211-0007
378 Tenjinchou Kamimaruko Nakaharaku
Kawasakishi Kangawhken Japan

ISSN: 2423-8376

International journal of terrorism & national security

2018 3(2)

<Index>

J-INSTITUTE

2018 3(2) 1-7 Submission: 2018/11/10, Peer review: 2018/11/20, Accepted: 2018/11/25, Published: 2018/12/30

International journal of terrorism & national security

Publication state: Japan
ISSN: 2423-8376

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

Corresponding author
E-mail: huhuhuu7@naver.com

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

http://dx.doi.org/10.22471/terrorism.2018.3.2.01

Review of Legislations on Location Tracking Investigation on TERRORISM

Yu Byung-hu

Osan University, Osan, Republic of Korea

Abstract

The reason why intelligence agencies investigating the crimes that threaten national security, such as terrorism today, uses location tracking in its investigation is that it is the most effective way to investigate individuals, who were at the scene of crime, to identify suspects. In this case, the intelligence agency and the investigation agency will acquire the number of all mobile phones through the base station that is responsible for the area in question, and if there exist a certain phone number and a number of call records already known by the intelligence agency and investigation agency, information of a specific person to be responsible for the crime-related behavior, then the scope of investigation is limited to the telephone numbers of persons who have shown communication or conduct related to crime such as communication information that has been confirmed to stay in a nearby area for a long time or that they have also contacted other base stations related to the crime.

However, location tracking using a base station will also get a minimum amount of calls for people who are not related to the crime. In some cases, the information that communicates with a particular base station is equivalent to the information that the communication was present near the base station. Therefore, even if the accuracy of the location information is low as long as the location information is obtained through base station investigation, the location information through base station investigation is strong. For these reasons, it is argued that it should be protected and should not be included in the communication confirmation data.

Finally, if not included in the data confirming the communication, the protection of the level of the search warrants should be maintained, and related legislation on crimes that threaten national security, such as terrorism, should be closely discussed and examined.

[Keywords] ***Location Tracking Investigation, Base Station Investigation, Communication Data, Communication Identification Data, National Security***

1. Introduction

The Korean investigation agency narrows crime suspects by requesting communication details of a specific base station instead of requesting transmission and reception communication details of a specific telephone number and acquiring all telephone numbers that are communicated with the base station. It acquires all the mobile phone numbers communicated with the base station in the sleep mode, not when the actual mobile phone calls are made. This is the base station investigation method which accounts for 98.6% of the acquisition of communication fact finding data. The number of times to confirm the communication details of the object after specifically specifying the object to be investigated is relatively lower than the case where the entire base station is searched and limited. Each telecommunication base station in the nation usually extracts about 7-8 thousand telephone numbers and extracts 37 million telephone numbers.

In particular, the reason why intelligence agencies and investigation agencies investigate

the suspects by tracing the location of crimes that threaten national security, such as terrorism, is usually because it is most effective to interrogate people who were at the crime scene as the only way to identify suspects. In this case, it is common that the intelligence agencies and investigation agencies collect and analyze the information of all mobile phones through the base station which is responsible for the area.

On the other hand, in order to obtain the communication identification data through the base station, it is necessary to approve the application that calls for the investigation and the approval of the court similar to the US law. However, it is true that there is a need for detailed requirements and procedures on how to extract the results of base station investigations that occur every year in Korea that need to be investigated. The reason for such a large number of base station investigations is that the investigation authorities have a large amount of all communication history of people who cannot be identified and analyze the data to identify the subject of investigation. Communication identification data can correspond to pen register and trap/trace information among US investigation terms, and specific telephone numbers or IP addresses transmitted and received are examples.

In this article, it aims to discuss the definition and necessity of location tracking investigation and a comparative review of location tracking system in the perspective of prevention of crime against national security.

2. Necessity and Issues of Location Tracking Investigation

2.1. Necessity of location tracking system

First, there is no precedent that establishes the legal logic that the accuracy of location information is comparable to the content of communication in terms of endurance. If it is required to treat the information differently from other communication fact-finding data only by the fact that approximate location information can be derived, it is possible to obtain the approximate location through the communication confirmation data such as the IP address or the landline telephone number New discussions are also needed. The development of technology and case law needs to be watched hereafter.

Also, much of the communication history obtained through the base station investigation is not the actual communication between the users, but the mobile phone communicates with the base station in a sleep mode. In some cases, the communication at this time is not included in the communication identification data because it is not a communication as a means of communication between people, and therefore, the base station communication information should not be acquired by the confirmation of communication and should be acquired by a seizure search warrant. However, this topic will not be discussed in this article. It is because the Communication Privacy Protection Act is intended to protect the secret of communication that contains the intention of the person among the secrets of the private life as a special rule. If the sleep mode communication is not communication, it can be claimed without any court permission, which is opposed to the author’s intent that it is not a type of communication.

In this regard, in the case of Germany, the technical signal of a communication means is merely a communication to guarantee the technological compatibility or readiness of communication. Data transmitted through a telecommunication facility is only qualified as a form of communication and content of communication when it is used to exchange ideas and information. In addition to the actual communication process, the commencement of the preceding communication is not a communication because it does not receive the same fundamental rights protection, so that it can be obtained without a warrant or other court's permission[1].

In the United States, however, there is a lot of controversy about whether pending communications is still included in pen registers/traps and traces. What is clear is that US courts consistently warrant a warrant for acquiring highly accurate location information using the waiting records of a plurality of base stations rather than a single base station.

2.2. Issues in location tracking system

A key problem with location tracking is approval by the court that although the police can

be authorized to obtain telecommunications data under weak criteria, the police are required to obtain the communication details of the majority of people who are unrelated to the crime in order to secure a suspect. Our reliance on most investigative techniques is due to the belief that we are not subject to investigation techniques, including requests for communications fact-finding data, except for some suspected criminals. However, base station investigations have taken the communication history of people who have nothing to do with the crime, and as a result, there is a fear that the police will treat almost all the people as potential criminals, and regardless of the intention of the investigating agency to search for the suspects, As long as it is revealed to the investigating authorities, the violation of many people can happen at the level of the suspect.

3. Comparative Law Review

3.1. United States

In the United States, Chapter 2 of the Electronic Communications Privacy Act(ECPA), called the Telecommunications Privacy Act, and the Stored Communications Act(SCA), called the Storage Communications Act, and Article 18 of the US Code, No. 2701-2712, And the request procedure for the 'stored communication information' of the investigation agency corresponding to the communication fact confirmation data[2]. The Telecommunications Privacy Act, which was amended several times since it was enacted in 1986, has a storage communications law as its detailed law, which has the authority to restrict access to "stored" or "past" telecommunications data[3].

For the purpose of security, the authority of the intelligence agency's overseas intelligence information and restrictions on communication restrictions are stipulated in the Foreign Intelligence Surveillance Act(FISA 1978). In Chapter 1 of the ECPA, eavesdropping, in Chapter 2, acquisition of stored communication information, and in Chapter 3, in the future, it is regulated about communication confirmation data.

In addition, US federal law does not distinguish between telecommunication data and telecommunication data, unlike the case in Korea, and the former telecommunication related records which do not include the telecommunication contents prescribed in Chapter 2 of ECPA are comparable to the concept of telecommunication data in domestic law However, this is interpreted as a concept that includes the communication confirmation data of Korea because it includes the communication related records besides the personal information of the subscriber.

In the SCA, "previous communication related records that do not include communication contents" are referred to as "basic subscriber information", including (A)name, (B)address, (C)(E) telephone number, equipment number, other user number or identity, temporarily assigned network address, (F)service cost, Payment method(including credit card number or bank account number). According to the Securities and Exchange Act, when an investigation agency requests 'communication information or records of a user' based on 'legitimate purpose or meet certain requirements', the operator may autonomously disclose information or records related to his/her work(optional) or mandatory.

In the event that it is determined in good faith that the contents of communications or other information or data of the subscriber should be disclosed without delay, in the urgent matter that may cause death or serious bodily injury, the carrier may arbitrarily disclose it to the appropriate investigation agency. However, if ① the court's warrant ② the order of the court ③ the request of the communication data according to the request of the document submitted by the government agency, the carrier must comply with the request.

A court's warrant requires proof of the plausibility of a criminal offense and requires a demonstration of 'relevance to an ongoing criminal investigation' as a less stringent requirement for a general warrant under a court order. In the case of telemarketing fraud investigation, it is possible to obtain telecommunication data by soliciting documents from the investigating agency without a court warrant order, and even if the applicant submits in writing the 'relevance between the information to be collected and the investigation of international terrorism or secret

intelligence activities' The communication data can be obtained without written permission. Regarding the procedures related to the notification of information collection by the investigating agency, if the communication data is obtained based on the warrant, the investigating agency is not obliged to notify the communication users of the communication data acquisition.

On the other hand, it seems that, in relation to the right of access to the users of the communication service, it does not require the communication users to read the information provision status as in Article 30 of Korea's Information and Communication Network Act.

In the meantime, the USA Freedom Act of 2015, which was enacted in the US in 2015, "Act for the United States Integration and Strengthening through Effective Control of Rights Realization and Monitoring in 2015" New legal standards have been laid down in relation to the 'record of continuous call history' corresponding to some of them. One thing to watch carefully in the Act is the introduction of the concept of 'call detail record' and 'specific selection term'. 'Call history record' means 'session identification information(incoming and incoming phone number, international mobile phone subscriber identification number, international portable device identification number), phone call card number, time and time of call'. The term 'specific selection term' means ‘a term or other specific identifier that identifies a person, an account, an address, or a personal device, and the use of this term’. For example, comprehensive selection terms such as 'residents in Asan City' or 'KT subscribers' restrict the use of strictly structured 'specific selection terms' because mass information may be collected indiscriminately. In the past, only 'relevance' had been called to the court when receiving permission to record 'continuous call history'. As a result of the revision of the law, 'relevance' and 'specific screening terminology', it must prove a "reasonable and clear charge" that is related to those involved.

In the past, only 'relevance' had been called to the court when receiving permission to record 'continuous call history'. As a result of the revision of the law, 'relevance' and 'specific screening terminology', it must prove a "reasonable and clear charge" that is related to those involved. Consecutive call log entries enhance the availability of large amounts of information in the range of time and scope of the data to be collected and increase the risk of privacy invasion.

3.2. Germany

The criminal justice system in Germany, which explicitly stipulates the investigation of telecommunication data using GPS location information[4], is similar to Korean criminal justice system, and the investigation using GPS location information is also explicit in relevant laws such as the Criminal Procedure Law And it is meaningful to refer to the legislative proposal in the future[5].

There is much controversy as to whether GPS location information can be viewed as an object of seizure or search. In this regard, it is necessary to discuss what kind of concept GPS understanding of GPS tracking information in Germany is. In Germany, the Criminal Procedure Law seizes Beschlagnahme as "the formal preservation (Sicherstellung) or the ordering of such preservation by transferring any object to an official state of preservation."

Objects of confiscation include all kinds of dynamic objects(bewegliche sache), including digital information. An order of the seizure(Anordnung der Beschlagnahme) is, in principle, carried out by a judge and, if there is an imminent danger(Gefahr im Verzug), it is also possible by an inspection or an order of the police Article 98(1) of the Sentencing Law.

On the other hand, GPS position tracking or collection of the information is distinguished from seizure. In other words, the term "beschlagnahmeähnlicher Vorgang" is used for the cases of Articles 100a, 100b, 100g and 100i of the German Penal Code for the verification of telecommunication data[6].

On the other hand, GPS location tracking based on Article 100h of the Sentencing Law uses a different concept of Observation, different from seizure. In other words, in the case of GPS location tracking, it is understood as 'a kind of surveillance' as a means similar to latent and follow-up as a traditional investigation method,

rather than as a conceptually 'seizing location information'. For example, if a police officer attaches a GPS location tracker to his vehicle to locate a vehicle or suspect owned by the suspect, such investigation does not involve confiscating or searching for any object, i.e. location information, which is the same as observing latency, tailing, etc., in order to confirm the movement path of the suspect vehicle. In this way, it is not necessary to discuss whether the GPS location information corresponds to the seized object, because the GPS location tracking investigation in Germany is classified as surveillance differently from the seizure. In other words, the GPS location tracking investigation is different from the conventional investigation methods such as seizure, and therefore it stipulates separately.

Article 100h of the German Criminal Procedure Code provides that, if it is difficult to accomplish the purpose of investigating the facts relating to serious crimes or confirming the place of stay of the suspects, other technical means may be used for the purpose of the Observations. It can be used in situations where the subject is unaware[7], including the GPS location tracker. In other words, this clause is a factor of ① serious crime, ② investigation of facts or identification of suspects, ③no other appropriate measures(principle of subsidiarity, subsidiaritätsgrundsatz), ④ special technical means for monitoring purposes, and ⑤ confidentiality. The law does not specify a specific means of GPS locator, but rather defines it as a "special technical means." Since the police can not specify in the text all the new means that the investigative agency can use to investigate, it is not against the law[8].

Article 100h of the Criminal Procedure Act stipulates the object of surveillance. Special measures such as GPS location trackers can, in principle, be used only for suspects(Article 100h Article 2(1)). However, you can only use the GPS location tracker for someone else unless the exception is related to the suspect and there is reason to believe that there is a serious difficulty in investigating the facts or finding the location of the suspect through other means. For example, it may be necessary to attach a GPS location tracker to the vehicle of his spouse to identify the location of the terrorist, and it is expressly stipulated in the Criminal Procedure Act on the assumption of such a situation.

This means is also permissible if the use of the GPS location tracker inevitably leads to the collection of third party information(Article 100h Article 3). In other words, if a GPS locator is attached to the vehicle of a suspect or a person who is related to the suspect, it is stated that the location information can be collected even if the vehicle is accompanied by a person who is not related to the event at all. This is a regulation that assumes that if it is unavoidable, it may infringe the right of self-determination of personal information by collecting location information of a third party.

3.3. Japan

In the case of Japan, it has been argued that it is an arbitrary investigation that the possibility of invasion of privacy is minimal because the GPS attached investigation technique is merely a means to assist the obedience and latency and the automobile is exposed to the general public. Regarding this issue, the Japanese court also ruled on whether it was "random investigation" or "forced investigation". The Supreme Court concluded that it was a "forced investigation".

The Japanese Supreme Court's rulings are as follows. According to the case, when the theft of stolen vehicles stole 4 million-yen worth of vehicles and clothes in 2013, Osaka police officers attached GPS trackers without warrants to 19 criminals and motorcycles for 8 months. In connection with the alleged theft, the defendants acknowledged the crime and were convicted of a sentence of five years and six months 'imprisonment. In response to the Japanese police' s unauthorized use of the GPS tracker, the Osaka District Court issued the "offense" The High Court ruled that it was "lawful." On the other hand, the consensus of the Supreme Court(15 people) interpreted that the investigation of attaching the GPS tracker seriously infringes on privacy, so it is obvious that it is a "forced investigation" that requires a warrant.

Therefore, it was concluded that it was illegal to attach a GPS without a warrant, while the general seizure search warrant was obliged to present before the enforcement, but it was impossible to investigate GPS attachments. Regarding legislative proposals, strict procedures

are required, and 'examples of a third party participation, term limitation, notification of parties' are listed as an example. In addition, some judges have proposed supplementary opinions[5] that it is possible to investigate GPS attachments only for extremely serious crimes in order to supplement the gap until the new law is established.

4. Implications

In the United States, when filing a "continuous call record" application, the court order should include: (1)Approval of daily call history is limited to a period of 180 days or less. (2)The intelligence agency can use 'specific screening terminology' to request the quick submission of the call history record of the first session, and then use the session identification information or phone card number identified in the 'specific screening term' To request a quick submission of call history records of subsequent secondary sessions. (3)Provided call history records should be in a form useful to intelligence agencies. (4) By protecting the confidentiality of records and minimizing disruption to business operators, the intelligence agency may direct personnel to provide all information, facilities and technical assistance to achieve the purpose of obtaining records. (5)If it is deemed that the call record provided pursuant to the court order is not intended for overseas intelligence information, a minimum procedure for the prompt destruction of all relevant call records shall be established and the record shall be destroyed pursuant to this procedure. You can tell the intelligence agency. (6)The court may approve the request for tangible goods only by using the "specific selection terms" stipulated in the Act.

The '2015 US Freedom Act' authorizes the Attorney General to request the provision of telecommunications-related materials without obtaining the order of the court in the event of an emergency. In this case, however, the Attorney General is obliged to follow strict procedures. If there is reason to believe that the material is needed prior to obtaining the order of the court due to an emergency situation, there is a factual basis for issuing a court order Limitations were made only when reasonably judged. In addition, the Attorney General must notify the Judge of the Foreign Intelligence Surveillance Court of the urgency judgment and apply for submission to the Judge of the Foreign Intelligence Surveillance Court within 7 days after the request for urgent data is submitted.

In Germany, the legal basis for GPS positioning is explicitly defined in the Criminal Procedure Act. These requirements include ① serious crimes, ② investigation of facts or identification of suspects, ③supplementing, ④special technical means for surveillance purposes, ⑤ confidentiality, and the obligation to notify, it is stipulated specifically in the Criminal Procedure Law. Regarding the warrant for GPS location tracking, we are tracking the GPS location based on the seized search verification warrant, but we understand it as one of the surveillance means that is separate from seizure in Germany.

Short-term GPS surveillance within 24 hours is allowed to be based on the order of the inspection or the police because it is not much different from the latency or follow-up as the conventional investigation means in the degree of infringement. However, the long-term GPS surveillance over 24 hours or more than two consecutive days requires a warrant issued by a judge because there is a significant difference in the degree of infringement of the basic right with latency and follow-up performed by a person. Of course, these judges' warrants need to be understood as' warrants for surveillance ', not our seizure verification warrants.

5. Conclusions

Since the end of the Cold War, terrorism has attracted attention as a major international issue that threatens international peace, including human rights and poverty. Terrorist aspects and terrorist environments are also gradually diversifying in response to changes in domestic and overseas security environments. In addition, the development of artificial intelligence technology and the possibility of exploitation of artificial intelligence, terrorism and crime related by AI are also required to be prepared.

No one will deny the need for communication restrictions in criminal investigations. In other words, the problem of the eavesdropping on the

communication is not whether to allow eavesdropping, but how to minimize the abuse. Restrictions on communication such as Internet wiretapping and location tracking investigation are inevitable as an inevitable measure to maintain national security and order against major terrorist threats at home and abroad, as well as serious crimes that violate people's lives, property and freedom.

However, as the Constitution argues, there is a concern that the confidentiality, privacy, and confidentiality of privacy may be infringed by the restriction of communication. Therefore, the procedure for approving general communication restrictions is more carefully executed, it is time to actively discuss ways to ensure that the due process is ensured in the process.

Currently, wiretapping is evaluated as an effective method to deal with serious crimes such as drugs, terrorism and national security, or global crimes. Prohibition of the technology that is currently available makes it impossible for the investigating authorities to tempt illegal tapping it is because. In addition, it has been confirmed that wiretapping is a kind of other communication restriction measures such as the method of information collection and the amount of information to be collected, Therefore, it is considered unnecessary to make an attempt such as the legislative discussion to permit or prohibit wiretapping, or to stipulate requirements for wiretapping under the "Communications Confidentiality Protection Act" unlike the general wiretapping.

On the contrary, it strictly stipulates the procedures for requesting the eavesdropping system and requesting the eavesdropping permission, recording the necessary information among the information gathered by the eavesdropping process, discarding the remaining information, supervising the eavesdropping procedure, it is necessary to first consider the measures that can minimize the infringement of the confidentiality of the personal communication.

6. References

6.1. Journal articles

[4] Park CK & Kang DW. The Problem and Improvement of Communication Data in the Telecommunications Business Act. *Journal of Law and Politics Research*, 14(1), 9-41, (2014).

[5] Kim JO & Park WK. A Legal Study for Using GPS Location Tracker for Investigation. *Review of Public Security Administration*, 15(2), 81-112 (2018).

[7] Lee SK. Discussion on the Legal Obligation of the Telecommunication Operators in Providing Investigation Authorities with Communication Confirmation Data & Communication Data. *Journal of Law and Politics Research*, 14(1), 43-67 (2014).

[8] Park HY. Befugnis zur Erhebung und zum Ersuchen von Verkehrsdaten in Deutschland und in Korea. *Journal of Police Science*, 9(3), 33-61 (2009).

6.2. Thesis degree

[3] Kim JO. A Legal Study on the Improvement of Communication Investigation Procedure. Korea University, Master's Thesis (2018).

6.3. Additional references

[1] BVerfG, Beschluss vom 22.8.2006 - 2 BvR 1345/03.

[2] 18 U.S.C.A. § 2703.

[6] Meyer-Grossner, Vor §94 Rn. 3, 2013.

Author

Yu Byung-hu / Osan University Professor
B.A. Honam University
M.A. Dongguk University
Ph.D. Dongguk University

Research field
- Improvement Plan of the Police Employment Examination through Trend Analysis of Introduction of Police Science, Korean Journal of Police Science, 15(3) (2016).
- The Current Position of Private Security, and Prospect, Journal of Private Security, 17(1) (2018).

Major career
- 2017~present. Korean Association of Terrorism Studies, Member
- 2017~present. International Society for Terrorism and National Security, Member

2018 3(2) 8-14
Submission: 2018/11/10, Peer review: 2018/11/20, Accepted: 2018/11/25, Published: 2018/12/30

International journal of terrorism & national security

Publication state: Japan
ISSN: 2423-8376

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

Corresponding author
E-mail: didsun99@kimpo.ac.kr

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

http://dx.doi.org/10.22471/terrorism.2018.3.2.08

Research on Potential TERRORIST Threat and NATIONAL SECURITY Crimes

Yang Seong-don[1]

Kimpo University, Kimpo, Republic of Korea

Kim Hyung-wook[2]

Kimpo University, Kimpo, Republic of Korea

Abstract

Today, national security throughout the world is expanding and deepening the scope and types of transnational threats such as terrorism, cybercrime, weapons of mass destruction, and drug offenses. In recent years, transnational national security threats have been dominated by non-state actors, such as individuals or various interest groups within a country, multinational corporations, international organizations, and terrorists. As these non-state actors transcended borders, their importance and role in the international society increased. In the past, information activities were mainly conducted at the national level, but the task of collecting and analyzing information about non-state actors was added.

On the other hand, potential terrorism threats that threaten national security is different from traditional security threats in response. Traditional security threats, such as war and military threats, could be resolved to some extent by a realistic approach that focuses on alliances, balance of power, and collective security measures across countries. However, transnational security issues such as terrorism are largely out of the realistic framework of consciousness, and information security cooperation among nations can be relatively smooth because of the low possibility of a security dilemma in the case of such a transnational security threat.

Transnational crimes that threaten national security are far more difficult tasks than traditional warfare with traditional sovereign states. It is not easy to capture the target of the terrorist organization easily, it carries out the war in the form of defensive rather than the attack by nature, and even if the current leader of the terrorist organization is arrested or dies, the successor appears constantly and it is very difficult to reach the final crush. In addition, the bottom of the issue of terrorism is based on the assumption of religion and conviction that most terrorist organizations are convinced of their final victory and never accept defeat, so that the war on terror is much more difficult and persistent than the war between countries.

In addition, terrorism is a deadly threat to national security because terrorist organizations do not limit their targets even in case of attacks against innocent civilians. The emergence of such transnational threats further demands a close link between the national intelligence community and the law enforcement community. Thus, national intelligence also demands a statutory understanding comparable to that of law enforcement, which is the incarnation of the rule of law.

Therefore, only when it is accompanied by a lawful understanding and understanding of national intelligence, it will provide permanent and constant value to national intelligence activities. It can be said that it is a way to systematically develop democracy, openness and national intelligence, but it should be done within the scope that the purpose of counterterrorism based on rule of law is not undermined.

[Keywords] ***National Security, National Security Crime, Terrorism, Transnational Crime, Security Dilemma***

1. Introduction

In modern society, indiscriminate terrorist crimes against unspecified number of people continue to occur due to social conflicts derived from various reasons such as political ideology, religion, gap between the rich and the poor, ethnic background, and history. The number of terrorist attacks that threaten the national security and society, such as the cyber attacks against NH Bank in Korea and ISIS use of the Internet for terrorist purpose. In other words, unlike the past, the purpose of terrorism is not limited to political and military ones, but also extends to religious and social problems or economic interests. In addition, terrorist attacks are being developed through the Internet, science and technology, and the subject of terrorism is not a large organization, but is organized or personalized, and the object of terrorism is not an individual, And it is evolving into a new form, such as being carried out against those who are innocent and non-specific victims[1].

In addition, the scope and the field of intelligence activities are expanding as various elements threatening national security are highlighted. Uncertainty of intelligence targets and diversification of intelligence agenda have increased the difficulties of effective intelligence activities by intelligence organizations[8]. Recently, the notion of the National Security Crime(NSC) can occur locally, such as terrorist attacks derived from radicalized ones or the destruction of constitutional order by anti-state groups, and it must defend liberal democracy through proactive and active defenses against NSC.

Ultimately, the world is already doing its best to set up special procedure for criminal justice by establishing a special law on criminal law in order to cope with not only new forms of terrorism crimes but also transnational crimes that threaten national security.

On the other hand, in case of Korea, the law on crime of terrorism and other national security threats is insufficient. Under the general criminal law system, evidence collection and criminal investigation are conducted in the same manner as other criminal cases. In the end, the current legal system is forced to focus on criminal investigations after the incident threatening national security, and it is very difficult to achieve the goal of protecting the State and its citizens, who are the ultimate victim in cases of crime against national security.

In this article, it aims to discuss the meaning and nature of terrorism, which may be a potential threat to national security.

2. Backgrounds of National Security Crime

2.1. Definitions

Although the term "national security" is illustrated in the Korean Constitution, there is no definite conceptual definition of national security, and there is no concept of national security in national laws such as the National Intelligence Service Act. Therefore, it is unclear in Korea what constitutes a crime that threatens national security and who is an offender of a crime against national security. On the other hand, the intrinsic meaning and scope of NSC in Korea can be broadly expanded. In general, NSC is a crime that violates national legal interests such as criminal insurrection, foreign aggression and violation of the National Security Act by a terrorist organization that has an enemy for the destruction of the Korean constitutional order[7].

2.2. Definitions of NSC in the United States

In American society, the NSC defines crimes aimed at harming the national security itself, not the hate of any individual, but the community order[3][5]. The crime of national security is classified as a crime of treason, espionage, sabotage, and terrorism, which are related to both of rebellion and foreign criminality. These types of NSCs are areas where intelligence and investigation are linked, and a wide range of surveillance activities and non-classification systems are applied. Needless to say, the NSC is simply an area that can not be coped without the role of national intelligence activities. In that case, intelligence activities are not only a means of policy provision, but are connected with law enforcement for final judicial decision, and since the investigation does not start from the beginning, it brings lots of controversies in

realizing justice through general criminal law[2].

However, due to the close relationship between intelligence and investigation, it raises a difficult question as to what can be done under the Constitution in order to prevent and punish the national security crime when the legal system on national security is not completed. For example, the question of how to meet judicial demands for evidence laws when there is a possibility that a national intelligence agency that does not have individual investigation rights against terrorism or sabotage activity may lead to judicial judgment even if it is the information or intelligence gathering level is a challenge.

The conflict goes on in case of a terrorist attack that threatens national security. Here is an example. If the case is major threat to national security, would it be possible to conduct a wide range of interception targeting suspicious individuals, to investigate them by following and putting surveillance, or to torture them? The nature of the unique crime and the conflict of the choice of policy means in the bridging of the existing judicial system are heightened. Despite the risks of indiscriminate massive violation of human rights, the question of whether to use body search, and intelligence and investigation techniques for greater goal for national security is a challenge in the real world.

In the end, the choice is related to a distributive justice, and the request for a distributive justice largely requires a decision between two values. It is still necessary to endure the due process of the national catastrophe in order to adhere to the due process and to avoid the risk of violation of human rights against suspects, or to take measures designed to counter the threat, though not without the risk of violation of human rights against the suspect. It is a matter of choosing whether to secure security and thus protect the freedom and peace of most ordinary citizens. Finally, the key to problem solving is the issue of the distributive justice of how much exemption can be allowed in each country's security environment, and to what extent the data obtained by information-gathering activities are acceptable as evidence of judicial condemnation.

Therefore, in cases where the existing criminal proceedings are still adhered to in the trial of the NSC, there is almost no exception, resulting in the issue of evidence of illegal collection, and in many cases the judgment of innocence is expected and the actual legal punishment for the NSC appears as a difficulty[6].

3. Types of NSC

3.1. Treason

The treason includes the rebellion and the landesverrat crime, as well as sedition. The treason is defined and illustrated in the 18 U.S. Code Chapter 115. Types of crime illustrated as treason are as follows:

§ 2381 - Treason

§ 2382 - Misprision of treason

§ 2383 - Rebellion or insurrection

§ 2384 - Seditious conspiracy

§ 2385 - Advocating overthrow of Government

§ 2386 - Registration of certain organizations

§ 2387 - Activities affecting armed forces generally

§ 2388 - Activities affecting armed forces during war

§ 2389 - Recruiting for service against United States

§ 2390 - Enlistment to serve against United States[6].

3.2. Espionage

Espionage is defined and illustrated in Economic Espionage Act(EEA) and 18 U.S. Code Chapter 37. Types of crime illustrated as espionage are as follows:

§ 792 - Harboring or concealing persons

§ 793 - Gathering, transmitting or losing defense information

§ 794 - Gathering or delivering defense information to aid foreign government

§ 795 - Photographing and sketching defense installations

§ 796 - Use of aircraft for photographing defense installations

§ 797 - Publication and sale of photographs of defense installations

§ 798 - Disclosure of classified information

§ 799 - Violation of regulations of National Aeronautics and Space Administration

§ 2388 - Activities affecting armed force during war

and violation of Foreign Agent Registration Act(FARA)[6].

3.3. Terrorism

In the Counterterrorism Section(CTS) of the Federal Ministry of Justice, type of terrorism is illustrated as follows: § 2332a - Use of weapons of mass destruction § 2332b - Acts of terrorism transcending national boundaries § 2332d - Financial transactions§ 2332f - Bombings of places of public use, government facilities, public transportation systems and infrastructure facilities § 2339B - Providing material support or resources to designated foreign terrorist organizations

§ 2339C - Prohibitions against the financing of terrorism

§ 2339D - Receiving military-type training from a foreign terrorist organization

49 U.S.C. §§ 46501-07 Aircraft piracy and related offenses

§ 32 - Destruction of aircraft or aircraft facilities

§ 115 - Influencing, impeding, or retaliating against a Federal official by threatening or injuring a family member

§ 1651 - Piracy under law of nations

§ 1203 - Hostage taking

§ 2332 - Criminal penalties

§ 956 - Conspiracy to kill, kidnap, maim, or injure persons or damage property in a foreign country

§ 2339A - Providing material support to terrorists

§ 2339B - Providing material support or resources to designated foreign terrorist organizations

§ 2339C - Prohibitions against the financing of terrorism

§ 2339D - Receiving military-type training from a foreign terrorist organization

§ 175 - Prohibitions with respect to biological weapons

§ 831 - Prohibited transactions involving nuclear materials

§ 1091 - Genocide

§ 2441 - War crimes

§ 2340A - Torture

3.4. Sabotage

Sabotage activities are intended actions aimed at achieving the purpose through overturning, obstacles, confusion and destruction of production facility or transportation machinery of national important facilities. Punishment is discussed as destructive activity rather than simple espionage. Types of sabotage are illustrated in section 105 of the United States Code of Federal Regulations:

§ 2152 - Fortifications, harbor defenses, or defensive sea areas

§ 2153 - Destruction of war material, war premises, or war utilities

§ 2154 - Production of defective war material, war premises, or war utilities

§ 2155 - Destruction of national-defense materials, national-defense premises, or national-defense utilities

§ 2156 - Production of defective national-defense material, national-defense premises, or national-defense utilities[6].

4. Essential Difference between Crime and General Criminal Offense for National Security

4.1. The nature of NSC

The NSC is different in nature from the criminal offenders in general. NSCs do not fear punishment after the arrest, but have some features that makes individuals or organizations unique from others with solidarity and confidence that surpasses national authority. First, the NSCs are thorough experts, and they are thoroughly trained in physical, mental, and technological ideology, ideologically the best crime specialists, in addition to the crime methods and the responses in the investigation and trial. After a careful judgment, they commit the crime. They are trained spies, weapon dealers, manufacturers, and financial and organizational leaders.

Second, NSCs are extremist mass criminals who are motivated and hope for the greatest possible national disaster as much as possible of the type of conduct or consequences of their choice. They are the ones whose ultimate goal is to destroy the regime or the target nation. They try to use the most violent means, such as attempting to launch a war against the sovereign state, to initiate a war based on subjective ideology or political antipathy, to try to start a war, to destroy national infrastructure, to assassinate factors, They are some kind of social contract violators who are trying to induce tremendous fear.

Third, the NSC is an unfamiliar crime in the perspective of investigation and trial. It is important to keep the secret that how intelligence activities and investigation have been carried out in order to penetrate into the national security system and be caught by the authorities so as to arrest them. Thus, it would never be justified to disclose the investigative method and documents in individual case no matter how there is a principle of open trial.

Fourth, the difficulty of identification and detection of NSC leads to the scarcity of the number of occurrences. However, it must be recognized that the threat of insurgence, landesverrat or espionage still exists. It is not unkown to the public because there is no traitor or spy. In the context of confrontation with hostile forces and very rarely, but when it does occur, it is not difficult to guess how many spies and national security conspiracy crimes have been committed unknowingly. Like where there is competition, spies exist. The threat to national security does not cease, but it is only the tip of the iceberg that it is difficult to uncover the reality.

Fifth, there is always not enough evidence in the court to convict the NSC and punish it. It is the most effective and international solidarity to be developed in connection with the foreign powers or hostile countries in the nature of national security crimes. Therefore, the nature of such crimes is that the half of the evidence is always in the enemy country or abroad. As a result, it is impossible to expect a proper investigation of evidence[5].

4.2. The characteristics of NSC

In general, the nature of NSCs that threaten national security has different characteristics from ordinary criminal offenses. First, the NSCs are thoroughly trained criminal experts, and they are extremist serious criminals who are more willing and hopeful of national disasters than to infringe on personal legal interests. In addition, NSCs appear to be highly confidential in investigations and court proceedings due to the risk of processing crimes, and the difficulty of detecting and detecting information and investigation agencies due to NSC's secret means and methods leads to the scarcity of incidents However, it must be recognized that it is by no means a threat to national reconciliation, landesverrat or espionage, and terrorism, or to mean that there has never been such a thing. Because NSC is always lacking enough evidence to prove and punish the crime, there are difficulties and considerable restrictions on the collection of evidence by intelligence and investigation agencies.

5. Conclusions

Transnational crimes that threaten national security, such as terrorism throughout the world today, are wars against nations without borders, but they are far more difficult tasks than

traditional warfare with traditional sovereign states. It is not easy to capture the target of the terrorist organization easily, it carries out the war in the form of defensive rather than the attack by nature, and even if the current leader of the terrorist organization is arrested or dies, the successor appears constantly and it is very difficult to reach the final crush. In addition, the bottom of the issue of terrorism is based on the assumption of religion and conviction that most terrorist organizations are convinced of their final victory and never accept defeat, so that the war on terror is much more difficult and persistent than the war between countries.

In addition, terrorism is a deadly threat to national security because terrorist organizations do not limit their targets even in case of attacks against innocent civilians. The emergence of such transnational threats further demands a close link between the national intelligence community and the law enforcement community. Thus, national intelligence also demands a statutory understanding comparable to that of law enforcement, which is the incarnation of the rule of law[4].

Therefore, only when it is accompanied by a lawful understanding and understanding of national intelligence, it will provide permanent and constant value to national intelligence activities. It can be said that it is a way to systematically develop democracy, openness and national intelligence, but it should be done within the scope that the purpose of counterterrorism based on rule of law is not undermined.

6. References

6.1. Journal articles

[1] Choi DH. Criminal Investigation Practice and Law in U.S Domestic Terror. *Institute of Justice*, 31(2), 397-480 (2016).

[2] Barak ED. Distributive Justice in National Security Law. *Harvard National Security Journal*, 3, 283-307 (2012).

[3] Creegan E. National Security Crime. *Harvard National Security Journal*, 3, 373-430 (2012).

[4] Han HW. A Study on the Legal Character of the National Intelligence Activities: Focusing on the Lesson from U.S.A Intelligence Community and the Legality of National Intelligence. *Review of National Intelligence*, 4(2), 95-125 (2012).

[5] Han HW. A Legal Normative Study on the National Security Innovative Model According to the Newly Transformed Security Environment. *Journal of Criminal Law*, 49, 239-281 (2015).

6.2. Books

[8] National Intelligence Studies. 21 Century National Counter-intelligence. Parkyoungsa (2014).

6.3. Conference proceedings

[6] Han HW. Security Reform and Counter-communism Investigations. Korean National Security and Criminal Law Association (2018).

[7] Lim YS. Meanings and Challenges in National Security in Modern Times. Korean National Security and Criminal Law Association (2017).

Lead Author
Yang Seung-don / Kimpo University Professor
B.A. Soonchunhyang University
M.A. Dongguk University
Ph.D. Dongguk University

Research field
- Application Plan of U.S. Aviation Profiling for Prevention of Air Terrorism in Korea, Korean Security Review, 38 (2014).
- A Study on the Trend and Countermeasure of Cyber Terrorism, Review of Korean Terrorism Studies, 11(2) (2018).

Major career
- 2011~present. Korean Association of Terrorism Studies, Member
- 2015~present. Korean Association of Police Science, Member

Corresponding Author
Kim Hyung-wook / Kimpo University Professor
B.A. Yongin University
M.A. Yongin University

Research field
- Against the Punitive Preliminary Provisions of the Terrorist Attacks, Review of Korean Terrorism Studies, 10(4) (2017).
- A Study on the Trend and Countermeasure of Cyber Terrorism, Review of Korean Terrorism Studies, 11(2) (2018).

Major career
- 2010~present. Seoul Association of Taekwondo, Board Member
- 2015~present. Korean Association of Terrorism Studies, Member

2018 3(2) 15-18 Submission: 2018/11/10, Peer review: 2018/11/20, Accepted: 2018/11/25, Published: 2018/12/30

International journal of terrorism & national security

Publication state: Japan
ISSN: 2423-8376

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

Corresponding author
E-mail: borapark@inss.re.kr

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

http://dx.doi.org/10.22471/terrorism.2018.3.2.15

Introduction of Asia Dialogue on TERROIST Use of the ICT

Park Bo-ra

Institute for National Security Strategy, Seoul, Republic of Korea

Abstract

Technology in the digital age has become a new battleground for countering terrorism. The Internet has no time and space constraints, and it has established a cyber space that allows free expression of opinion, exchange of thoughts, rapid speed of sharing information, and building friendship with individuals from all walks of life and the place. This feature is why terrorist organizations use the Internet to achieve their goals and spread their propaganda. For this reason, the Internet has become an effective means of communication to maintain the terror network, and the spread of social media has led to the expansion of cyberspace and the multichannels of interactive communication. As a result, security threats such as the use of the Internet for terrorist purposes has also emerged.

In this article, it aims to introduce how the international community has respond to the emerging threat focusing on the terrorist use of the ICT. In particular, it aims to illustrate and discuss Asia's effort to counter terrorist use of the ICT.

The international community including the United Nations is responding to security threats such as the use of the Internet for terrorist purposes by establishing a legal and policy framework, investigating cases of Internet use for terrorism purposes and gathering information, building international cooperation, and building public-private partnership(PPP). With the advent of the Fourth Industrial Revolution, the scope of its effort has been expanded to the use of Internet and other technologies for terrorism purposes.

The new type of security threat is not a single type, but the sum of a small variety of non-state actors who have relatively little influence from the traditional security perspective. In particular, the extreme terrorism based on religion has been pointed out as the most important security threat. The diversification of terrorist organization, which is characterized by new terrorism, and the worldwide spread of fear of terrorism due to informationization, developing active measures for counterterrorism is getting more and more difficult.

Terrorist threats that exploit information and communication technologies in the era of globalization are growing and expanding, so a more comprehensive approach to terrorism related to the Internet and information and communications technologies is required.

[Keywords] ***Asia Dialogue, Terrorist Use of the Internet, UNCTED, Terrorist Use of the ICT, UN Security Council Resolution***

1. Introduction

Technology in the digital age has become a new battleground for countering terrorism. The Internet has no time and space constraints, and it has established a cyber space that allows free expression of opinion, exchange of thoughts, rapid speed of sharing information, and building friendship with individuals from all walks of life and the place. This feature is why terrorist organizations use the Internet to achieve their goals and spread their propaganda[1]. For this reason, the Internet has become an effective means of communication to maintain the terror network, and the spread of social media(SNS)

has led to the expansion of cyberspace and the multichannelization of interactive communication. As a result, security threats such as the use of the Internet for terrorist purposes has also emerged.

In this article, it aims to introduce how the international community has respond to the emerging threat focusing on the terrorist use of the ICT. In particular, it aims to illustrate and discuss Asia's effort to counter terrorist use of the ICT.

2. UN's Efforts for Countering Terrorist Use of the Internet and ICT

2.1. UN security council

The international community including the United Nations is responding to security threats such as the use of the Internet for terrorist purposes by establishing a legal and policy framework, investigating cases of Internet use for terrorism purposes and gathering information, building international cooperation, and building public-private partnership(PPP). With the advent of the Fourth Industrial Revolution, the scope of its effort has been expanded to the use of Internet and other technologies for terrorism purposes.

In addition, the UN Security Council Resolution No. 2129(2013) and the UN Security Council Resolution No. 2354(2017) provide concrete action plans to prevent the exploitation of information and communication technology (ICT) by terrorist organizations. Some of each resolution is as follows:

The UN Security Council Resolution 2129 (2013) is a report on the use of information and communication technologies, such as the Internet, for terrorist organizations to conduct terrorist acts, recruit terrorists, It is pointed out that the relationship between information and communication technology is evolving in UNSCR 2129. The resolution also instructs the UN Counter-Terrorism Committee Executive Directorate(UNCTED) to continue to address these issues through cooperation with Member States, international organizations, regional organizations, interregional organizations, the private sector and civil society. In addition, the resolution instructs the UN Counter-Terrorism Committee to make recommendations on future directions on these issues as well[2].

UN Security Council Resolution 2354(2017) calls for the United Nations Counter-Terrorism Committee to develop initiatives to strengthen public-private partnerships in response to terrorism narratives, and welcomes the *Comprehensive International Framework to Counter Terrorist Narratives(S/2017/375)* confirming UNCTED's "Tech Against Terrorism"[3].

2.2. UNCTED

In 2016, United Nations Counter-Terrorism Committee Executive Directorate(CTED) and the ICT4Peace Foundation in Switzerland started a project to encourage private sector cooperation to combat the exploitation of ICT technologies for terrorism. The project was designed to include governments, the private sector, trade associations, the city community, academia, various stakeholders and private initiatives. The final report of this project covers in-depth analysis of the gap between each participant, policy recommendations, obstacles to public-private partnerships, and current trends. The follow-up project is the "Tech against Terrorism (TaT) Initiative"[4].

On June 26, 2017, the Global Internet Forum to Counter Terrorism(GIFCT) was established around Facebook, Microsoft, Twitter, and YouTube. The purpose of the forum is to develop technical solutions, conduct related research, and share knowledge with small and medium-sized ICT companies in order to contribute to global counter-terrorism activities. In the future, the Global Counter-Terrorism Internet Forum(GIFCT) will conduct a number of activities within the TaT initiative led by the UNCTED.

On November 29 of the same year, the TaT Initiative established and implemented an online Knowledge Sharing Platform(KSP) in cooperation with the Korean government and the Global Counter-terrorism Internet Forum. On-line Knowledge Sharing Platform provides tools and resources for start-up or small and medium-sized ICT companies to counter terrorist Internet abuse. The TaT approach will encourage active involvement of the private

sector, support autonomous regulation of the industry, and promote the ICT enterprise's responsibilities.

3. Asia Dialogue on Terrorist Use of the ICT

3.1. The 1st meeting of Asia dialogue: Jeju, Republic of Korea

Based on continuous cooperation, the United Nations Counter-Terrorism Committee Executive Directorate(CTED) and the Global Counter-Terrorism Internet Forum(GCTIF) are looking forward to working with key stakeholders, including civil society organizations and academia, as well as start-up companies and encouraging dialogue for effective and robust cooperation of key stakeholders. In this context, in May 2017, with the support of the Korean Ministry of Foreign Affairs, "Asia Dialogue to Prevent Exploitation of ICT by Terrorist Organizations" was held in Jeju, Korea.

UNCTED and Ministry of Foreign Affairs of the Republic of Korea(MOFA) convened a two-day workshop on terrorism and information communication technologies. The first workshop consisted of three regional workshops aimed at building confidence among relevant stakeholders, within the framework of international and regional cooperation to counter terrorism in respect for human rights standards.

As UNSCR 2129(2013) notes the evolving nexus between terrorism and information and communications technology(ICT), in particular the Internet, as well as the use of such technologies to commit terrorist acts and to facilitate such acts through their use to incite, recruit, fund or plan terrorist acts, participant shared experiences and challenges encountered in countering incitement and violent extremism leading to terrorism, developing counter-narratives, gathering digital evidence, enhancing the practices of private online intermediaries, and empowering online communities[5].

They also explored practical ways to strengthen implementation of *UNSCR 1624(2005)*, on incitement; *UNSCR 2178(2014)*, on countering violent extremism; and the Council's presidential statement of 11 May 2016(S/PRST/2016/6), on the development of counter messaging and alternative messaging[5].

3.2. The 2nd meeting of Asia dialogue: Bangkok, Thailand

The follow-up meetings were held in Bangkok, Thailand in January 2018. Participants was able to discuss the experiences of terrorism and violent extremism, the development of counterterrorism and counter-extremist narratives. In addition, they shared experience on implementing empowerment of online communities, enhancing public-private partnership, and challenges in implementation.

Furthermore, participants also explored practical ways to strengthen implementation of UNSCR 1624(2005), UNSCR 2129(2013), UNSCR 2178(2014), UNSCR 2322(2016), UNSCR 2341(2017), UNSCR 2354(2017), and UNSCR 2396(2017). They encouraged to implement *International Framework to Counter Al-Qaida and ISIL Narratives(S/2017/375)* as well[6].

3.3. The 3rd meeting of Asia dialogue: Kuala Lumpur, Malaysia

At the third meeting held on both November 7 and 8, 2018, the agenda of the first and second meetings and the implementation of the aforementioned UN Security Council resolutions were considered as the main agenda. Especially, in the nature of the Asian dialogue, the General Assembly decided to implement the UN Security Council resolution to prevent terrorism-related information and communication technology(ICT) and use of the Internet and cyber activities by foreign terrorist fighters(FTFs) in connection with the spread of violent extremism in Asia. Participants shared their government' efforts to prevent the abuse of ICT by terrorist groups in Asia.

The discussions by working groups were divided into the following topics: online violence against extremism and anti-extremist narrative development, public-private partnership for preventing abuse of ICT by terrorist organizations, self-regulation in ICT industry, and cyber protection of important national infrastructure. Particularly in the case of the

Philippines, the prevention of violent extremism was recognized as an important national task in conjunction with the political instability in the southern region. In the Asian countries where tourism industry such as Thailand was developed, cyber terrorism prevention is a prerequisite for sustained economic growth.

Also, in countries such as Indonesia and Malaysia where the rapid growth of mobile-based economies such as Grab, anti-terrorism ICT abuse has been recognized as an important security challenge. Particularly, since the activities of foreign jihad combatants and the recruitment of extremist organizations are being carried out mainly on social media such as Facebook, abuse cases and countermeasures for each media have been actively discussed[6].

4. Conclusion

The new type of security threat is not a single type, but the sum of a small variety of non-state actors who have relatively little influence from the traditional security perspective. In particular, the extreme terrorism based on religion has been pointed out as the most important security threat. The diversification of terrorist organization, which is characterized by new terrorism, and the worldwide spread of fear of terrorism due to informationization, developing active measures for counterterrorism is getting more and more difficult.

Terrorist threats that exploit information and communication technologies in the era of globalization are growing and expanding[7], so a more comprehensive approach to terrorism related to the Internet and information and communications technologies is required.

5. References

5.1. Journal articles

[1] Park BR. Terrorist Use of the Internet and Its Response in Korea. *International Journal of Terrorism and National Security*, 1(1), 1-4 (2016).

[7] Chung TJ & Rhee GM. The Study on IOT Security and International Crime Countermeasure Strategy. *Korean Journal of Police Science*, 19(5), 279-302 (2017).

5.2. Additional reference

[2] http://www.un.org/ (2018).

[3] https://www.un.org/ (2018).

[4] http://www.techagainstterrorism.org/ (2018).

[5] https://ict4peace.org/ (2018).

[6] https://www.un.org/ (2018).

Author

Park Bo-ra / Institute for National Security Strategy
Research Fellow

B.A. Dongguk University
M.A. Dongguk University
Ph.D. Dongguk University

Research field
- A Study on Extremism -Focused on the Psychology of Extremist Terrorists-, Review of Criminal Psychology, 14(1) (2018).
- Influencing Factors of Terrorist Attacks and Its Implication for Counterterrorism Policy, INSS Research Report, (2018).

Major career
- 2011~present. Korean Association of Terrorism Studies, Board Member
- 2018~present. Institute of National Security Strategy, Research Fellow