Additional references

[1] http://news.heraldcorp.com/ (2016).

[3] http://terms.naver.com/ (2016).

[4] Gunaratna R. Central Asian Republics in Frank Shanty and Raymond Picquet Encyclopedia of World Terrorism 1996-2002 (2003).

[5] http://www.vox.com/ (2016).

[9] http://news.chosun.com/ (2016).

[10] Europol. European Union Terrorism Situation and Trend Report (2016).

[13] Ludes M. Attacking Terrorism: Elements of a Grand Strategy (2014).

Lead Author
Cho Sung-taek / Sunmoon University Professor
B.A. Hankuk University of Foreign Studies
M.A. Hankuk University of Foreign Studies
Ph.D. Hankuk University of Foreign Studies

Research field
- A Study on the Countermeasure and Analysis of Anti-money Laundering in South Korea, Journal of Korean Public Police and Security Studies, 9(4) (2013).
- A Study on the Terrorism and Dispute of Africa, Korean Terrorism Studies Review, 8(4) (2015).

Major career
- 2009~present. The Korean Association for Terrorism Studies, Member
- 2013~2014. Ministry of Security and Public Administration, Evaluation Staff

Corresponding Author
Kim Seok-joo / Sunmoon University Professor
B.A. Hankuk University of Foreign Studies
M.A. Hankuk University of Foreign Studies
Ph.D. Hankuk University of Foreign Studies

Research field
- A Study on Vitalization of Operation on Cioc in Korea, Journal of Korean Society for Public Personnel Administration, 10(3) (2011).
- A Study on the Effects of Battalion Commander Leadership Style on Organizational Effectiveness of the Individual Soldiers: Focused on Mediated Effect of Trust, Journal of Korean Society for Public Personnel Administration, 15(1) (2016).

Major career
- 2001~2003. Presidential Special Commission of Electronic Government, Secretary General
- 2008~2010. The Korean Association for Regional Information Society, Chairperson

2016 1(2) 27-36 Submission: 2016/11/10, Peer review: 2016/11/20, Accepted: 2016/11/25, Published: 2016/12/30

International journal of military affairs

Publication state: Japan
ISSN: 2423-8775

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

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

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

http://dx.doi.org/10.22471/militaryaffairs.2016.1.2.27

NORTH KOREA'S CYBER ATTACK: Terror Cases and Cyber Capabilities and Current State of Affairs of North Korea's Cyber Terror Force

Son Man-sik[1]
J-INSTITUTE, Gumi, Republic of Korea

Jo Sung-gu[2*]
Kyungwoon University, Gumi, Republic of Korea

Abstract

Republic of Korea is an IT powerhouse where smartphone use is universal and Koreans can enjoy fast internet anywhere in Korea. Such entrenchment of the smart phone in daily life has aided the country's democratic development such as advancing freedom of speech and human rights but the high dependence on information technology has also introduced new threats.

One of these threats is none other than North Korea's cyber terrorism. So far, the most notable North Korean cyber terror attacks are 7.7 Distributed Denial of Service(DDoS) Attack(2009), Nonghyup Bank Network Hack(2011), and JoongAng Daily Website Cyber Attack(2012). North Korea has conducted countless cyber terror attacks against Republic of Korea and the attacks were estimated to have caused over 1 trillion won of damage.

Currently, North Korea is offering curriculum on cyber terrorism in academic institutions such as Kim Il Political Military University, Kim Chaek University of Technology, Pyongyang Computer Technology University and it has been estimated that it employs around 6,800 specialists to bring chaos to the international community through utilization of cyber space. Furthermore, North Korea is considered the world's fourth most powerful nation in cyber warfare only behind the United States, China, and Russia, thus emerging yet as a new threat to the world.

Experts identify North Korea's unchecked expansion of cyber terror force as a serious threat that can bring crisis to Northeast Asia. Therefore, the international community must pay attention to not only North Korea's nuclear test and missile development but also its rapidly growing cyber terror force.

[Keywords] ***North Korea, Hacker, Cyber Attack, Cyber Terror Force, DDoS***

1. Necessity of Research

While observing the Iraq war between the United States and Iraq, which was then considered to have similar military power as North Korea, Kim Jongil realized the significance and importance of military use of information technology combined with advanced weapons. He has since stressed the importance of cyber warfare stating "Internet is a gun," "Know Republic of Korea's computer networks like the back of your hand," and "Cyber space is a shelter where national security law doesn't apply"[1].

Ever since, North Korea's cyber warfare capabilities have been growing at an alarming rate. At present, under the leadership of Workers' Party and Reconnaissance General Bureau, there are seven organizations of 1,700 hackers and approximately 4,200 employees working in this field in North Korea. From 2005 to 2007, North Korea engaged in website and email hacking. Then from 2008, it launched large scale cyber attacks using

* Funding Agency: This work was supported by Kyungwoon University Research Grant in 2016.

chatting, vaccine, and file-sharing websites. It is employing more sophisticated hacking techniques such as DDoS Attack which uses a network of zombie computers, penetration of websites and servers, data deletion, and self-destruction as of late[2].

As such, after the dictatorship has been passed on to the third generation, despite international condemnation, North Korea continues to conduct nuclear tests, fire missiles, and strengthen their cyber terror force. The strength of the current cyber terror force has grown so much that it can no longer be compared with that of the past.

This study examines the cyber attack cases of North Korea and the strength of its cyber terror force and makes an academic suggestion that can prevent cyber terrorism in the future.

2. Preceding Research

This <Table 1> summarizes the preceding research on North Korea's cyber terrorism.

Table 1. Previous studies.

Researcher	Main Content
Jung, Lim, Kwon (2016)	Analyzes cases of Republic of Korea's response and International response to North Korean cyber attacks and proposes countermeasure at a national level[3].
Lee, Lee (2015)	Proposes course of development for carrying out cyber warfare by conducting international law review of North Korean cyber attacks[4].
Kim (2014)	Analyzes the threats of North Korean cyber warfare and proposes countermeasures[5].
Kim (2014)	Examines cyber terror cases confirmed to be North Korean and discusses countermeasures[6].
Byun, Kim (2014)	Seeks practical countermeasure by analyzing the close correlation of internal power conflict due to changes in North Korea's high-ranking officials and terrorism[7].
Lim, Kwon, Jang, Baek (2014)	Objectively analyzes characteristics and pros and cons of the North Korean cyber terror force through examining North Korean cyber attack cases and relevant materials[8].
Kim (2013)	Investigates actual performance and capability of North Korean cyber terror force and proposes specific countermeasures at a national and military level[9].
Um (2012)	Proposes defense strategy that can efficiently prevent and cope with cyber attacks in a strategic and tactical stand point[10].
Bae (2011)	Analyzes North Korean cyber threat, proposes comprehensive course of development on preparedness at national military strategy level[11].
Park (2009)	Proposes national countermeasure against North Korean cyber attacks[12].

3. Researcher Summary

3.1. North Korea's 7.7 DDoS attack

On July 5, 2009 and on Independence Day on July 4, 2009 in the U.S., major U.S. websites, including those of the White House, fell victim to DDoS Attack. Beginning with this attack, from July 7 to July 10, Republic of Korea was hit by three simultaneous DDoS Attacks. As a result, access to 22 domestic websites, including those of the Blue House, was restricted[13]. The following <Table 2> lists the

14 U.S. websites, including those of the White House, that fell victim to the cyber attacks.

Table 2. 7.7 DDoS american victim institution[14].

Type of institution	Victim institution	Website
Government agency	White House	www.whitehouse.gov
	Federal Aviation Administration	www.faa.gov
	Home Land Security	www.dhs.gov
	U.S. Department of State	www.state.gov
	U.S. Department of Defense	www.defenselink.mil
	U.S. Department of the Treasury	www.ustreas.gov
	United States Forces Korea	www.usfk.mil
Financial institution	New York Stock Exchanges	www.nyse.com
	Nasdaq	www.nasdaq.com
	U.S. Bancorp	www.usbank.com
Miscellaneous	Voice of America	www.voanews.com
	Washington Post	www.washingtonpost.com
	Yahoo	www.finance.yahoo.co
	US Auction	www.usauctionslive.com

South Korean National Intelligence Service confirmed that the IP address which was used for the DDoS Attacks was the same one which North Korea's Ministry of Post and Telecommunications uses. The source of the attacks on major institutions of the Republic of Korea and the U.S. was tracked down and it was confirmed that the attack originated from a North Korean hacking organization stationed in North Korea.

Ministry of Post and Telecommunications is a government ministry in North Korea which is responsible for the postal service, telephone system, and media.

The institution that provides mobile communication and internet connection services is Korea Post and Telecommunications Company(KPTC) which is nominally controlled by the Ministry of Post and Telecommunications. Its servers are located overseas and it uses an assigned IP address. North Korea which only uses intranet internally, has its servers in China and users must type in IP addresses that are in numeric format to access the internet[15].

The currently existing DDoS Attacks originate from tens or millions of computers injected with malware which receive command directly from the C&C(Command & Control) server and flood websites with an enormous amount of simultaneous requests until the website's bandwidth resources become exhausted. The hijacked devices render a network inaccessible by generating a type or amount of network traffic that crashes the servers[16].

However, the 7.7 DDoS Attack showed different patterns from the existing DDoS Attack. With the 7.7 DDoS Attack method, a timer and attack command were embedded in the malware itself. It also included the malicious behavior command of damaging the hardware or the hijacked computers. Notably, it was an intelligent attack that combined the latest security threat circumvention techniques such as collaboration model among malwares, small-scale attacks that can circumvent existing security devices, and mixed attack into an intricate mechanism[17].

In addition, the purpose of existing DDoS Attacks is financial gain whereas the 7.7 DDoS Attack was aimed at instigating social disorder. The following <Table 3> summarizes the differences between existing DDoS Attacks and 7.7 DDoS Attack.

Table 3. Existing DDoS attack and 7.7 DDoS attack difference[18].

Category	Existing DDoS attack	7.7 DDoS attack
Existence of command and control server	Command-and-control server that receives commands from hacker exists	A server that updates malwares exists
Method of attack	Real time attack control through command-and-control server	Attack through scheduling and update of malware on a regular cycle
Method of infection	Website malware that exploits vulnerability of Windows or browsers	Malware that the attacker hid in a normal program
Defense method	Block command-and-control server	Remove malware of attacking PC
Target of attack	One or two websites	Simultaneous attack on multiple websites
Number of malware	Download one malware that carries out the DDoS attack	Download malware in the form of compressed file, perform various malicious behavior
Network Connection information	Able to monitor attack command contents by communication through plain-text channel	Unable to confirm communication content due to use of encrypted channel
Malicious behavior	Continuous execution of hacker’s command	Execute short-term attack then delete hard disk
Purpose of attack	Financial gain	Instigate social disorder
Hacking entity	Hacker organizations based in China	North Korea's ministry of post and telecommunications

In response, Korea Communications Commission(2009) increased its budget for hacking virus response system from 10.8 billion KRW to 38.4 billion KRW in 2009 in order to prevent the recurrence of 7.7 DDoS Attack and effectively respond to hacking viruses. The increased budget will be used towards establishment of DDoS emergency shelter, expansion of malware detection target websites, enhancement of cyber attack detection and response system. In addition, it will increase the budget to protect users for convergence service information protection correspondence which notifies internet users of a hacking victim or virus infection, provide vaccines, and provide information security forecasting service by providing the latest security information during national crisis situations.

3.2. North Korea's 3.4 DDoS attack

For three days from March 4, 2011, 40 major domestic websites were attacked by inserting malware in a domestic P2P website using 746 servers in 70 countries. The targets were the websites of major domestic government institutions including the Blue House, financial institutions, and internet portals.

Out of the 40 websites, financial institutions were attacked the most with 10 and 9 national defense websites were attacked as well. Unlike the 7.7 DDoS Attack where Republic of Korea and the United States were the targets, instead of the U.S., domestic national defense websites such as those of Joint Chiefs of Staff, Army Headquarters, Air Force Headquarters, Navy Headquarters, United States Forces Korea, Defense Acquisition Program Administration, and Defense Media Agency were targeted[16].

In addition, similarities in the design and communication method of malware from 7.7 DDoS Attack were found as shown in <Table 4>.

Table 4. 7.7 DDoS attack and 3.4 DDoS attack similarities[19].

Category	Content
Malware distribution location	P2P website
Computers used for attack	Mostly personal PC
Method of Attack	Command received from external server, pre-planned attacks
Target of attack	Public institutions, financial institutions, major internet portals
Purpose of attack	Unclear
Conclusion of attack	Concludes attack with destruction of hard disk

On the other hand, according to AhnLab's analysis, the increase in targets of attack, ability to update vaccines for the purpose of interrupting treatment by altering the infected computer's file, and ability to obstruct access to a website shows evolution from previous attacks. The following <Table 5> summarizes the difference in the 7.7 DDoS Attack and 3.4 DDoS Attack.

Table 5. 7.7 DDoS attack and 3.4 DDoS attack compare[19].

Category	7.7 DDoS attack	3.4 DDoS attack
Target of attack	22 Major websites including those of Blue House	40 Websites including those of the government such as the Blue House, major web portals such as naver and United States Forces Korea
Duration of attack	Three days from the 7th to the 9th. from 6pm to 6am the next day	Abnormalities detected in the afternoon on the 3rd. Began between 10am and 6:30pm on the 4th. End of attack is unclear
Damaged operating system	Windows based on .NET framework 2000/XP/2003	All Windows operating system

File configuration	Multiple attacks with the same file configuration	File configuration changes after each attack
Change in command	No changes	Changed command according to response
Treatment interruption	None	Disruption of vaccine update by altering host and obstruction of homepage access
Hard disk and File corruption time	In midnight on the 10th, the last day of attack when the file was corrupted, computers without vaccines had to change system date back	If the system date was set before infection date or noise0.3dat file which recorded the infection time was deleted, it was planned to be 7 days and 4 days after the infection, but it was changed to be damaged immediately after 9pm on the 5th.
Number of hijacked computers	115,044	116,299
Method of response	Massive confusion due to lack of preparation	Corporations and institutions were prepared after 7.7 DDoS, cooperation with security companies and related organizations minimized damage

3.3. Strength of cyber terror force

North Korea instructed the top leaders of the North Korean army after the 2003 Iraq war that "if the 20th century war is an oil war and a bullet war, the 21st century war is an information war so prepare for an electronic war" and encouraged the strengthening of cyber warfare capabilities. Accordingly, in order to overcome the gap in economy and military after 2000, North Korea focused on cultivating specialists in preparation for nuclear, missile, and cyber warfare by strengthening cyber warfare capabilities of Kim Il Political Military University, Kim Chaek University of Technology, Pyongyang Computer Technology University which were prepared in the mid-1990s, and cultivated and dispatched 300 hacking experts annually to the task force of Reconnaissance General Bureau, National Security Agency and North Korean espionage operations in the South[20].

As a result, North Korea is carrying out a security threat using cyberspace to instigate social disorder of Korean society and with systematic training since the beginning of the 1990s, about 6,800 cyber warriors have been put into North Korean espionage operations in the South. North Korea's cyber infrastructure is generally poor, but its cyber terrorism capability alone is ranked fourth in the world after the U.S., China, and Russia[21]. The following <Table 6> is analysis on the strength of North Korea’s cyber terror force.

Table 6. Cyber power analysis in North Korea[8].

Category	Content
Cyber Infrastructure	Poor infrastructure, very scarce Internet availability, and the use of a separate internal intranet are strategic advantages in defending, able to make the most of China's high quality Internet infrastructure in attack.
Interest and investment in cyber terror force	Like past leader Kim Jongil, Kim Jungeun has high interest in cyber warfare and is investing heavily in them.

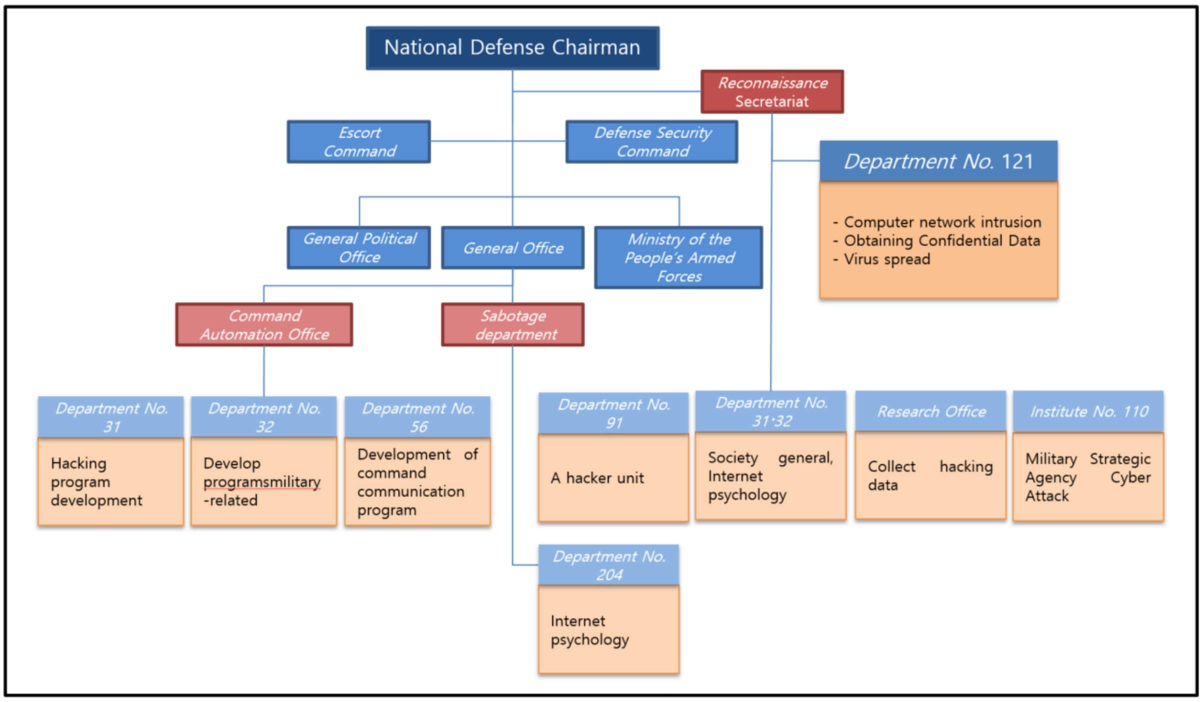
Cyber weapon system and technological capability	Offensive weapon system includes electronic weapons systems such as EMP and Jammer. Logical weapon system includes DDoS Attack, APT tools, malware, and logical bombs. Psychological weapon system includes spear phishing. Intranet security uses the defense system developed by North Korea, while maximizing use of security capabilities of Chinese security under attack.
Cyber agent	It is estimated that there are more than 6,800 cyber warriors, and an organized system of cultivating, utilizing, and rewarding cyber warriors exists. Cyber warriors enjoy high social status and various benefits.
Training system	Selects excellent workforce from youth, conducts intensive training from middle school to college. Outstanding cyber warfare specialists graduate every year are produced and dispatched in cyber terror forces and government agencies.
Organization system	It has a subordinate system to carry out hacking and psychological warfare under the Reconnaissance General Bureau and some units carry out tasks in Chinese territory

3.4. Cyber terror institution

North Korea's cyber terrorism is under the control of Cyber Jeonjidoguk121 under Reconnaissance General Bureau, while Leadership Formation and Jukgongguk are separately in charge of hacking program development and internet psychological warfare department and is overseen by the general staff department.

The North Korean Cyber Unit was reorganized in 2012, and the following <Figure 1> shows the department and main duties of the North Korean Cyber Unit.

Figure 1. North Korean cyber unit[15].


National Defense Chairman
Reconnaissance Secretariat
Escort Command
Defense Security Command
Department No. 121
- Computer network intrusion
- Obtaining Confidential Data
- Virus spread
General Political Office
General Office
Ministry of the People's Armed Forces
Command Automation Office
Sabotage department
Department No. 31
Hacking program development
Department No. 32
Develop programsmilitary -related
Department No. 56
Development of command communication program
Department No. 91
A hacker unit
Department No. 31·32
Society general, Internet psychology
Research Office
Collect hacking data
Institute No. 110
Military Strategic Agency Cyber Attack
Department No. 204
Internet psychology

In February 2009, North Korea's Reconnaissance General Bureau was newly established by integrating the Reconnaissance Bureau under Ministry of the People's Armed Forces and Operation Division under Korean

Workers' Party, and Room 35 with the purpose of directing espionage operations in the South and overseas and cyber warfare unit.

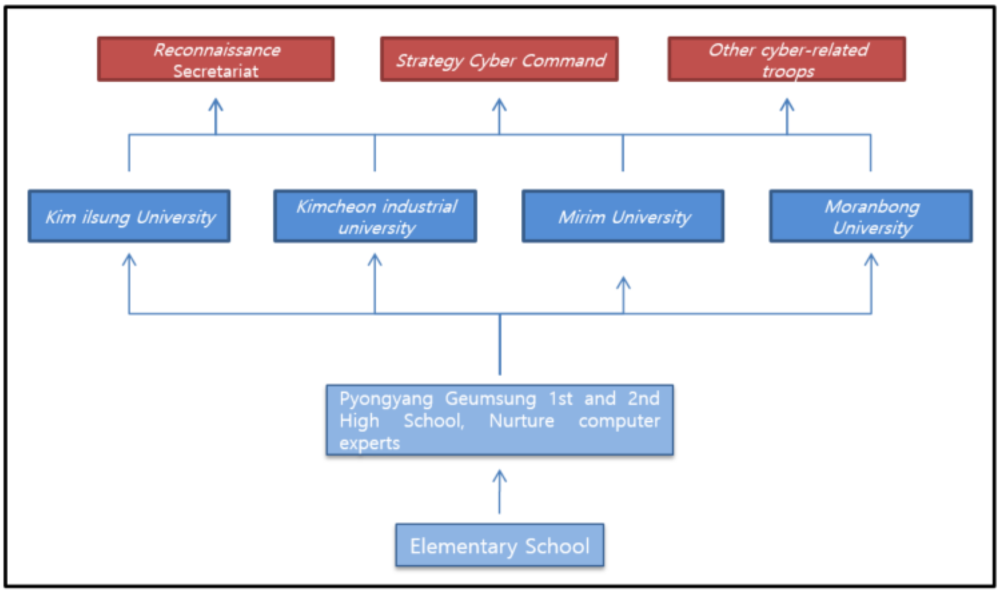
North Korea's Reconnaissance General Bureau consists of Cyber Jeonjidoguk121 which is in charge of invading computer networks and obtaining secrets, distributing computer viruses, and hacking, 91 So which is a hacker unit, 31 and 32 So which carries out psychological warfare in the general field of society, Research Office which collects information by hacking political, economic, and social institutions, and Laboratory 110 which is in charge of carrying out cyber attacks on military and strategic agencies.

Furthermore, separate organizations of Leadership Formation University Jukgongguk exist under the General Staff Department. Leadership Formation University consists of 31 So in charge of developing hacking programs, 32 So in charge of developing military programs, and 56 So which develops command communication programs. Jukgongguk consists of 204 So which in charge of internet psychological warfare.

3.5. Cyber terror education

North Korea's education system for cyber warfare specialist cultivation consists of three level. First level is Geumsung Middle School 1 and 2 which only the top students in elementary school are eligible, second level consists of Kim Ilsung University, Kimchaek Industry University, Leadership Formation University, Moranbong University, and the third level consists of the top students of the academic institutions of level 2 who undergo professional education and subsequently dispatched to cyber agencies such as Reconnaissance General Bureau and Strategic Cyber Command. North Korea considers cultivation of cyber warfare specialists as critical and is undergoing such process in a national level in professional academic institutions. The following table summarizes the process of North Korean cyber warfare specialist cultivation.

Figure 2. North Korean cyber warfare agent curriculum[15].


Reconnaissance Secretariat
Strategy Cyber Command
Other cyber-related troops
Kim ilsung University
Kimcheon industrial university
Mirim University
Moranbong University
Pyongyang Geumsung 1st and 2nd High School, Nurture computer experts
Elementary School

North Korea's representative cyber warfare specialist education institution is Kim Il Political Military University. In 1981, Mirim University which was established under the direction of Kim Ilsung was renamed to Leadership Formation University in 1986 and received support from the Soviet Ministry of Defense. In 1990, it was renamed yet again back to Kim Il Political Military University and has been producing over 100 cyber warfare specialists annually.

It produces around 500 to 600 graduates per year, and around 20 to 25 percent are specially dispatched to military staff related to cyber warfare. Currently Kim Il Political Military University is the most advanced computer university in North Korea and its self-developed software was even highly regarded in Japan[22].

In addition, Kim Il Sung University, Kimchaek University of Technology, and Moranbong University have been continuously selecting computer prodigies as North Korea’s generals and has been improving its operational organization command ability in regards to hacking attacks[13]. According to recent news reports, cyber warfare specialists cultivated from such academic institutions are 1,700 strategy personnel, 5,100 technology personnel, totaling 6,800.

4. References

4.1. Journal articles

[1] Kim SJ. Cyber Attacks and Our Response in North Korea. *Journal of North Korean Studies*, 516, 66-71 (2014).

[2] Song BS. North Korea's Cyber Attack Capability and Response. *Journal of North Korean Studies*, 525, 18-21 (2015).

[3] Chung MK & Lim JI & Kwon HY. A Study on North Korea’s Cyber Attacks and Countermeasures. *Journal of Information Technology Services*, 15(1), 67-79 (2016).

[4] Lee JS & Lee SJ. Defense Cyber Warfare Development Direction Based on the International Legal Review of the Nk's Cyber Attacks. *Journal of Security Engineering*, 12(4), 319-336 (2015).

[5] Kim DH. North Korean Cyber Warfare Threat and South Korean Action. *The Journal of the Institute of Internet Broadcasting and Communication*, 14(2), 1-10 (2014).

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

[7] Byoun CH & Kim EJ. The Changing Aspects of North Korea's Terror Crimes and Countermeasures: Focused on Power Conflict of High Ranking Officials After Kim Jong-IL Era. *Korean Security Science Review*, 39, 185-215 (2014).

[8] Lim HI & Kwon YJ & Jang GH & Baek SJ. North Korea`s Cyber War Capability and South Korea`s National Counterstrategy. *The Quarterly Journal of Defense Policy Studies*, 102, 9-45 (2014).

[10] Eom JH. Cyber Defense Strategy for Information Superiority in Cyberspace. *Journal of Security Engineering*, 9(5), 377-386 (2012).

[11] Bae DH. Direction for Coping with Cyber Threats of the North Korea in the Level of National Military Strategy. *Strategic Studies*, 52, 147-174 (2011).

[12] Park DK. Possibility of Cyber Terrorism by North Korea and National Preparedness Strategies. *Journal of Korean Association for Crisis and Emergency Management*, 1, 53-66 (2009).

[20] Shin CG & Lee SH. A Study of Countermeasure and Strategy Analysis on North Korean Cyber Terror. *The Journal of Police Science*, 13(4), 201-226 (2013).

[22] Kim SK & Lee DS. New Terrorism of North Korea and Countermeasures. *Unification Policy Studies*, 18(2), 67-96 (2009).

4.2. Thesis degree

[13] Chung YS. A Study on North Korea's Cyber Threatening Capabilities and ROK Forces Counter-response Polic. Sangji University, Master's Thesis (2013).

[14] Lee SU. A Study on Cyber Terror Response Model. Korea University, Master's Thesis (2015).

4.3. Books

[16] Son YD. Endless War of 0 and 1. Info the Books (2013).

4.4. Conference proceedings

[9] Kim KS. North Korea's Version Threat and Countermeasures. The Korean Association for Policy Studies Conference (2013).

4.5. Additional references

[15] http://www.yonhapnews.co.kr/ (2016).

[17] http://www.etnews.com/ (2016).

[18] http://www.mediadot.co.kr/ (2016).

[19] AhnLab. 3.4 DDoS Analysis Report (2011).

[21] http://www.unityinfo.co.kr/ (2016).

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

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

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

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

Research field
- The Study on the Domestic Adoption of the Air Marshal System in the U.S.A. Journal of Korea Security Science Association, 14(2) (2015).
- The Recognition of Koreans in Air Terrorism and Crime Outbreaks in Northeast Asia. International Journal of Criminal Study, 1(1) (2016).

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