

211-0007

ISSN: 2423-8767

378 Tenjinchou Kamimaruko Nakaharaku

Kawasakishi Kangawhken Japan

# International journal of justice & law

2016 1(1)

## <Index>

1. Strengthening the Capacity of LAW Enforcement Agency in Line with the New Security Situation  
/ **Yoon Hae-sung**
2. Examination on the Digital Evidence and Hearsay RULE in Republic of KOREA  
/ **Kim Young-hyun**
3. CHINA's Economic Growth and the Role of Criminal JUSTICE Agency: A Comparison between Ministry of Public Security of the People's Republic of CHINA and the National Police Agency of KOREA  
/ **Kang Ho-gu, Wang Lin-lin, Jo Sung-gu**
4. Review on National Security Oriented JUDICIAL System of Republic of KOREA  
/ **Lee Hyun-jung**
5. The Study of Acceptability of Search and Confiscation for another Digital EVIDENCE  
/ **Park Woong-shin**

# J-INSTITUTE

Publication state: Japan  
ISSN: 2423-8767

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

Corresponding author  
E-mail: [sung9987@kic.re.kr](mailto:sung9987@kic.re.kr)

Peer reviewer  
E-mail: [editor@j-institute.jp](mailto:editor@j-institute.jp)

<http://dx.doi.org/10.22471/law.2016.1.1.01>

© 2016 J-INSTITUTE

## Strengthening the Capacity of LAW Enforcement Agency in Line with the New Security Situation

Yoon Hae-sung

*Korean Institute of Criminology, Seoul, Republic of Korea*

### Abstract

*The Korean Peninsula is one and only divided country around the world, which has been divided since the cold war system caused by ideological conflict. In this context, there have been ideological conflicts in our Korean society.*

*The North Korean spy cases or the unconstitutional dismissal of political party have been related to the national security issue up to now. Whenever such incidents break out, many issues heat up our society, including the existence and safety of our country, the meaning of democracy and the existence of people who are pro North Korea. However, such cases may not be seen from the prospect of ideological conflict, but from that of national law on how constitutional law and order will be established.*

*Assurance of national security is a precondition to protect people's safety, life, freedom and rights. The Constitutional law Article 1-2 states that a nation's sovereignty shall lie in people and all the rights of the nation shall come from people, which means the subject of a modern democracy and constitutional country. However, it is important that people herein means the whole people, and the interest of the entire nation takes precedence over that of an individual person. In this regard, the Constitutional law Article 37-2 states that all freedom and rights of the people may be limited by law in order to guarantee national security.*

*Unlike in the past, all the rights of an accused person or a criminal defendant are now guaranteed according to the Constitutional law and laws even for national security related cases, including the principle of legal process, the presumption of innocence and the principle of legality. Therefore, national security related cases such as a spy case, does not depend only on such a suspect's own confession or evidence like in the past custom of investigation. Under the current legal system, it will be difficult to give criminal punishment, unless they have clear evidence on a spy or terrorist.*

*The bottom line is that today's national security needs to be beyond the conventional concept, and be considered within a new paradigm where the concept of comprehensive security is focused across an individual and society. In order to ensure national security, it needs to be achieved based on each legal basis. The concept and scope of national security plans need to focus on the concept of comprehensive security, based on National Security Law, National Intelligence Service Act, spy and important counterespionage investigation, and important leftist investigation.*

**[Keywords]** Law Enforcement Agency, National Security, Comprehensive Security, Criminal Investigation, New Security Situation

## 1. Understanding of New Security

### 1.1. Concepts of the new security and the new security situation

Security refers to "total defensive means as all measures taken to guarantee and protect national security". The concept of security is used very comprehensively, as seen in the commonly used terms such as security

police, national security law, security criminal, security of communications and security censorship. Moreover, 'security police activity' refers to the activities of the police to protect national interest such as the national system, order, people and their properties, as a part of natural actions to maintain social wellbeing and public order. As such, Korea's security police does the activities based on conventional concept of national security[1].

In the new paradigm where comprehensive security is emphasized across an individual and society beyond the conventional national security concept, security police activities are now based on the police law, police officer's job enforcement law and other laws as well. As such, the concept and scope of security includes National Security Law, National Intelligence Service Act, spy and important counterespionage investigation, and important leftist investigation, which indicates the current trends of emphasis on comprehensive security.

Generally, 'security' refers to protecting oneself against threats or danger, without worry, fear and anxiety. The concept of security in the past cold war times, had been focused on national security concept, where such countermeasures were taken using military forces(war) or armed forces[2]. However, after 9.11, a comprehensive concept of security has emerged, which is defined as new security, adopting a very wide range of security concepts including not only the use of armed forces but also the removal of non-military weaknesses such as political democracy, economic market system, maintaining social community, maintaining stable environment for survival, and cyber terrorism[3][4].

In particular, the security related legal system has been rapidly changing as it becomes more intelligent, more globalized and more covert after 9.11. In this regard, the situation is that some cases cannot be solved with the past intelligence and investigation methods. Such a changed environment is new security situation that is not limited to the security concept of the past cold war era, because security is threatened in an international and radical environment. Developed countries also see the concept of security to be very

broad, exerting effort on complete national security by allowing their intelligence agencies to collect intelligence and information, which is because they think the past legal system cannot deal with the current new security situation. Therefore, as we know in the concept of security and safety, the concept of security is now also expanded in South Korea, along with the discussion and debate across the job scope of our security police. There is a need for capacity building of law enforcement agencies in South Korea as well, as other countries see the concept of new security to be very broad in line with the current situation around the world and are exerting efforts on complete national security by allowing their law enforcement agency to collect intelligence and information.

## **1.2. Strengthening the capacity of law enforcement agency**

The roles of intelligence agencies and investigation agencies are as follows.

First, there is need to strengthen their information collection and investigation activities to find out and arrest national security criminals as a part of activities to root out and arrest the national security offenders. Currently, the police is expanding the activities to find out and arrest security threatening people[2] by setting up and implementing '100 days investigation planning for security threatening criminals'[5], to take countermeasures against concerns of their infiltration into every area of our society to stir up social chaos. Second, in consideration of larger portion of security activities in cyber space, there are more rapid application of national security threatening activities using cyber space. Such national security threatening forces use the Internet space as a means of achieving socialism revolution, reinforcing the so-called cyber struggle. The reason why national security threatening forces are making a heated effort to struggle in cyber space is because the good cyber infrastructure of South Korea including the number of Internet users and ultra speed Internet subscribers is at a world class level. Third, the security activities need to be supplemented. The intelligence and investigation agencies need to

make the best possible effort on security activities and intelligence collection activities for initial response and prevention.

In this context, there is the need to strengthen the capacity of national security intelligence and investigation agencies[6]. As the recent international trends require strong legal system against terrorism, we need to consider adopting advanced legal systems according to such international trends and needs. If the security activities of national agencies are being strengthened all over the world, there is the need to reinforce our approach from the security aspects as well[7].

At this time, it is an important issue how far the principles of democracy and adequacy will be considered. Nevertheless, the concept of security is expanding recently in South Korea, while there are also growing interest in security issues internationally. In addition, given the rapidly changing legal system after 9.11, it is the proper time for South Korea to also seek an advanced legal system in line with global trends, from the prospects of strengthening the capacity of national security.

## **2. Criminal Policy Directions for Security Offenders**

### **2.1. Review of law with respect to the participation of attorney**

In Germany, the Criminal Procedure Code Article 112-3 states that security offender such as terrorist may be arrested even with no concerns of escape and no possibility of destruction of evidence. Further, with respect to meeting with an attorney, the participation of attorney is partially limited if it is a threat to national security. The Criminal Procedure Code Article 138-b states “If there is a specific fact determined that the participation of attorney(seine Mitwirkung) may cause a threat to the security of Germany, an attorney(einVerteidiger) may be excluded from the procedures”[8][9]. Indeed, it does not deprive ‘the accused of the rights to defend’, but this statement can exclude certain attorneys and their groups who protect security offenders.

If so, it is in question, if it is reasonable for a certain attorney group as in South Korea to defend an individual or a group who benefits the enemy. We need to see if it is reasonable to allow meeting with attorney up to 87 times, from the aspects of protecting fundamental rights, from the aspects of the principle of proportion, and from the aspects of legal interest. Any other country would not misuse fundamental rights for security offenders who destroy national security and constitutional law and order. In most of countries, national legal interest takes precedence over social and individual ones, and the approach of proactive prevention is made with very strong punishment, by defining any threat or infringement of a nation as the criminals based on the attempted crime or the abstract endangerment offenses category. If so, national security is significant from the aspects of legal interest as well. Therefore, it needs to be looked at on whether it is reasonable, in the principle of proportion, to protect the fundamental rights of the security offenders too generously and thoroughly, in spite of a major crime.

### **2.2. Implications of major countries with advanced security**

There are the following implications to review, from the characteristics of security related criminal legal system in developed countries with advanced security.

First, developed countries with advanced security such as the U.S. reflect their intent of proactive countermeasures in their laws, to no longer experience such a national crisis and to protect their national security[10]. That is, the premises are not changed that individual's personal information and privacy rights are important, however, there are trends in which national legal interest takes precedence over personal interest, and public interest over an individual's interest from the perspective of proactive prevention against any crime that threatens a nation such as terror, mass destruction and property damage. This has led to enactment and revision of laws for proactive prevention rather than reactive countermeasures, which further resulted in the expanded functions of

law enforcement agencies. For example, functions to monitor calls and e-mails and to see medical and financial records were drastically reinforced but also regulations on limiting investigation into espionage activities were largely alleviated. In particular, considering that they legalize wiretapping or monitoring with regard to security crime, there is a need for us to have a different approach in limiting privacy between security crime and non-security crime, taking into account the intent of enactment against security crime in other countries.

Second, with respect to security, major countries specify the basis that allows them to acquire personal records sensitive in secret espionage activities, thereby reinforcing the collection of information. In the US, intelligence or investigation agencies may request the court to provide law enforcement agencies with documents to be submitted by all individuals and groups such as information or evidence regardless of records or tangible goods. German law enforcement agency may be provided with any related information such as name, address or service history of a concerned person from a financial institution, postal business, air transport business and communications business, if it is necessary to perform duties in terms of national benefit and protection of the law and if there is any factual basis for serious danger. Furthermore, such law enforcement agency is allowed not to reveal or notify such information owner of the fact that such information was provided. For the necessity of the investigation, they need to only prove that 'that was for overseas intelligence investigation or for protection against international terrorism or for protection from a secret intelligence agency', or they need to prove the fact that such information collection was essential to accomplish a mission. The issue is that abnormal and unlimited rights should not be given to a law enforcement agency, with respect to excessive information collection. Therefore, even when such system is established, it should be accompanied by thorough judicial monitoring[11].

Third, major countries with advanced security have prepared special code and regulations of criminal procedures to strengthen the rights of a law enforcement agency such as expansion of the monitoring system, permission of secret search and extension of detention. The legal system methods and contents were different depending on countries, but they commonly focused on reinforced rights for monitoring activities and investigative function to prevent security threats in advance. It seems that criminal special procedures were derived from the judgment that human rights of the accused need to be limited to a certain degree as far as security investigation was concerned. With the development of science and technology and advanced techniques, any legal system set apart from technology and reality will limit and bind the functions of the law enforcement agency. Therefore, careful consideration needs to be given if there is a need to introduce special rules of criminal procedures, in the context of at least terrorism and investigation into security offenders as in other countries, before making any legal system to cope with major security crimes.

### **3. Shedding New Light on Criminal and Judicial System**

#### **3.1. Consideration of criminal special procedures law based on new security situation**

South Korea has gone through the pain of division, facing the environment close to security offenders. Even without such division, developed countries do not make any compromise with a terrorist against the threat of terrorism as they compromise with the broad principle in criminal law. The Anglo-American law leaders such as the U.S. and the Continental Law leader such as Germany have a strict criminal justice system against any forces threatening their national security, even though they are developed countries emphasizing the protection of human rights. Furthermore, major countries with advanced security specify special cases of criminal procedures that limits the basic human rights in the

constitution, reinforcing the rights of law enforcement agencies. This is to facilitate crime-evidencing in line with more advanced criminal techniques, taking the risk of limiting basic human rights by having a fair comparison of interests between the protection of basic human rights and public interest.

In other words, as criminal techniques are growing more and more advanced, intelligent and international, only when the criminal evidence laws or related policies is supported, the national security and people's safety can be protected from a preventative aspect. In South Korea, its security related criminal legal system has not changed much from the past, even when it faces a new security situation, threatened by international terrorism as the criminal techniques are growing more advanced. Moreover, because there is a strict standard of observing constitutional due process, unless there is evidence laws and special cases in the criminal procedures law as in developed countries with advanced security, admissibility of evidence is denied even during the trial stage after arresting a terrorist or spy through intelligence or investigation. This can lead to discouraged investigation activities by the law enforcement agencies.

### **3.2. Consideration of principle of proportionality**

Technically and scientifically developing terrorism and criminal techniques of security offenders cannot be actively dealt with under the current South Korean security related criminal law system. Countries with advanced security approach in public interest rather than respect for fundamental rights of international terrorists similar to security offenders, giving strong punishment without any paternalism. Compared to that, there is paternalism rather than actual penalty for security offenders by the Korean judiciary branch, weakening the rights of intelligence and investigation agencies. It does not meet the principle of proportion under such a new security situation, that national security offenders go through the same criminal procedures with common criminals, because looking back at the reality of our security, the act of benefiting the enemy and espionage, and national

interest infringement are often treated as the same between common criminals and security offenders. This is not desirable from the principle of proportion. Under the current new security situation, it is contradictory that such investigation environment has not been improved but going backward.

In many developed countries with advanced security, they have prepared the related legal system by viewing security crime(terrorism) that may cause major crisis to a nation differently from general crimes and justifying this, based on balancing conflicting interests and the principle of proportion, even when it may be major infringement to constitutional fundamental rights. From that, there is need for us to review if there is a need to strictly respond as far as security crimes are concerned, by reflecting the intent of proper or additional punishment, still observing the principle of proportion[12].

## **4. Conclusion: Security Situation of South Korea**

From the aspects of proactive protection of national legal interest, the purposefulness of punishment against an act is different from personal and social legal interest. Because an individual cannot exist without a nation, and their fundamental rights such as economy, welfare, and happiness are satisfied within the frame of a nation, national security is just as important. Because a nation exists, we are here, and the nation exists to protect us.

Considering that our criminal law specifies rebellion and Landesverrat within the system of the existence and wellbeing of a nation, the benefit and protection of the law of a nation takes precedence over any other issue. It is a fact that even major countries with advanced security have reinforced their related laws by introducing criminal special cases and procedures, in line with this context and in response to the reality of their security.

Although advanced countries make an effort for the proactive prevention of terrorism through intelligence collection and analysis, South Korea, despite having two threats: international terrorism and divided country in



a cease fire, neglects such efforts just because there is no immediate, visible threat.

Furthermore, as seen in the security incidents such as the so-called Ilsimhwae, Wangjaesan, and underground revolutionary organization(RO), the judiciary branch had judged even major crime that infringes upon national interest and destroys the constitutional law and order on the basis of the same standards as common crime. This constantly requires special rules of criminal procedures against national security offenders. Therefore, there is need for a new approach while breaking away from the existing old-fashioned investigation environment, modeling the foreign terrorism related laws based on the concept of new security. In order to do this, at least the legal system with respect to the national security offenders need to be shed with new light and improved to be in line with the new security situation.

## 5. References

### 5.1. Journal articles

- [2] Lee MJ. Security Threat from North Korea and the Role of Police. *Korean Police Studies Review*, 10(2), 149-176 (2011).
- [8] Seong B. Review on Improvement Plans of the Criminal Procedure Law Based on the Judicial Precedent Analysis about National Security Case. *New Trends of Criminal Law*, 46, 243-279 (2015).

### 5.2. Books

- [1] Choi ER & Cho BI & Lee HW. Introduction to Police Science. Korean Institute of Criminology (2012).
- [4] Choi JC. Capacity Building Method of South Korea's National Defence Diplomacy Security Research Series. Security Institute of Korea National Defense University (2007).
- [10] Kim IS. What Love Means in Criminal Law and Order. Sechang (2013).
- [11] Vincent EH. Developing Local Law Enforcement's Strategic Capacity to Combat Terrorism in the United States. Prentice Hall (2005).

### 5.3. Conference Proceedings

- [3] Yoo DR. Current Issues and Countermeasures of North Korea's Cyber Threat Against South Korea. Conference Materials of the Institute for National Security Strategy (2014).
- [6] Lim YS. Debate Text Examination of Security Criminal Law System. Grand Debate to Improve South Korea's Security Criminal Law System (2015).
- [7] Kim SG. Debate Text Diagnosis and Countermeasures on Security Criminal Law System. Debate on Security Criminal Law (2015).
- [12] Yoon HS. Examination of Security Criminal Law System. Grand Debate to Improve South Korea's Security Criminal Law System (2015).

### 5.4. Additional references

- [5] <http://www.police.go.kr/> (2016).
- [9] <http://www.law.go.kr/> (2016).

#### Author

**Yoon Hae-sung** / Korean Institute of Criminology Researcher

B.A. Seowon University

M.A. Sungkyunkwan University

Ph.D. Sungkyunkwan University

#### Research field

- The Current Trends of Voice Phishing Fraud, Korean Association of Criminology, 25(2) (2013).
- A Review on National Security Criminal Justice of Republic of Korea in the New Security Situation, Korean Police Studies Review, 14(2) (2016).

#### Major career

- 2014~2015. Yonjin University, Lecturer
- 2016~present. International Society for Justice & Law, Vice President

Publication state: Japan  
ISSN: 2423-8767

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

Corresponding author  
E-mail: [kasfa0415@hanmail.net](mailto:kasfa0415@hanmail.net)

Peer reviewer  
E-mail: [editor@j-institute.jp](mailto:editor@j-institute.jp)

<http://dx.doi.org/10.22471/law.2016.1.1.07>

© 2016 J-INSTITUTE

## Examination on the Digital Evidence and Hearsay RULE in Republic of KOREA

Kim Young-hyun

*Kimpo University, Kimpo, Republic of Korea*

### Abstract

*Korea is ranked a top country in the aspect of digital technologies, device production and distribution. However, the decisive digital evidence achieved by observing proper legal procedure based on the warrant issued by the Ministry of Justice loses its admissibility in the process of the trial upon the refusal from the accused.*

*Here, most defendants do not admit the admissibility as the party with the opposition to the government during the criminal trial on the digital evidence which plays a decisive role in forming the confident belief of the judge while having direct and indirect relations to proving criminal charges, requiring serious discussions.*

*The object sincerity of the data shall be proven for the digital evidence to be proven with the admissibility in the criminal trial. The proof on the sincerity is about the legal procedure law like the proof on the voluntariness and enough by the free proof from the judge.*

*There are issues judged by free proof with various methods from the judge including whether the HDD is confiscated by the defendant, whether to verify hashes in all the HDDs despite taking a long period of time, whether to sample mobile memories or some HDDs with low capacity and follow the testimony of the investigators or witnesses, whether to verify with the write protection device for the original copy and whether to write the image for the verification with a copy in the legal procedure.*

*In addition, the data identity among media shall be accepted and in the verification process, the mechanical accuracy of the computer, program reliability, professional skills and accuracy of the operator for input, process and output shall be secured.*

*In short, the electronic document with the statement of the defendant may be taken as evidence if the sincerity of the document is proven and the statement is especially provided under the reliability even though the defendant denies the sincerity regarding the hearsay rule of the digital evidence.*

*This means the circumstantial security of the reliability on the evidence and the prosecutor shall specifically claim and prove the existence but the free proof is enough for the fact in the legal procedure.*

*In addition, the admissibility may be provided by a relevant clause if the electronic document saved to the computer, Internet and SNS posts and e-mail are included in the exemption of the hearsay rule in the Criminal Procedure Act as the hearsay evidence.*

**[Keywords]** Hearsay Rule, Digital Information, Digital Evidence, Admissibility, Hearsay Evidence

### 1. Introduction

Today, the digital information application in the digital information era raises the possibility for finding the truth and expanding the evidence collection in various criminal trials

and contributes to rapid and effective evidence collection. However, there exists the possibility for the information distortion and deformation due to the digital evidence variation and improper control of this would collapse the ideology of the criminal procedure act based on finding facts and taking legal



procedure. This is why there shall be focus on especially the identity or integrity of the digital evidence even though there are a lot of legal disputes to be reviewed by the features of the digital evidence.

The legal procedure relevant to the value of the criminal trial, realistic fact-finding and rapid and efficient procedure are still effective in the digital information era. However, there remains the task on how to implement such principles depending on the feature of the digital evidence and the digital evidence has close ties with the legal and technical affairs, requiring the cooperation between the two entities.

A series of recent accidents regarding the national security show that the digital evidence is fully under the hearsay rule based on the general criminal evidence act, there is a need to investigate exceptional regulations to apply the hearsay rule on material legal right infringement at the national level. In addition, material crimes in the digital information era are professionally and covertly performed and this is why the legislation properly reflecting the situation and environment the current digital information is required for the criminal evidence act. Furthermore, there are frequent cases in which the important evidence for the criminal proof disappears by formally applying the hearsay rule on the general criminal evidence act on even digital information. Therefore, it ought to fully consider and reasonably interpret the crimes which exploit the environment and special feature of the digital evidence and information.

## **2. Theoretical Discussion About the Hearsay Rule on The Digital Evidence**

### **2.1. Concept of digital evidence**

The electronic evidence is the term for the electronic information or record from the viewpoint of the evidence act. This shows that the electronic evidence is formed when the evidence becomes electronic information (electronic method or electric or magnetic storage or transmission). The term, 'special media' like electronic record, has

been used in Article 336 of the Criminal Act, etc. Here, 'special media' like electronic record, means the record stored by electronic or magnetic method to certain storage media[1] and may not be read or checked through additional display or output device because the media itself does not have objective substance. In addition, opinions or behaviors of a lot of people may be engaged in the production process and additional data are automatically combined with the existing information by programs to create a new electronic record. In the process, it is not independently used with the objective and fixed meaning. Rather, it is established by the individual or company to generate, process and output the information through electronic method, and is used in the system for operation and installation to perform anticipated proving functions[2]. The established rule of the Supreme Prosecutors' Office, 'Regulation on the Collecting and Analyzing the Digital Evidence' defines digital evidence as the information valuable as evidence saved or transmitted through digital method.

Ultimately, it means that the digital evidence defines the digital information in the digital device from the viewpoint of the evidence act and may be simply defined as the information valuable as evidence transmitted or saved through digital method. Likewise, it becomes a useful legal concept that can be independently discussed apart from the development in various media, information contents and existence of the producer following the development in science and technology[3].

### **2.2. Feature of digital evidence**

#### **2.2.1. Non-readability and invisibility**

Human perception may not recognize the existence or contents of the digital information. Therefore, to investigate the digital evidence in court, an action shall be taken on the digital media to convert the media to analog information that is suitable to be perceived by a human being[4]. It means that the digital data may play a role as visible evidence only after the conversion process as potential evidence. The analog evidence, for example,

a document, requires the proposal and reading for the evidence investigation but the digital evidence requires further process of turning the evidence into analog form prior to the proposal and reading. Of course, the process of turning the evidence into analog is not generally performed in the court. Rather, it is performed outside the court and requires the conversion for visibility by experts because it may not be directly recognized or deciphered by normal people[5].

### **2.2.2. Importance of original copy**

Humans may only see the digital device which stores or transmits the information because the digital information is not visible, and it is important which original information is stored or transmitted. In addition, the digital device is sophisticated and sensitive, requires the manipulation by experts but is much more vulnerable to intentional deletion or falsification by malicious experts than analog evidence[6]. It means that it is much easier to falsify, forge and delete the digital evidence but difficult to prove this fact, posing the issue whether the digital evidence submitted to the court was falsified or adhered to the proper procedure for evidence acquisition.

### **2.2.3. Replicability of information**

The digital evidence holds the mutual independence from the digital media, contains the same contents regardless of the media type and repeats the same form anytime and anywhere. It means that the digital evidence does not show quality degradation in the repeated copy process only if the value is the same unlike analog data[7]. Regarding digital evidence, it is not easy to distinguish the original from the copied version. Therefore, a decision has to be made on how the best evidence rule on the digital evidence is applied and at which level the admissibility and proof of the copied version instead of the original version are accepted[4].

### **2.2.4. Massiveness of information**

The development in the storage technology of digital information led to store massive amount of the digital information to a very

small storage device. The smartphone most people use today can store massive amount of digital information. Therefore, it may be difficult to confiscate and search for the data related to the crime among massive digital data to investigate a crime and cause various issues like the matter of applying the rule of exclusion on illegally collecting evidence[8].

In particular, considering that the comprehensive warrant is prohibited based on the warrant requirement rule, the digital information collected by exceeding the warrant range may be recognized as the collection without following the proper procedure and its admissibility may be denied.

### **2.2.5. Network connectivity**

The digital environment holds not only the standalone environment where each device or equipment works independently but also the network in which devices are connected to each other. Therefore, there may be cases which access the system resources through transnational network to collect valuable digital data for evidence[9]. This causes the jurisdiction or sovereignty issues, as well as coverage regarding the collection of the digital evidence[4]. Such digital evidence is characterized by the possibility to be transmitted through the Internet and other networks. In addition, there are more cases where the digital evidence is stored to a server managed by a third party through the network as Internet and cloud services are burgeoning. As a result, the issues like the place of search and seizure, land jurisdiction and even worse, limitation in law enforcement in the country [8].

## **3. Discussion on the Digital Evidence and Hearsay Rule**

### **3.1. Meaning of hearsay rule**

The digital evidence includes the entity produced by the mechanical process without human thought or process of statement, and the entity generated and processed by entering the data of the details a person is trying to express by a human-written program. The former becomes the non-statement evidence

and the latter becomes the statement evidence. The former has no room for applying the hearsay rule. The hearsay rule applies to the latter if the sincerity of the contents is factum probandum but does not apply in the case if the existence itself becomes the evidence. The Supreme Court follows the same legal principles.

### 3.2. Requirement for hearsay rule

There is no Korean case which specifically judges the requirement for the hearsay rule like the *Lorraine v. Markel American Ins. Co.* ruling in the US but the ruling of 2006 do 2556 of the Supreme Court in November 13, 2008 provides an implication. Basically, the Supreme Court precedent suggests that in case of using the digital evidence as the statement of evidence, since the hearsay rule applies to the sincerity of the contents, it can be used as evidence[10] only when it has exceptional requirement(in particular, Article 313.1).

## 4. Discussion on Hearsay Rule

Conceptual elements of the hearsay evidence are as follows: First, it shall be statement by the human(including the activities of statement); second, it shall state the fact of experience; third, the proof intention is to prove that the statement is true; fourth, it requires the statement outside the court[11]. It means that the hearsay evidence shall be understood by the relation with the factum probandum even though the hearsay evidence is the digital evidence containing the human statement. It is the same for the electronic document or web document where the digital evidence is in the computer or audio or video file which records the audio and video as electronic data. It matters "Whether there was such a statement" not "Whether the statement is true" from the conceptual element of the hearsay evidence for the text message or file which has recorded the black-mailing, meaning that the hearsay rule may not be applied to that particular digital evidence[12].

Normally, the contents without the process of human recognition, memory, expres-

sion and description and only with the mechanical processing are not included in the hearsay evidence because no subjective human statement is involved. For example, a computer log, Internet web history and entry status electronically recorded by the electronic entry system are only evidence not hearsay evidence. The digital evidence which contains the human statement is not included in the hearsay evidence if the statement is the intention expression or instruction rather than the statement of fact of experience. For example, the legal expression like the contract request or acceptance or the de factor expression like the case request by the public official or the instruction of crime are not included in the hearsay evidence[11].

In short, the digital evidence shall meet the prerequisite like the originality, identity with the original and integrity to receive the admissibility and exceptions in the hearsay rule mentioned below to the range where the hearsay rule is applied[8].

## 5. References

### 5.1. Journal articles

- [5] Kim BS. Digital Evidence and Forensic. *Information Telecommunication and Broadcasting Policies*, 21(6), 55-76 (2009).
- [6] Kwon OG. Concept Feature and Requirement for the Admissibility of the Digital Evidence. *IT and Legal Research*, 5, 291-318 (2011).
- [8] Kim YS & Park SY. Admissibility of the Digital Evidence in the Criminal Evidence Act: Focusing on the Prerequisite for the Admissibility and Exceptions in the Hearsay Rule. *Criminal Policy Research*, 26(2), 165-214 (2015).
- [9] Cho SS. Plan on Securing the Integrity to Upgrade the Legal Status of the Digital Evidence. *New Trend in the Criminal Act*, 27, 64-109 (2010).
- [11] Lee YG. Problem in the Hearsay Evidence and Sincerity of the Statement Under Threat. *Justice*, 139, 372-401 (2013).

### 5.2. Books

- [3] Son JY & Kim JS. Research on Judging the Admissibility of the Digital Evidence Research Series of the Judicial Policy Research Institute. Supreme Court (2015).
- [4] Park HS. Admissibility of the Digital Evidence in the Revised Criminal Procedural Act Paper for Overseas Training Prosecutor. Ministry of Justice (2009).
- [7] Tak HS & Lee SJ. Evidence Collection Procedure and Plan on Securing the Admissibility by the Digital Evidence Analysis Tool. Korean Institute of Criminology (2006).

### 5.3. Additional references

- [1] Supreme Court. Judgment 2000 do 4993 (2003).
- [2] Supreme Court. Judgment 2004 do 6132 (2005).
- [10] Supreme Court. Judgment 2007 do 7257 (2007).
- [12] Supreme Court. Judgment 2006 do 2556 (2008).

#### Author

**Kim Young-hyun** / Kimpo University Professor  
 B.A. Kyungwoon University  
 M.A. Yongin University  
 Ph.D. Yongin University

#### Research field

- A Comparative Study on the National Cyber Counter Terrorism Activity, Korean Terrorism Studies Review, 7(4) (2013).
- The Structural Relationships between Organizational Ethical, Job Satisfaction and Organizational Citizenship Behavior of Private Security Guards, Korean Security Science Review, 42 (2015).

#### Major career

- 2013. Myungji University, Lecturer
- 2016~present. International Society for Justice & Law, Member

Publication state: Japan  
ISSN: 2423-8767

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

Corresponding author  
E-mail: [linerwang@sina.cn](mailto:linerwang@sina.cn)

Peer reviewer  
E-mail: [editor@j-institute.jp](mailto:editor@j-institute.jp)

<http://dx.doi.org/10.22471/law.2016.1.1.12>

© 2016 J-INSTITUTE

## CHINA's Economic Growth and the Role of Criminal JUSTICE Agency: A Comparison between Ministry of Public Security of the People's Republic of CHINA and the National Police Agency of KOREA

Kang Ho-gu<sup>1</sup>

*Peking University, Peking, China*

Wang Lin-lin<sup>2\*</sup>

*Shanghai University, Shanghai, China*

Jo Sung-gu<sup>3</sup>

*Kyungwoon University, Gumi, Republic of Korea*

### Abstract

While China achieved the fastest economic growth in the world since it actively adopted market economy after its economic reform, it also saw increase in various crimes. There is very little research done on the Ministry of public security of the people's republic of China, but based on the previous research, the types of crimes can be summed up as following.

Firstly, the crimes in China are becoming organized and are becoming a commercialized profession.

Secondly, the Chinese crime organizations are covertly managing their fund circulations through 3rd party bank accounts and virtual accounts on the internet.

Thirdly, every time a new type of industry emerges, a new type of crime exploiting the industry grows rapidly.

Meanwhile, under the Chinese planned economy, the MPS had a major role on many components of social life in China. For example, the relationship among the MPS, the prosecutors and the court clearly shows that the MPS is relatively higher in status, and its authority is encroaching the Ministry of Civil Affairs of the People's republic of China, China administration of Taxation, and China Administration of Industry and Commerce, and is in need for a change through a reform.

Meanwhile, after achieving a rapid economic growth since the 1960's(83.1%), South Korea ranked first in human rights protection and international policing cooperation in the "Crime Index for Country 2015 Mid-Year".

The authority of China's MPS is a part of national administrative authority, which comes from the people. Therefore, one must consider whence the authority exercised by the MPS derives. Here are some problems of MPS identified in this research.

Firstly, the Chinese MPS is inefficient in tasks that utilizes human resources within the jurisdiction.

Secondly, it is difficult to communicate the information related to crimes collected by the MPS efficiently.

Thirdly, the MPS has limited ability in cutting the criminal funds.

Fourthly, the MPS fails to fully cooperate in criminal investigations.

Fifthly, MPS demonstrates an incomplete cooperation in Crime prevention tasks.

Therefore, to keep up with the rapidly grown economy, various discussions on the role of MPS and an international cooperation on the safety of people will become necessary.

**[Keywords]** Criminal Law, Economic Growth, Ministry of Public Security of the People's Republic of China, Korean Police, People's Safety

## 1. Preface

After China went through the economic reform between 1949 and 1978, a change in crime rates and types came along with rapid economic development.

During the early days of Chinese market economy, uncomplicated crimes like contract fraud, low-quality goods and counterfeit occurred in the goods distribution sector. But as the recent reform policy is causing shifts in

social components, the MPS is facing difficulties due to increased crime rate. MPS does have a task processing system in place, but the diverse regional uniqueness is causing difficulties in efficient task processing.

On the other hand, South Korea maintained a closed economy based on agriculture from the end of the Korean war all the way up to 1960 with \$121 of GDP per capita, but it expanded the market size through transitioning from light industry to heavy chemical industry in the 1970s, and privatized the market economy by deregulations in 1980s. As a consequence, South Korea became a member of the OECD, and became a strong economy ranked as the 11th highest in GDP.

In the process, in order to proactively respond to terrorism and other international

crimes, the South Korean police proceeded to cooperate with 71 international policing agencies to arrest international fugitives. Moreover, in 2016, the South Korean police established cooperation with 50 additional foreign police agencies.

Therefore, in this research, the direction of growth of the MPS following China's rapid economic growth will be discussed in comparison to the South Korean police, along with some suggestions on its future.

## 2. Preceding Research

The preceding research conducted in China and Korea on the same topic is organized in <Table 1>.

**Table 1.** Preceding researches.

Division	Researcher	Contents
Economic development of China and the role of Public security	Mei (2001)	Analyses the change in the role and the status of public security in accordance with the changes from the planned economy system to the socialistic market economic system of China from various angles[1].
	Liu (2004)	Claims the necessity of the scientific management and standardization in the various areas of the constitution of organization, the management of internal affairs, and education and training along with the discussion about and adaptation to the development and changes in the market economy in order to keep the social and political stability of China[2].
	Li (2007)	Presents the coping plan for the changes in the various areas of intelligent crimes, crime spaces with the rapid development of scientific technology and economic growth and categorizes the changes in the in-depth and systematic way[3].
	Li , Li (2014)	Discourses on the need of the China's public security work to contribute to the development of the domestic economy and summarizes the activities of the public security in the five focuses with the analysis on the related cases between the activities of the public security all over China and the economic development[4].
	Jin (2015)	Specifically analyzes the crime trend in the various areas in China based on the recent numeric data of China with a understanding of its features and factors and discusses the criminal law policy and the role of the police regarding this[5].
Economic development of Korea and the role of Police	Lee (2013)	Provides the future directions of the tourist police with the increased role in accordance with the increased tourists by via of the economic growth of Korea and Korean wave[6].
	Kim (2013)	Claims the necessity of the legislation regarding the expanded role of the police and enforcement of the police law in accordance with the economic growth of Korea and the changes in the social environment caused by the increased aged population[7].



	Yang (2014)	The necessity of introducing the local autonomy and the autonomous police system in accordance with the economic growth of Korea is being discussed. He claims that the autonomous police system adequate for the circumstances in Korea should be introduced[8].
	Shin (2014)	Suggests that the work boundary of Jeju autonomous police should be expanded in accordance with the economic growth of Korea and increased tourists, making the best of the tourist region[9].
	Hong (2015)	Asserts the need for cooperation with the agencies for intelligence and investigation and the detailed management of security in the private sectors in order to support the Korean police for preventing the leakage of the Korean industrial technology information, which is a driving force of the economic growth of Korea against the economic espionage[10].

### 3. China's Economic Growth and the Role of MPS

#### 3.1. China's economic growth

China's GDP recorded 10.4 trillion dollars and was ranked 2nd worldwide after the United States. The Chinese economic growth can be divided into three stages.

The first stage is the socialist planned economic stage that lasted from the foundation up until 1978's reform, which lacked the drive for the economic development due to the strict systemic frameworks of state-owned economy and collective economy and excessive interference from the state.

The second stage is the period of time between the 1978 reform and its membership in WTO, when China focused on developing the eastern coast. The reform comprises of external openness and internal reform, specifically on the economic system. From the economic perspective, the radical planned economy was reformed into a socialist market economy. Moreover, more political emphasis was given to democracy, and the legal framework was constructed to establish social stability and solidarity. Also, by opening its economy to the outside, the foreign trades largely contributed to the economic growth by supplementing resources, technologies and educated workforce that were lacking.

The last stage comes after the WTO membership up to this day, China is maintaining its

rapid growth, while establishing strategies to promote balanced development through projects like "the great west development," "Rise of Central China" and "the strategy of rejuvenating the old northeastern industrial base of China." China is maintaining rapid growth rate even through the developed countries' crises like the 2008 subprime mortgage crisis and the European debt crisis, and is serving as the engine of global economic growth.

#### 3.2. Types of crime in China and trends of their increase

Based on the criminal drafting statistics from the MPS and prosecuting agency, the agency throughout the country arrested 879,615 criminal offenders, with a large proportion of cases being terrorist violence, extreme personal violence, theft, fraud, food and drug-related crimes and cybercrime.

Especially, in 2014, total 400 thousand case of voice phishing occurred, which is a 30% increase from the same period in 2013, and the losses surmounted to 10.7 billion yuan. The voice phishing organizations are increasingly collectivized and specialized, with some of their bases located outside the country. Also, the fast distribution and development of internet is resulting in increased property infringement crimes such as cyber fraud. The occurrence and arrest record of crimes in China is summarized in <Table 2>.

**Table 2.** The occurrences of crimes and arrest in China.

	2005	2006	2007	2008	2009	2010
Occurrence	6,300,772	6,153,699	7,649,785	8,772,299	11,752,475	12,757,660
Arrest	4,648,401	4,653,265	4,807,517	4,884,960	5,579,915	5,969,892

The number of such crimes have been steadily increasing, and by 2014, reached 1.93 million cases, causing economic loss of 762.7 billion yuan, an increase of 54.8% from 2013. The characteristics of crimes following China's economic growth can be identified as following.

## 4. Korea's Economic Growth and the Role of Police

### 4.1. Korea's economic growth

The foundation for the Korean economic growth was established by President Park

Chung-Hee with his 1st 5-years economic development plan, and saw developments in HCI in the seventies and the eighties.

Afterwards, shipbuilding, cars, steel and construction companies began to grow under the government's oversight and in 1990, the semiconductor technology saw a great development and paved the groundwork for Korea to emerge as an IT giant. Nowadays, many technology-intensive industries emerged as a result, and Korea is ranked among the top in shipbuilding and semiconductor.

### 4.2. Korea's security environment

The occurrences of crime and arrests as reported by the Korea's national police agency is summarized in <Table 3>.

**Table 3.** Occurrences of crime and arrests in Korea[6].

	2005	2006	2007	2008	2009	2010
Occurrences	1,733,122	1,719,075	1,836,496	2,063,737	2,020,209	1,784,953
Arrests	1,512,247	1,483,011	1,615,093	1,812,379	1,811,917	1,514,098

The "Act on the Performance of Duties by Police officers" outlines that the police is performing protection of a citizen's life, body and properties, prevention and investigations of crime, subjugation of criminals, escorting key personnel, anti-espionage and anti-terrorism, collection and distribution of security

information, traffic control, international co-operation and other duties related to the public well-being and the maintenance of order[11]. As described, the police in Korea has its role throughout the society to ensure the citizens' safety and to establish a legal order. The status of human resources in the Korean police is shown in <Table 4>.

**Table 4.** Status of human resources in the Korean police.

Year	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
No. of personnel	95,336	95,613	96,324	97,732	99,554	101,108	101,239	102,386	105,357	109,364

As shown above in <Table 4>, after its economic growth, Korea entered a stable period and is increasing the number of personnel in the police steadily. As of now, each police officer is responsible for 456 citizens.

Meanwhile, according to an online statistics website called NUMBEO, the Crime Index for Country 2015 Mid-Year reported that only three countries – Korea(83.1%), Singapore(82.9%) and Qatar(80%) scored above

80%, and among the Asian nations, Japan(79.1%), Taiwan(78.7%) and Hong Kong(78.1%) followed in 4th, 5th and 6th places respectively. In contrast, Venezuela(14.8%) scored the lowest, with Honduras(19.3%) and Papua New Guinea(21.6%) closely followed. North Korea was excluded from this index[12].

## 5. Discussions

The high rates of economic crimes in China can have a negative impact on the Chinese government's economic reforms and the Chinese economy's long term development. As economic crimes are increasing both quantitatively and qualitatively, the problems that MPS faces in its duties is can be identified as following.

First, the MSP human resource utilization is inefficient. Nowadays, economic criminal offenders are scattered across throughout the country, but the MSP only deals with local criminal offenders within the jurisdiction. It seems apparent, then, that a close cooperation with the public security agencies in different regions underlies the solution to the criminal matters. Also, due to the rapid increase in economic crime, there is an insufficiency of human resources in the MPS to respond to a large-scale economic crime committed against the general public.

The second problem is that it is difficult to efficiently share the crime-related information collected by the MPS. It is difficult to separate the jurisdiction in case of an economic crime against the general public, and so sharing crime-related information among the MSP agencies in different regions. However, the exchange of information is not being done in a timely manner, and the personnel are being assigned redundantly, leading to a loss of manpower.

The third problem is that the MSP has very limited ability to cut the flow of funds. Under the oversight of MSP, each sub-agency is constructing an information system related to the investigation of the flow of funds and blocks. However, due to the differences between the departments, there is no real-time

management of the information on the flow of funds.

The fourth issue is that there is an incomplete system of cooperation between the regional branches of the public security agency, and so they are independently investigating each issue without being able to share the resources such as human resources and information. Also, due to the high mobility of economic crimes, crimes are spreading quickly into different regions, while the MSP seems to be unable to effectively suppress multiple outbreaks of crime at a national level. Additionally, the disparity in the economic growth also leads to visible difference in performance of local public security agencies.

Lastly, there is a lack of cooperation between the public security and other administrative departments. The economic criminals often approach the public as a company or as some other venture investor. Especially, administrative department is most familiar with laws and regulations concerning economic management and know the illegal economic activities best, but have very limited cooperation with the MPS. The public security agency can acquire quick understanding and the flow of the incidents, so it is crucial to cooperate with departments related to industry and commerce, tax and finance.

## 6. References

### 6.1. Journal articles

- [1] Mei JM. Social Contract Theory Market Economy and the Role of Police. *Journal of Shandong Public Security College*, 2, 40-43 (2001).
- [2] Liu JS. Strengthening the Regularized Management of the Public Security Staff to Adapt to the Demands of the Development of Market Economy. *Journal of Hubei Police Officer College*, 5, 54-57 (2004).
- [3] Li XH. Scientific Culture and Trend of Intelligence Crime. *Journal of Jiangsu Police Officer College*, 22(4), 5-10 (2007).
- [4] Li JM & Li JQ. Police Works Serves Economic Development. *Journal of Liaoning Police Academy*, 2, 30-34 (2014).

- [5] Jin GF. Crimes in China: An Analysis of the Situations in 2014 and the Trends of Development in 2015. *Journal of Chinese People's Public Security University Social Science Edition*, 2, 1-8 (2015).
- [6] Lee YN. A Study on the Developmental Strategy of the Korean Tourism Police System. *Korean Police Studies Review*, 12(4), 311-334 (2013).
- [7] Kim WJ. A Review on the Police Enforcement Concerning the Safety of the Old in Korea. *European Constitution*, 13, 321-346 (2013).
- [8] Yang JY. A Study on the Operational Strategies of the Korean Municipal Police System. *Korea Municipal Police Studies Review*, 7(1), 63-92 (2014).
- [9] Shin HK. A Historical Overview on Jeju Municipal Police. *Korea Municipal Police Studies Review*, 7(1), 3-34 (2014).
- [10] Hong SS. A Study on the Police Policy to Counter Industrial Espionage. *The Police Science Journal*, 10(3), 65-93 (2015).

## 6.2. Additional references

- [11] [www.law.go.kr/](http://www.law.go.kr/) (2016).
- [12] [www.numbeo.com/](http://www.numbeo.com/) (2015).

### Lead Author

**Kang Ho-gu** / Peking University Ph.D.

B.A. Soongsil University

M.A. Peking University

Ph.D. Peking University

#### Research field

- 韩国在华 OFDI 对母国劳动生产率的影响因素分析, 现代管理科学, 10 (2016).
- OFDI 产业结构效应中的产业空心化浅析——以美国、日本为例, 现代管理科学, 11 (2016).

#### Major career

- 2012~2016. The Chinese Government Scholarship, Full Scholarship
- 2016~present. International Society for Crisis & Safety, Editor in Administrator

### Corresponding Author

**Wang Lin-lin** / Shanghai University Lecturer

B.A. Zhengzhou University

M.A. China University

Ph.D. China University

#### Research field

- 多元刑事司法模式共存语境中的量刑基准研究, 政法论坛, 3 (2016).
- “被害人谅解”情节在量刑中的规范化适用, 人民司法, 16 (2016).

#### Major career

- 2014~2016. Institute of Law of Chinese Academy of Social Sciences, Postdoctoral Research
- 2015~present. The Tenth Youth Forum of China Law Society, First Prize

### Co-Author

**Jo Sung-gu** / Kyungwoon University Assistant Professor

B.A. Kyungwoon University

M.A. Kyungwoon University

Ph.D. Kyonggi University

#### Research field

- Participation Types of Private Security Guards in Leisure Activities and the Effect of Leisure Constraint on Life Quality, Journal of The Society of Disaster Information, 7(2) (2011).
- Development of Chinese Security Service and Its Assignments, Journal of Korean Public Police and Security Studies, 7(4) (2011).

#### Major career

- 2006~2009. Republic of Korea National Assembly, Secretary
- 2010~2014. Korean Association for Public Security Administration, Secretary General

Publication state: Japan  
ISSN: 2423-8767

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

Corresponding author  
E-mail: [d61326@gdsu.dongseo.ac.kr](mailto:d61326@gdsu.dongseo.ac.kr)

Peer reviewer  
E-mail: [editor@j-institute.jp](mailto:editor@j-institute.jp)

<http://dx.doi.org/10.22471/law.2016.1.1.18>

© 2016 J-INSTITUTE

## Review on National Security Oriented JUDICIAL System of Republic of KOREA

Lee Hyun-jung

*Dongseo University, Busan, Republic of Korea*

### Abstract

*According to this comment, the argument that the investigation method of the national security authority need to be changed can gain persuasive momentum. For the national security investigation to be effective, legal. Systemic devices shall be systemized to fit the recent situation. To put it more concretely, it is necessary to amend the Protection of Communications Secrets Act to enable legitimate execution of monitoring warrant etc. according to the development of digital technologies in the course of investigation by the investigation authority in national security cases, and to approach with the special provisions on criminal procedure for national security offenders. For example, as the technologies and IT industry developed drastically, the approach to the act to serve the interest of the enemy needs to be diversified. In other words, based on current law system, even though the act to serve the interest of the enemy and behavior of communication with spies(information delivery, instruction, recruiting personnel, education, publicity, etc) using SNS etc. , the proofs obtained in the course of investigation are incapacitated, as national security investigation is impossible due to the problems such as the declared policy of non-acceptance of monitoring warrant on Kakao Talk messenger and non-acknowledgement on statements of evidence on national security offender etc. Accordingly, in consideration of domestic situation where telephone communications within the territory or with foreign territory are to be monitored for the purpose of national security but cannot be submitted to the court as proof, it is necessary to progressively embark on special legislation in consideration of the special characteristics of spy investigation by systemizing mobile phone monitoring or restriction on the right to interview and communicate with counsel and closed trial etc.*

*The national security criminal exemption law systems in advanced overseas countries are connected to the power of law enforcement institutions. In case of information or investigative agency enforcing legal system, the retrogression of evidence rule or related policy according to the criminal skills developing every day causes contraction in information or investigation activities. Of course, the strict criterion of compliance with due process by the Constitution, but without acknowledgement on the advanced country-type evidence rule or exemption pursuant to criminal procedure, terror or spy suspect is arrested through intelligence or investigation activities but the evidencing power may be denied at the trial stage, causing demoralization and contraction on investigative activities. In addition, if the legal system cannot trace the corresponding criminal skills, then the investigative activities would be contracted and crime prevention effect would not be anticipated. This is because any restriction on investigation activities on even the crime that could cause serious threat to the benefit and protection of the social or national law such as terror or spies due to an inferior legal system can revive the nightmare of another 9/11 terror. Within the new security environment of the threat of international terrorists and the division into North and South co-existing, Korea's legal system and policy cannot respond to the new national security situation with old-fashioned position and complacent attitude. In such a new security environment. a new approach is required at this point in time.*

**[Keywords]** National Security Criminal Law, National Security, Terrorism, Privacy, Criminal Procedure Exception



## 1. Introduction

Since the outbreak of 9/11 terror, the U.S. has adopted and enforced reinforced laws on the crimes that infringes upon the national benefit and protection of the law. This Act named the USA Patriot Act is assessed as the legislation that acknowledged the exemption on normal investigation procedure. As such, for security crime that involves mass casualties of human lives or property damages such as terrorism, it is more important to prepare a pre-preventive system rather than working on a reactive system. In addition, due to the recent IS hostage incident and French terror case, chief of states of Japan and France are considering legislative action to reinforce the power of law enforcement agencies like the USA Patriot Act. In this regard, this study reviews the security criminal exemption provisions in the judicial procedure of each country, and aims to devise a means for Korea to respond.

## 2. Comparative Review on National Security Oriented Judicial System

The security oriented judicial systems of major countries provide much implications to Korea. These can be reviewed as follows;

Firstly, according to the review on the legislative purpose of major anti-terror laws adopted by the U.S. and the U.K, the premise that individual person's right on information and privacy remains unchanged. However, in case the existence of the country is threatened or in case of significant offense on security, it is found that national protection benefit and protection of the law is in higher priority than the personal protection benefit and protection of the law[1]. In other words, the rights of investigative agency to monitor telephone and email, and perusal of records such as medical finance etc. are expanded greatly, and restrictive provisions on foreigners' espionage activities within the national territory are significantly relaxed. Therefore, Korea needs to ponder on a different approach on the scope of privacy restriction between security crime and non-security crime,

in consideration of the legislative purpose of these major countries.

Secondly, the National Security Letter issued independently by government agencies such as FBI or CIA without approval by court, as a kind of administrative summon is based on requirement for issuance pursuant to Article 505 of the Patriot Act 2001. which is more relaxed than before. Accordingly, no reasonable cause needs to be presented upon issuance. This obligation for non-disclosure was determined as unconstitutional at 2004 Doe v. Ashcroft decision[2]. Due to revision in 2005, in case an obligation for non-disclosure was granted on bad faith by lessened requirement for composition such as unreasonable, oppressive, or otherwise unlawful demand for information, then the court is entitled to revoke or change it. However, in case bad faith is not proven, then there is no way to overturn it[3].

Therefore, regarding the issue of abused National Security Letter, it is proper to prevent granting of abnormal and unlimited power to an investigative agency in the legislation of anti-terror acts, and it is essential that thorough judicial supervision is accompanied even if these legal system is inevitably newly established. More than anything, close inter-agency cooperation is necessary, through proper role sharing by organic integration rather than strict role allocation between intelligence agency and enforcement agency and through continued mutual feedback[4].

Third, with regard to terror crimes, punishment is being strengthened by newly establishing the crime of organizing a terror group. Korean Criminal Act Article 114 adopted the crime of organizing a terror group by stipulating "A person who organizes a syndicate or group with the intent to commit a crime is punishable by the punishment determined on the particular crime. Provided, that the penalty may be mitigated". However, terror crime has a particular purpose and the risk and subsequent damage is unimaginable, so consideration should be given on whether to newly establish the crime of organization of terror group and whether it is necessary to



punish it more severely than the crime of organizing a crime group. Of course, the principle of proportion shall be complied, hence it would be proper to adopt the provision that the judicial punishment shall be imposed applying the purposed crime *mutatis mutandis*, or aggravated to the purposed crime[5].

Fourth, like the German Criminal Act Article 129-a, it is necessary to consider whether it is necessary to expand the possible punishment to terror offender, by adopting the crime of supporting terror group, and crime of publicizing to recruit a member of applicant to terror groups. The crime of supporting terror group can practically be equivalent to crime of aid to terror crime. However, in case it is regulated by separate requirement for composition, the application of the judicial reduction provisions at the Criminal Act article 32 paragraph 2 may be excluded, hence the practical benefit of regulation exists[6].

As such in case of developed countries, the adoption of criminal exemption procedure was based on the determination that the human rights of suspects shall be limited to a certain degree in case of security related investigation. Meanwhile, in comparison with foreign practice, it is true that the Korean situation is behind the legal system of developed countries. In case of security crime, the judicial system well away from the reality is no different from demanding evidencing power and legal procedures at an identical level of normal criminal cases, with the hands and feet of the anti-communist agency tied up. Therefore, if the Patriot Act of the U.S. or the U.K. and Germany's anti terror legal system is difficult to follow, it is time to enact the criminal exemption provisions in our special act or at least prepare special provisions at the Criminal Procedure Act on security offenders.

### **3. Improving Measures for National Security Oriented Judicial System**

#### **3.1. Necessity to amend protection of communications secrets act**

##### **3.1.1. Relaxed requirement for limitation**

#### **on telecommunication**

As reviewed in each country's security exemption provisions, terrorists prepare and execute terror mainly with an international organization network, hence it is found that limitation on telecommunication on wired-wireless communication is found as necessary, in order to collect crime information and trace terror suspects. The behavioral type of terror has similar aspects with the behavioral type at the Protection of Communications Secrets Act, article 5[7]. It would be an error of analogical interpretation if we deem this as considerably threatening to national security or to be by activities of hostile country, anti-state group. Therefore, in case of terror crime not committed by North Korea, it would be proper to execute limitation on telecommunication by applying the Protection of Communications Secrets Act, article 5. However, the period of two month at article 6 paragraph 7 stipulating the monitoring period pursuant to Protection of Communications Secrets Act article 5, is the provision prepared in consideration of domestic offender who can be controlled in timespace[8]. So it would be proper to extend the permitted period in order to overcome the obstacles due to the required time for interpreting the code words in foreign language and the time difference between regions.

Therefore, in order to collect and trace the information on terror organization and terror plan, emergency monitoring period of 5-7 days is required. In this regard, while the emergency monitoring period on domestic resident is 36 hours, it is criticized that any extension of foreigner monitoring period on a foreigner suspect is unfair discriminative treatment by special discriminative management of foreigner who entered and is staying legally pursuant to laws and regulations, or emergency disposal on communication in violation of the principle of proportionality.

However, review of the legislative cases of major countries on monitoring, shows that the U.S. allows up to 120 days of monitoring period to foreigners, and extends the period to a maximum of one year if necessary. The U.K. also allows up to 180 days of monitoring

period on terror suspects, and extends the period to a maximum of one year if necessary. Germany, allows up to 90 days of monitoring period, and permits an extension within the scope of 3 months. The U.K. is concretely specifying it as a terror suspect. In case of the U.S. and Germany, though there is no particular mention of terror crime, but allows the monitoring period of 3 months to a maximum of one year, in consideration of a significant crime in case like terror. In case of these major countries, it is found that the monitoring period is allowed longer than in Korea, and the extended period is acknowledged longer as well. Therefore, it is worth to consider whether to add terror related crime to the eligible crime pursuant to the Protection of Communications Secrets Act article 5. In consideration of the characteristics of terror crime, the monitoring period currently regulated as two month and two months' extension as necessary shall be changed to at least 3 months as in the case of Germany, and it would have to be considered to allow further extension if the preconditions thereof are met. In consideration of the aspects of the importance of the issue of terror crime prevention, justification of purpose and relevancy of measures, and enhanced international cooperation for terror crime prevention, extension of emergency monitoring period for foreign terror suspects is acknowledged as purposeful, and is regarded as not in breach of the principle of proportionality.

Considering this in relation to security offender, it is necessary to include security offender as the monitoring target by amendment of the protection of communications secrets act, if regulation is necessary on monitoring for national security practically for proactive prevention. Therefore, it is necessary to add the requirement on security offender to the requirement for emergency monitoring, and to allow emergency monitoring. As an example, it is proposed that the prosecutor, judicial police or the chief of information investigative agency can take the action of limitation on telecommunication without a court's approval, if the cause of emergency such as serious crime is planned or committed that conforms to the requirement for national security crime leading to

preparation, conspiracy, risk of direct death or serious injury threatening the national security. This is because it is difficult for the public authority to act in advance and obtain evidence even with the monitoring permit being obtained by court's strict review if the National Security Act offender such as serious criminals or spies use mobile phones, as examined above. In this regard, it is necessary to introduce developed countries' level of monitoring system composed of three participants of approval(permit(court and the president) -execution(information investigation agency) -cooperation(telecommunication carrier) on all communication means including mobile phones, by guaranteeing legitimate monitoring through transparent law enforcement procedure such as the preparation of legal devices that can protect the freedom of communication and personal privacy of the general public.

### **3.1.2. Systemized introduction of monitoring equipment**

In case of major developed countries, it is found that monitoring by law enforcement agencies are expanded in execution in case of security offenders such as terrorism. In Korea, such system is necessary so that monitoring can be performed on security offenders only. For this purpose, legislation shall be pursued to have the enterprises introduce monitoring equipment compulsorily. In addition, in case of investigation, submission of data on security offender by enterprises shall be made compulsory rather than in voluntary submission form so that the admissibility of evidence thereof can be acknowledged. Main contents is comprised of establishment of new provisions obliging the telecommunication carriers to introduce equipments necessary for execution of limitation on telecommunication, and to establish the technical advisory committee on the limitation on telecommunication for technical advice and opinion gathering from related agencies such as adoption of related standard and equipment development etc.

### **3.2. Necessary personal compulsory measures on security crime suspects**

It is no exaggeration to say that the success or failure of national security crime investigation is dependent on arrest and detention of suspects. However, it is not easy to determine whether relevant crime was actually intended when arresting security crime suspects, and after national security crime execution, the arrest of crime suspects would not be significantly meaningful from the aspect of crime prevention. In this regard, each country has relaxed the requirement for effective arrest and detention on security crime offenders, despite the debate on the infringement of human rights through proper procedures. Korea also needs to consider the special provision on personal compulsory measures on security crime suspects for the purpose of protecting the lives and safety of the public through effective control on security crimes.

For detention procedure of security crime suspects, the extension of detention period can be considered top priority. According to the current Criminal Procedure Act, detention period is; ① within 10 days in case judicial police detains the suspect, ② within 10 days in case a prosecutor detains the suspect or receives notice of suspect from judicial police ③ prosecutor is entitled to apply for extension of detention period only once to the judge of district court to the extent not exceeding 10 days in case of justifiable reason for continuous investigation on the suspect under detention[9].

As mentioned before, because the verification of suspicion on security crime is more difficult than common crime due to the secrecy, systemicity, internationality of the crime, consideration on extension of the detention period is necessary. As the legislation reference case for extension of the detention period, the special provision introduced in National Security Act article 19 can be suggested. According to this Act, the first extension is allowed to the judicial police and the second extension is allowed to prosecutor if justifiable in the course of the crime investigation. Hence, a similar special procedure may be considered in security crime investigation. Of course, careful approach is required here, as the relaxation on the detention requirement for security crime suspects is an issue that

could be in conflict with the protection of basic rights of the suspect and a violation of proper procedure. However, in consideration of the fact that security crime is differentiated from common crime in the degree of illegality and the difficulty in recovery of the damages, introduction of such special provisions may be worth considering.

### **3.3. Discussion and application of secret search and emergency access right**

As reviewed before according to the current law, a staff in charge of an investigative agency has no right for forced entry or investigation upon arrival at a dangerous site, if the resident denies such entry or investigation. The crime types requiring prompt response (terror crime, security crime etc.) may lead to huge human casualties or national loss, if proper response is delayed. Therefore, forced entry or investigation, if executed properly, could be a useful system to protect the citizen from a powerful and impending crime. In this regard, secret search system is operated in advanced countries. In Korea, the emergency access right as the similar right thereto, was discussed. The emergency access right is the right granted upon an outbreak of an emergency situation to the investigative agency to enter other people's residence and investigate the site and the people at the site by force, for the purpose of clearing risks. The emergency access right is based upon the premise of an extremely exceptional situation. This is never intended to intervene the peaceful living of the people in a normal situation. It is the obligation of the nation to establish a legal system corresponding to the crisis in the modern society where crisis always exist. However, the emergency access right will have life only when preemptive response to the concern on infringement of the citizens' human rights is in place beforehand. The procedural transparency shall be secured as the pre-condition. By sufficient explanation on the purpose of emergency access, the understanding from the resident shall be obtained. After exercising emergency access right, the investigator shall be obliged to report to his/her senior officer immediately. Furthermore, if necessary, judicial control system shall be prepared to supplement

the legitimate procedure that has not been satisfied in advance. Furthermore, in consideration of the direct purpose of introducing emergency access rights, it is necessary to limit the scope of exercise thereof to the threat to national security and the lives and health of the people. Accordingly, in order to satisfy the conflicting requirements of protecting the peoples' lives and safety by positive intervention by the public authority, simultaneously with non infringement on human rights in the process of exercise thereof, systemic supplementary measures are essential.

#### 4. Conclusion

This study has reviewed the domestic situation related to national security investigation as well as overseas national security criminal exemption cases. It is true that Korea is facing an environment that is vulnerable to casualty of security by offenders. In case of developed foreign countries, the government never compromises or negotiates with terrorists but compromises with the threat from international terrorists under the grand criminal law principle even without the historical situation of national division, occasionally extending detention period or allowing communication monitoring on case by case basis. As such, the developed countries emphasizing protection of human right such as the U.S. as leader of Anglo-Saxon law as well as Germany as the leader of continental law are found to be equipped with strict criminal judicial system against the forces threatening the national security.

Since the 9/11 terror, the U.S. enacted the Patriot Act that stipulated the exemption on criminal procedure to restrict the constitutional basic rights for the purpose of opposing security threats and terror prevention, and acknowledged not only broad monitoring but also the power of investigative agencies broadly in the course of search and execution of confiscation warrants. The act allows monitoring of e-mails on terror or spy suspects for one year subject to decision by an investigation authority without court approval. In addition, monitoring is allowed on all phones of

terror suspects to facilitate the communication tracking. Furthermore, U.S. federal administrative judge comprehensively acknowledges and issues search and confiscation warrants on the properties and people all over the country in terror and spy cases.

The U.K. also introduced Anti-terror Crime Safety Act to permit arrest and detention of terror suspects for 7 days without warrant. And in case of foreign terror suspects, the U.K. allows emergency detention and account supervision. Furthermore, the criminal evidence rule adopted the provision to restrict the right of the suspect to interview solicitor if it is concerned that evidence may be erased for terror prevention is thwarted[10]. In case of Germany, criminal procedural exemptions such as detention condition and bank account search contrary to usual criminals, are acknowledged in case of terror or spies. The investigative agencies in Japan and Australia have expanded the scope of monitoring on suspects, and the trend is accepting restriction on basic rights by search of residence without warrant and long detention period, and facilitating verification on crime, by sentencing in comparison between protection of basic rights and the public interest in case of security offender such as terrorists and spies[11].

These countries operate the special laws that could restrict the basic rights guaranteed by the Constitution, showing the feature of granting huge rights to investigation on terror or spies, sparing no systemic support. To the contrary, Korean national security investigation is reputed as having reached the limit due to the recent court's denial on the statements of evidence against national security offenders, and the impossibility of monitoring mobile social networks.

As shown at the failure cases of investigation so far, active response to the crime technique of terror and security offender's crime, that has been evolving technically and scientifically, is not possible. In case of developed countries, no paternalism is practiced on international terrorists similar to security offenders, and punishments are being stepped up, by approaching from the aspect of public interest rather than honoring the basic rights

of terrorists. Meanwhile, Korea is shown as weakening the rights of information agencies and investigative agency, and the judicial branch is also trending towards paternalism to national security offenders rather than sentencing their imprisonment. This is in contrast to the practice of developed countries, likely to cause distrust in the judicial branch. However, current status quo in Korea allows no anticipation on progressive legal system and investigation environment[12]. Therefore, Korea needs to break away from the old fashioned investigation environment, while modeling foreign legal system against terrorists based on the new concept of security. For this purpose, this study emphasizes again the fact that the legal system on national security offenders need to be revised at least to conform to the new security environment.

#### Author

**Lee Hyun-jung** / Dongseo University Professor  
B.A. Sungkyunkwan University  
M.A. Sungkyunkwan University  
Ph.D. Sungkyunkwan University

#### Research field

- Improvements in Sentencing Guidelines Based on Theory of Scope of Responsibility, Korean Journal of Comparative Criminal Law, 13(1) (2011).
- Possible Responses in Criminal Law to Government Subsidy Frauds, Foreign Law Review, 35(3) (2011).

#### Major career

- 2010~2011. Institute for Legal Studies in Yonsei University, Post Doctor
- 2016~present. Central Police Academy, Lecturer

## 5. References

### 5.1. Books

- [1] Kim IS. Meaning of Love in Criminal Act Order. Sechang (2013).
- [4] Vincent EH. Developing Local Law Enforcement's Strategic Capacity to Combat Terrorism in the United States. Prentice Hall (2005).

### 5.2. Conference proceedings

- [12] Kim SG. Diagnosis and Countermeasures on Security Criminal Law System. Debate on Security Criminal Law (2015).

### 5.3. Additional references

- [2] American Civil Liberties Union V. Ashcroft (2004).
- [3] [www.nytimes.com/](http://www.nytimes.com/) (2016).
- [5] [www.moj.go.kr/](http://www.moj.go.kr/) (2016).
- [6] Criminal Law in Germany (2016).
- [7] [www.moleg.go.kr/](http://www.moleg.go.kr/) (2016).
- [8] Communication Secret Protection Act in ROK (2016).
- [9] Criminal Procedure Law in ROK (2016).
- [10] Anti-terror Crime Safety Act in UK (2016).
- [11] [www.verfassungsschutz.de](http://www.verfassungsschutz.de) (2016).



Publication state: Japan  
ISSN: 2423-8767

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

Corresponding author  
E-mail: [pws7897@skku.edu](mailto:pws7897@skku.edu)

Peer reviewer  
E-mail: [editor@j-institute.jp](mailto:editor@j-institute.jp)

<http://dx.doi.org/10.22471/law.2016.1.1.25>

© 2016 J-INSTITUTE

## The Study of Acceptability of Search and Confiscation for another Digital EVIDENCE

Park Woong-shin

*Sungkyunkwan University, Seoul, Republic of Korea*

### Abstract

*The issue with digital evidence has been discussed continuously in Korea because its unique characteristics such as independence, invisibility, mixture. In this sense, question is that whether or not the principles of traditional Criminal Procedure Act can make application to digital evidence.*

*This thesis focus on investigative agency that cope with seizing digital information that is not related to crime. When investigative agency seize digital information, most of them are not original evidence but copied evidence according to article 106 of Criminal Procedure Act. Thus, this study examines whether or not the investigative agency should get search and confiscation regarding another digital evidence despite having copied image evidence. This thesis points out that precedent cases that judge investigative agency should get another search and confiscation in order to continue investigation should be criticized because it can hinder dynamics of investigation.*

*However, in the case of independent search and confiscation, abuse of authority can concern. So, the thesis insists jurisdiction should adopt limited search and confiscation against dangerous power which harm national security.*

*The digital evidence holds unique features like media independence, information with no shape, easy replication, vulnerability, massiveness and network relevance but most regulations in the current criminal evidence act do not presume such digital evidence, creating a vacuum in the legal regulations.*

*The relevant regulations in the current criminal evidence act should be interpreted by considering the feature of the digital evidence. However, the interpretation has limitations in filling the vacuum in the criminal act with established principles in prohibiting the guessing and implementing strict interpretation.*

*Therefore, the criminal evidence act should be amended to cover digital evidence. All the evidence requires sincerity but digital evidence additionally requires unique prerequisites like the identity with the original version, integrity and reliability.*

*Judicial precedents on how to prove such prerequisites have been gradually accumulated but in the long term, specific rules should be clearly developed for law enforcement agencies to follow, and the customs or legislation amendment is required that can accept or guess that the prerequisites above are satisfied if the rules are proven to be observed.*

**[Keywords]** *Justice, Electronically Stored Information, Seizure and Search of Electronically Stored Information, Warrant in Principle, Seeking for Selection*

## 1. Introduction

Nowadays, the main issues of digital information is not elemental question whether digital information is object of confiscation or not, but whether it can regard as a material

evidence under same procedure. To be more specific, it is obvious that Search and confiscation of digital evidence take long time compared to material evidence. In this case, whether limited statute that is for material ev-



idence can make application to digital evidence. For this reasons, the issue under criminal procedural code has been discussed, but the thesis focus on how to deal with digital evidence that is not related to crime in the process of search and confiscation. For example, when the investigative agency which have confiscation warrant for case A found out another digital evidence for case B, how investigative agency cope with another information? This is because criminal procedural code requires relevance in order to seize[1].

This study examines the characteristics of digital evidence and the relationship between this and specific security cases. Also, the study analysis legal principles and cases for unrelated digital information.

## **2. The Characteristics and Problems of Digital Evidence**

The digital evidence is unique because 1)its storing medium and information itself of independent context is used 2)it is invisible so it needs to change process in order to see 3)it is high probability of contamination in the process of change procedure. 4)it is mixed with unrelated information because of its feature[2].

These characteristics can bring about not only difficulty for application of warrant requirement but community's safety of our country where divided two parts. This points can be understand by analyzing different kinds of cases that contributed to make legal principle concerning digital information.

## **3. Whether another Digital Information in the Process of Confiscation of Digital Evidence is Permitted**

### **3.1. Introduction**

When the investigative agency which have confiscation warrant for case A found out another digital evidence for case B, how investigative agency cope with another information? If objet of confiscation is material evidence, it cannot be seized even if investigative agency

find another evidence of crimes. This is because it is not related to original purpose of warrant that had issued. They should issue a warrant in order to seize it. However, in the case of digital evidence, copied image evidence was already under investigative agency, should they issued a warrant for B suspicion again?

### **3.2. Judicial precedent regarding confiscation of another digital evidence**

Korean Supreme Court says that "if investigative agency finds information which is related to crime by accident in process of seizing digital information that is in order, the investigative agency should stop to search and then take search and confiscation again for new information. Also, only when they issued warrant, they can confiscate" and "Another process of search and confiscation is totally different from original process of it. If there is not special situation, the investigative agency should take action for protecting someone who is seized objects and issue a list of confiscated goods under article 219, article 212, and article 129 of criminal procedure code[3]. The judicial system requires to issue a new warrant for new crime suspicion in spite of taking time. This attitude of case cause problem because the evidence can be damaged from suspect and make hinder the dynamics of investigation.

### **3.3. The solution for finding another digital information during confiscation**

The cases that investigative agency found another digital information accidentally during the investigation and then stopped search and issued a new warrant is not a specified to digital evidence. That is, the discussion about how to cope with new material evidence during search and confiscation have been suggested continuously[4]. It is difficult to seize individual evidence in the situation that cannot arrest suspect because exemption of warrant requirement under current law. There are, of course, two ways to solve the problems which are to receive voluntary submission from owners and to issue another warrant as precedent's purpose.

However, in the case of voluntary submission, it is impossible to have evidence if owner of it doesn't agree. Also, it is expected to dissipate if investigative agency issue new warrant. For these reasons, adopting to urgent search and confiscation system is suggested in order to reveal substantial truth[5][6][7]. However, there has also been criticism toward this opinion on the grounds that independent urgent search and confiscation that doesn't have warrant limit warrant requirement for just convenience[8]. This problem should be solved by enhancing quick and efficient investigation technology of investigative agency[9]. Even if it is urgent situation to seize evidence during investigation, it is not worth of giving up warrant requirement and cannot be justified.

Judicial system permit search and confiscation which doesn't have warrant for urgent situation Article 216, article 217 of criminal procedure code. However, these rules are only applied in the case of arresting of restraint suspect, independent search and confiscation, especially digital evidence is for search and confiscation which are not related to arrest and restriction. Therefore, if independent urgent search and confiscation system is adapted for digital evidence, this is not exemption of warrant requirement. Moreover, criminal procedure code regulates to specify object for seizing and place, but it is difficult to expect which object is exist and is invalid from requesting and issuing warrant until each information reveal to obvious evidence[7][10]. If independent and urgent search and confiscation is adapted in order to accidental evidence, investigative agency can issue a warrant after confiscation regarding another evidence that is found accidentally and if that evidence is not related to crime for warrant is revealed invalid, the object can return.

I think it is reasonable to institute independent urgent search and confiscation system in the current situation that has control possibility about urgent confiscation. The notabilia is that even if investigative institution take act independent urgent confiscation, the thing should be divided into two parts: first,

confiscation of that evidence; second additional search[11].

### **3.4. Whether or not independent emergency system permits regarding security offender**

If independent emergency search and confiscation is adapted, it should be determined which crimes can be applied. This is because application of it for crime can violate principle of proportion even if approval for another evidence that found independently admit. To do this, there are two ways. First, it can be determined by the standard of statutory punishment; second it can be judged by the crimes in specific areas. Korea Constitution article 12(3) regulates that "Warrants issued by a judge through due procedures upon the request of a prosecutor shall be presented in case of arrest, detention, seizure or search: Provided, That in a case where a criminal suspect is an apprehended flagrante delicto, or where there is danger that a person suspected of committing a crime punishable by imprisonment of three years or more may escape or destroy evidence, investigative authorities may request an ex post facto warrant." Thus, independent emergency search and confiscation system can be adopted only in the case of penalty that imprisonment for life or imprisonment for 3 years.

Also, application or not can be determined by standard of specific kinds of crime. This case can be considered by specific crime that has high possibilities threatening against life and body of members of community. This case can be suggested like murder, robber, and security crime.

However, in the case of violent crimes, it is improper to institute independent emergency search and confiscation preferentially due to the fact that material evidence can be found in this kinds of crimes Security crime is particular crime unlike normal criminal cases in that it threaten constitution system and safety and existence of community. Intelligence and investigative agency require not only to collect direct evidences which are related to prove suspicion but also to collect indirect evidences which are helpful to process itself[12]. This is because investigative

agency should prove the suspicion of national security offender that they endanger to national safety and existence. Therefore, I suggest that independent emergency search and confiscation should be applied national security offender first.

## 4. Epilogue

Korean Supreme Court says that “if investigative agency finds information which is related to crime by accident in process of seizing digital information that is in order, the investigative agency should stop to search and then take search and confiscation again for new information. Also, only when they issued warrant, they can confiscate” Then, Seoul Central District Court developed ‘The improvement plan digital evidence investigation practice’. This data was difficult to collect, but it can be supposed to like this:

- Investigative agency can collect digital information which is related to crime in storing medium.
- Investigative agency should attend all process of searching, printing and copying of seized information.
- Investigative agency should delete, discard, and return the unrelated information which are found during confiscation.

Investigative agency should have discretion about another information that is not expected before issuing a warrant so that they can counteract to investigation situation. Especially, this is strongly needed to cooperate crime, intelligence crime, and national security crime rather than criminal crimes. To be more specific, warrant requirement can be exemption in the case of high possibility of damaging evidence for example, when investigative agency enforce search and confiscation for embezzle, they found secret funds, evasion of taxes; when they enforce search and confiscation for communication crime under national security code, they find information regarding piracy of a rebellion.

The problem is that criminal defendant's right can be limited if their attendance right admitted narrowly, but investigative agency's

power to search and confiscation of information enlarge. This problem can be combined with limited rights to have lawyer in the national security offender and lead to weakening criminal defendant's rights. This is not coped with the fair comparison of interests between truth and safety of community, but it should be solved by establishing special court and make regulatory plan including judicial control in the long run.

## 5. References

### 5.1. Journal articles

- [1] Jung DH & Lee SM. The Question of Relevance in Searches and Seizures of Digital Evidence. *Korean Criminological Review*, 26(2), 95-130 (2015).
- [5] Son DK. A Study on the Search and Seizure of Digital Evidence in Amendment Criminal Procedure Acts. *Korean Journal of Criminology*, 23(2), 325-349 (2011).
- [9] Cho K. Requirement of Legitimate Search-and-seizure. *The Journal of Comparative Criminal Law*, 5(2), 29-782 (2003).
- [10] Park HS. Practical Research on Search and Seizure of Digital Information. *New Trend in Criminal Law*, 44, 76-113 (2014).
- [11] Kim SY. Vorläufige Beschlagnahme eines Zufallsfundes im Bezug Auf Die Elektronischen Informationen. *New Trend in Criminal Law*, 49, 106-158 (2015).

### 5.2. Thesis degree

- [2] Park MW. A Study on the Due Process of Law in Search and Seizure of Digital Evidence. Korea University, Doctoral Thesis (2016).
- [6] Kim ES. A Study on the Scope and Criteria of Exclusionary Rule of Illegally Collected Evidence for Seized Articles. Chonnam National University, Master's Thesis (2014).

### 5.3. Books

- [4] An SS. Criminal Procedure Law. Pakyoungsa (2010).
- [7] Roh MS & Lee WK. Criminal Procedure Law 4th Ed. SKKUP (2015).

[8] Lee EM. Criminal Procedure Law 5th Ed.  
Pakyoungsa (2015).

#### 5.4. Additional references

[3] [www.scourt.go.kr/](http://www.scourt.go.kr/) (2016).

[12] Supreme Courten Banc Decision (2010).

##### Author

**Park Woong-shin** / Sungkyunkwan University Senior Researcher

B.A. Sungkyunkwan University

M.A. Sungkyunkwan University

Ph.D. Sungkyunkwan University

##### Research field

- On the Study of the Role of the State in Knowledge Information Society -Debate Centered on the Improvement of Accredited Certification System-, Sungkyunkwan Law Review, 25(4) (2013).

- A Study of Terror Concept, Korean Terrorism Studies Review, 6(2) (2013).

##### Major career

- 2015~present. Korean Institute of Criminology, Appointment Researcher

- 2016~present. International Society for Justice & Law, Editor in Administrator