Abstract

**Purpose:** Counter-intelligence means any act in response to hostile foreign intelligence activities. Since the activities of intelligence agencies inherently recognize security as the greatest virtue, it was not easy to approach it in the academic field. However, the global information environment is changing rapidly. In the traditional concept of espionage, espionage was carried out mainly in the political and military areas, but in comprehensive security situations, information collection on various forms can take place, requiring a flexible strategy.

**Method:** However, despite the fact that anti-spy operations can directly be involved in infringement of the basic rights of the people, the fact that minimal ground rules exist is a problem that requires improvement in terms of the rule of law of information activities. Furthermore, the problem of this study is that even assuming the objective consideration that anti-spy work is necessary to guarantee basic rights of the people, and that it is not appropriate to impose public and judicial control such as investigation procedures, it is unfortunately not. In response, this study proposed improvements to prevent concerns about infringement of the basic rights of the people by guaranteeing practical anti-spy work in a changing environment.

**Result:** The first is the expansion of the concept and scope of the anti-spy. In other words, if the Framework Act on Anti-Spy is enacted, the concept of anti-spy should be set as an active and active anti-spy concept, not a passive or passive anti-spy concept, to diversify anti-spy operations and respond to both traditional and non-traditional threats. In addition, the government proposed the expansion of spy agencies to cope with the diversification of security threats due to changes in the information environment. Second, he pointed out existing problems and made some forward-looking suggestions regarding the smooth performance of anti-spy operations. The most important confirmation here is the stipulation of the means of collection and verification of anti-spy information. The method of collecting anti-spy intelligence can be distinguished in legal and realistic ways, and the factual methods such as collecting human information, technical information, and public source information are problematic.

**Conclusion:** In particular, legal grounds and reliability, such as-undercovering the identity or operating an informant, are problematic in the intelligence officer’s performance of specific espionage tasks. In order to dispel this, it was confirmed that there is a need for evidence that the staff of the spy agency can impersonate their identity in specific tasks, and a legal basis that the spy agency can operate a cooperative.

**Keywords** Counter-Intelligence, National Security Law, Counter-Intelligence Intelligence, The Rule of Law of Intelligence Object, Comprehensive National Security

1. Intro

Counterintelligence activities are understood as all acts in response to hostile foreign intelligence activities and are recognized as a subclass of intelligence agency information activities in a systematic way. However, the activities of intelligence agencies inherently recognize
security as the greatest virtue, so accessing anti-spy from an academic perspective has been a challenging area. Furthermore, the normative discussion of the activities of intelligence agencies itself may lead to unnecessary misunderstandings (politization of so-called information) making it more difficult[1].

However, the global information environment is changing rapidly. The traditional security environment has been discussed under political and military confrontations centered on the polar system of the US and the Soviet Union, but with the rise of the 21st century, the concept of a traditional security environment has come to an end. The end of the Cold War, informatization, and globalization have sent traditional security concepts to a page of history, and the vacancy is occupied by a new security environment. In other words, the concept of state-central security, which traditionally emphasizes only the sovereignty of the state, has changed from a concept of comprehensive security that extends the subject of security to individuals, organizations, businesses, natural environments, and international organizations. In the traditional concept of espionage, espionage was carried out mainly in the political and military areas, but in comprehensive security situations, information collection on various forms can take place, which requires a flexible strategy.

But what is the legislative reality of our country about anti-spy activities? Currently, the National Intelligence Service Act is the only legal basis for espionage, and there are only "regulations for planning and coordination of information and security departments" and "regulations for espionage" under the presidential decree. Despite the fact that espionage can directly violate the basic rights of the people like other information and investigation agencies, there are many problems in terms of improving the efficiency of espionage activities and "the rule of law" under the global information environment. Furthermore, even assuming the objective consideration that anti-spy work is necessary to guarantee the basic rights of the people, and that public and judicial control is not appropriate, such as investigation procedures, questions are raised about whether the current regulations for anti-spy work can achieve a certain purpose.

As a result, this study aims to present improvements to prevent concerns over infringement of the basic rights of the people by enhancing the efficiency of the anti-spy work in a changing environment and guaranteeing practical anti-spy work. First of all, we will critically examine the current attitude of the law to regulate espionage, specifically focusing on the National Intelligence Service Act and sub-commands(2). This will lead to specific limitations of the anti-spy operations carried out in these legislations(3). Finally, we would like to present improvements to overcome the limitations of performing these anti-spy tasks(4).

2. Status of Anti-Spy Operations Under the Current Legislation

2.1. National intelligence service Korea act

Under the National Intelligence Service Korea Act, three major articles related to espionage are Article 1(purpose), Article 3(duties), and Article 15(request for cooperation with state agencies).

The problem is that under the current National Intelligence Service Korea Act, the target of Counter-Intelligence is limited to national security[2]. Of course, the National Intelligence Service Act, a direct basis for espionage, limits the scope of espionage to national security guarantees, which seems to lack awareness of the changing global security environment. In addition, Article 3(1) of the National Intelligence Service Korea Act limits domestic information services to some "domestic security information," but there is also a problem that the National Intelligence Service is too narrow in scope of its domestic espionage operations[3].

2.2. Regulations for planning and coordination of intelligence and security affairs
Regulations for Planning and Coordination of Intelligence and Security Affairs for the purpose of prescribing matters necessary for the planning and coordination of Intelligence and security affairs shall not directly prescribe Counter-Intelligence affairs. However, Article 2(Define) 2 stipulates that "the domestic security information is treated to ensure the safety of the country from harmful acts against spies and other anti-state activities" and Article 4 stipulates that "the measures to prevent or delay the leakage of secrets directly or indirectly by means of communication." In addition, the National Intelligence Service(NIS) designates the scope of planning and coordination work with related agencies(Articles 4 and 5) and stipulates procedures for planning and coordination work(Articles 6) and audit procedures for information business, budget and security work(Article 11).

The purpose of this regulation is to prescribe matters necessary for the planning and coordination of intelligence and security affairs. Therefore, the government should plan integrated planning and coordination of intelligence and security affairs with the Executive Branch, establishing basic guidelines for national security policies, legislative and judicial branches[4].

2.3. Counter-intelligence regulations

The National Intelligence Service has been performing counterintelligence in response to all-round domestic information activities of foreign intelligence agencies. Recently, the government-wide integrated counterintelligence system has been established to systematically and efficiently respond to foreign intelligence activities. According to the necessity of operation 2012.05.14. In accordance with Article 3(Occupation), Paragraph 2 of the National Intelligence Service Act, the “Counter-Intelligence regulations(Presidential Decree No. 3780)” are enacted and implemented.

The enactment of these regulations is a tangible achievement in the history of the country's Counter-Intelligence operations and is evaluated as the result of efforts by the National Intelligence Service and related agencies to efficiently carry out Counter-Intelligence operations at the government level[5].

However, the above regulations lack judicial control over espionage, which is likely to violate basic rights, as there are no sub-laws that have weak legal grounds and specific procedures for execution of duties.

2.4 Conclusion

As shown above, the National Intelligence Service Act is the only law that is based on the law to carry out espionage operations, and there are "Regulations for Planning and Coordination of Intelligence and Security Affairs" and "Counter-intelligence regulations" as lower legislation. The fundamental purpose of espionage is to seek national security as a means to guarantee the basic rights of the people. The problem is that the role of carrying out anti-spy operations can inevitably limit the basic rights of the people. Of course, this is the same investigative activities by investigative agencies, but there is a difference in the fact that while investigative activities have safety devices under various normative systems, including the Criminal Procedure Act, espionage has a profound legislative gap. In other words, the attitude of our law is not the case even though judicial control through the normative system considering the specificity of espionage can guarantee democratic legitimacy in the country's espionage operations. Furthermore, the performance of anti-spy operations under lower legislation can be criticized. In particular, the anti-spy business regulations can actually be seen as a minimum legislative device for anti-spy operations flood, as the anti-spy operations regulations do not have minimum conditions for performing anti-spy operations in a changing security environment.

In other words, the lack of democratic legitimacy, predictability, and court control despite the power of state agencies is the biggest problem and starting point of the norm system in charge of current Counter-Intelligence[6].
3. Problems of Counter-Intelligence Activities

3.1. Recent changes in counter-intelligence activities

The reorganization of the world order after the post-Cold War led to drastic changes in the intelligence environment, including changes in national security awareness and concepts. In the past, in the dichotomous structure of Cold War enemies and allies, intelligence priorities were limited to military security due to clear targets and goals. However, the post-Cold War intelligence environment expands the scope and scope of intelligence activities, ranging from traditional security threats such as military and defense to terrorism, environmental pollution, health and resource crisis[7]. And this requires intelligence organizations to expand effective intelligence activities[8].

Furthermore, the transnational phenomenon caused by the intensification of globalization shows a different aspect from existing national-centered intelligence activities in the subject, subject, scope, and response methods with the emergence of transnational threats[9]. In other words, the concept of state-central security, which emphasized only the sovereignty of the state and the state, was expanded to non-state entities such as individual, organization, business, natural environment, and international organizations, and the concept of comprehensive security[10].

On top of that, the rapid development of information and communication technology is seriously affecting the information environment at home and abroad, by promoting political pluralism and democratization in the international community as well as in the domestic society[11]. As the Jasmine Revolution in the Middle East in early 2011, the change in the information environment is having a tremendous ripple effect on the political environment.

On the other hand, the above changes may be seen as a demand for strengthening democratic control and monitoring of intelligence agencies by causing controversy over possession of basic rights due to the expansion of the scope of intelligence activities[12]. These sensitive issues result in citizens’ calls for stricter regulations and control of domestic intelligence activities on intelligence agencies, and calls for political neutralization of intelligence agencies are much stronger. Of course, information institutions need to be reformed in line with political and social changes, but as such weak information activities are likely to be used in the psychological warfare of hostile forces, it is a matter to be watched closely in terms of smooth national defense or strengthening security[13].

3.2. Lack of legislation of basic laws and enforcement ordinances of counter-intelligence

As previously discussed, the grounding law for espionage is a counterintelligence regulation in the form of a presidential decree based on Article 3(2) of the National Intelligence Service Korea Act, and there is no sub-law that regulates the specific process of execution of duties.

There are the following arguments as to what specific authority an counter-intelligence agency has in performing counter-intelligence duties and, furthermore, whether there should be separate legal grounds for individual performance of duties: "There is no country that has laws and regulations on the method or authority of individual or specific execution of duties, as there is no fixed form in the collection of information or counter-intelligence."

"Because it is very difficult to define specific methods or authority related to espionage by typifying specific methods of execution or authority in accordance with various specific circumstances, it is feared that the statute will limit the anti-spy work that should respond flexibly to specific situations," he said. Subsequently, "According to the theory of the Administrative Organization Act, the Administrative Office shall have general authority to execute its duties within the scope of the duties prescribed by the organization and the code of duties. Accordingly, the National Intelligence Service has general authority to execute its duties based on the National Intelligence Service Korea Act and the counter-intelligence duty regu-
lations, and does not require a separate act of reference"[14]. The above view is worth listening to the interpretation of current regulations that do not have a complete system of anti-intelligence law, especially if the National Intelligence Service’s job execution is aimed at the public, it can be exercised by organizational and job norms.

However, in the case of specific public power activities targeting individual citizens, such as anti-spy investigations, there shall be grounds for law in accordance with the principle of legal reservation and shall be carried out in compliance. The bigger problem is that as the concept of espionage expands due to rapid changes in the global information environment and the advent of the cyber era due to rapid changes in the information and communication environment, the democratic legitimacy of espionage can be easily undermined. Cases where such problems may occur are considered according to the type of espionage task as follows.

First of all, it is a typical case of espionage for foreign governments, organizations, or foreigners and Koreans related to them. According to the general legal theory, there is no need for a separate act of law to perform espionage in a non-powerful way, such as cooperation, but for investigation and power methods, a separate act of law is required. Next, it is the case of defensive espionage that detects, blocks, and checks information collection activities or secret operations against foreign countries. Defensive espionage is mainly carried out through follow-up monitoring, conversation monitoring, on-site recruitment, search activities, cyber activities, etc. Direct measures may be taken, such as arresting domestic or foreign agents employed by foreign intelligence agencies or expelling foreign intelligence agents disguised as diplomats. In the case of surveillance, however, there can be problems of infringement of rights, such as privacy secrets, and arrest or deportation is a direct exercise of public power over a particular person, which requires legal authority based on individual laws.

3.3. Lack of efficient means of counter-intelligence operations

Intelligence is probably the most important thing not only in criminal investigations but also in counter-intelligence. This is because clues are needed to serve as a basis for the performance of counter-intelligence, and due to the nature of espionage, intelligence-level information that is different from those of general investigations will be needed. Therefore, how and to what extent this intelligence will be collected will be the most important issue in the performance of Korea Act and counter-intelligence regulations are silent on the collection of such counter-intelligence intelligence. This can be interpreted that our legislation basically presupposes anti-spy in the concept of passive counter-intelligence, and that the uniform collection of counter-intelligence intelligence sets the inherent limitations of counter-intelligence work.

The collection of intelligence can be made in various forms. To distinguish this from legal and realistic methods, legal intelligence collection means legal collection activities under the Criminal Procedure Act and the Police Officers’ Duty Execution Act, and realistic methods mean collection of HUMINT, TECHINT, and OSINT. It is the collection of counter-intelligence intelligence that can be the starting point for counter-intelligence operations, and this is actually an area where infringement of the basic rights of the people can occur except for the collection of public intelligence. Therefore, there is a limitation that the means and methods for performing counter-intelligence operations can be collected on the internal basis of counter-intelligence agencies without prescribing minimum guidelines in advance, which do not in accordance with the principle of national law.

4. Improvement of Counter-Intelligence Operations for Efficiency and Legality

4.1. Enactment of the framework act on the performance of counter-intelligence
Currently, the performance of anti-spy duties is supplemented by the recently revised anti-spy regulations, which are basically carried out under Articles 1 and 3 of the National Intelligence Service Act. However, this reality cannot guarantee the democratic legitimacy of the anti-spy work, and it is a well-known fact that it is undermining the predictability of the people’s predictability. Therefore, it has long been argued that there is a need to enact a law on the basis of espionage [15]. In particular, the main school did not point out the limitations of the current counter-intelligence regulations, but there are limitations of counter-intelligence under criminal law, so legislative technology can establish the basis law for counter-intelligence and proactively improve the composition of counter-intelligence. Therefore, if the government intends to discuss the improvement of counter-intelligence activities, it must consider enacting the basis law, which is consistent with the principle of state and legal reservation.

However, the establishment of a ground law on the performance of counter-intelligence will strongly raise non-lawful issues, not legal issues. In the enactment of the Anti-Terrorism Act in 2015, he also experienced a severe division of public opinion, as the performance of anti-terrorism operations is more likely to be criticized than counterterrorism. In addition, it is possible to argue whether separate legislative measures are needed, as counter-intelligence work has been carried out in the form of the current enforcement ordinance. Non-law matters, especially controversy over political pros and cons, should also be considered in implementing legislative measures to carry out counter-intelligence operations. However, if the current counter-intelligence work is raised to the normative field, it is necessary not only to secure democratic justification for counter-intelligence work but to free the counter-intelligence agency from unnecessary political controversy. Therefore, there is an extraterritorial risk of political controversy, but the enactment of a basic law on the performance of counter-intelligence affairs is an area worthy of consideration.

4.2. The expansion of foreign concepts subject to counter-intelligence

Against foreign intelligence activities, in line with the interpretation of "North Korea" in the interpretation of the law, causes problems. As you may note, Article 3 of our Constitution stipulates that "the territory of the Republic of Korea shall be the Korean Peninsula and its affiliated islands," so the Republic of Korea Constitution applies to North Korea. The majority opinion and attitude of the Supreme Court are the same in constitutional academia [16]. In other words, South Korea's constitutional order, attitude of precedent and interpretation of the National Security Law make it impossible to respond to North Korea's intelligence activities under the current counter-intelligence rules because North Korea is not within the scope of the state. Of course, counterintelligence operations against North Korea may be carried out in practice, but in terms of the rule of law, practical reality should also be carried out under the normative power of the law.

In addition, if counter-intelligences are based on foreign concepts, they cannot respond to security threats by transnational criminal organizations that are not included in any country. Terrorism crimes are emerging as a serious threat to domestic safety worldwide, and in reality, where the importance of cyberspace by physical space is increasing, if a security risk incident occurs by a non-state actor or if it is raised for security, it cannot be responded by conventional counter-intelligence.

Furthermore, if you look back on the fact that you are a Korean, this raises a problem. In other words, the conventional concept of counter-intelligence is that foreign governments use Koreans to target counter-intelligence operations, but Koreans cannot voluntarily target counter-intelligence regulations if they engage in acts that can affect national security and national interests.

4.3. The need for diversification of counter-intelligence targets
The end of the Cold War era and the emergence of various non-state actors are in line with the emergence of new players who can inevitably threaten national security. In other words, security concepts can change depending on the times and circumstances [17]. In this regard, security targets were not limited to traditional military and politics, but shifted to pursuing security in other areas of everyday life, such as economy, technology, energy, environment, and cyber areas. That is, the manifestation of the concept of human security. However, criticism could be raised that such areas are too broad for security [18]. In addition, it is too broad to be targeted for counter-intelligence, which is feared to violate the basic rights of the people.

In other words, the UNDP’s proposals could include those included in economic, food, environmental, individual and community security, which meet the inherent purpose of espionage. Specifically, all areas of Korea, such as economic, technical, energy, environment, cyber, etc. shall be considered as targets for counter-intelligence [19].

4.4. Necessity of active counter-intelligence activities

According to the current counter-intelligence business regulations, counter-intelligence is essentially a passive concept. This means "all response activities". Having a passive and defensive personality was self-evident in that it carried out activities to protect the nation from the threat of hostile forces.

However, at a time when living under such a diversified security threat, passive activities are not appropriate because they are already inevitable after infringement on national security and national interests [20]. In the era of comprehensive security threats, security threats can occur in various areas, including economic and industrial security, advanced IT technology, munitions acquisition, international crime, and cybercrime, which are not only extremely difficult to recover, but also inevitably requires an active and preemptive concept. Strategic anti-spy concept is that when using anti-spy as a means of national security, it can perform offensive functions, not defensive functions, and contribute to the establishment of national strategies through countermeasures against foreign intelligence agencies' plans, intentions, and abilities [21].

Therefore, we should also consider converting the concept of anti-spy from conventional passive counteract activities to preemptive counteract activities. However, if the concept of espionage is a preemptive response activity, specific types of actions can be problematic in terms of the rule of law of information. To this end, the specificity of the type of act can be sought by listing examples such as "deception, destruction, subversion, special operation, etc." and details can be sought by resolving sub-legislation.

4.5. Reviewing the possibility of expanding the counter-intelligence agency

4.5.1. The starting point of the problem

According to the counter-intelligence activity regulations, counter-intelligence agencies are designated as the National Intelligence Service, the National Police Agency, the Korea Coast Guard, and the Military Security Support Command. However, such counter-intelligence organizations can only prepare for typical military and political security, and in the present reality of coexisting with various security threats, restrictions must arise to properly respond to security factors.

4.5.2. Problems to be expected and improvements

Then, if the scope of the counter-intelligence agency is expanded, it should be considered to what extent to which agency to add it. Under the counter-intelligence business regulations, counter-intelligence is essentially for the national interest, and national interest means that it can be threatened by various security threats. Furthermore, counter-intelligence organizations to respond to this will inevitably vary. In other words, interpreting
counter-intelligences regulations in an era of comprehensive security or human security requires all types of acts that may violate national interests and core values of the country to be considered counter-intelligences, as well as those subject to infringement.

If so, the definition of passive anti-spy agencies like this is limited, and the possibility of government departments in various areas such as economic and industrial security, advanced IT technology, munitions acquisition, international crime, and cybercrime should be considered first. In other words, organizations such as the Ministry of Strategy and Finance (DUSTOMS), the Ministry of Trade, Industry and Energy (MOC), the Ministry of Defense (DAPS) should participate in preparing for economic threats, and the Financial Services Commission (Financial Information Analysis Institute) should participate. Of course, the administrative branch itself presented above is not recruited as an anti-spy agency, but it is necessary for affiliated organizations to participate or create (or concurrently) a separate department to engage in anti-spy affairs.

However, criticism could be raised over the expansion of the counter-intelligence agency. First of all, the passive attitude of precedents to the scope of the National Intelligence Service’s job may be problematic. Our supreme court views Article 3 (1) of the National Intelligence Service Act, which sets the scope of the job of the National Intelligence Service, as a restrictive enumeration regulation whether it is an example regulation or a restrictive enumeration regulation [22].

Therefore, if the court’s attitude is maintained, related agencies, not counter-intelligence agencies, will inevitably become passive except for foreign contact management under Articles 7, 8 and 9 of the anti-spy regulations. Aside from the regret over the court’s passive attitude toward the changed security environment, it is necessary to push for a plan to reorganize related agencies into counter-intelligence agencies to overcome the court’s position.

The problem follows the expansion of these sector espionage agencies. Multiple ministries are in charge of espionage because it could lead to confusion in espionage and further following out the espionage. Of course, the National Intelligence Service established a National Defense Strategy Meeting under the National Intelligence Service in November 2018, and the National Intelligence Service established an anti-defense information sharing center to coordinate and control the overall anti-defense operation. However, if the anti-spy information sharing center is actually established, the relationship between the actual authority and the similar information sharing center under the National Intelligence Service (NIS), counter-intelligence business regulations, and anti-terrorism laws can be ignored [23].

In other words, if the scope of the anti-spy equipment is expanded as above, there is a need for revision to improve counter-intelligence operations to end up in a state of concern over confusion in the counter-intelligence operations. Therefore, a higher control mechanism is needed to prevent confusion in counter-intelligence operations. Therefore, it would be possible to consider long-term ways to establish a higher organization such as the U.S. intelligence community to coordinate and control information activities of intelligence agencies as well as counterintelligence operations.

4.6. Specification of means of collection and verification of counter-intelligence intelligence

Counter-intelligence is efforts to protect their intelligence activities both analytically and actively [24]. Therefore, the premise of counter-intelligence is that there is a counter-intelligence target, and it needs to be collected, defended, and attacked [25]. In other words, it is necessary to collect intelligence on forces that undermine national security and produce it as information to evaluate the threat to national security. Then, how to collect such intelligence here and how to determine the reliability and validity of the intelligence collected and produce it as information, and the basis is inevitably required. However, in this study, only the collection of human information is considered, which is a particularly controversial part of HUMINT.
4.6.1. Problems of collecting humint

Human Intelligence Collection (HUMINT) is an information activity that utilizes humans as a means of intelligence gathering, consisting of two pillars: intelligence officer and agent. Intelligence officers need to impersonate themselves so that their status is not exposed in certain tasks, which are divided into heads of public offices and heads of non-public offices. In addition, spies can be classified again as spies who actively recruit intelligence officers to work for intelligence organizations after laying the basis for information activities and cooperators who volunteer to help themselves.

In carrying out specific espionage operations, informants must pretend to be identified, and legal grounds are needed to ensure the salinity and validity of information activities. In addition, legal grounds will be needed for cooperators. The intelligence officer’s status is clear in that he is an employee of the spy agency, and the general intelligence officer has a sufficient review of the agent’s characteristics and purpose by the intelligence officer, and his legal status and credibility are guaranteed to some extent. However, not only is the status unclear, but there is essentially a question of reliability. In addition, it should be considered that spying by cooperators could lead to diplomatic and legal problems in the future.

Therefore, considering the rule of law in espionage, there should be a provision for evidence that anti-spy employees can pretend to be identified in specific tasks, and a stipulation that the credibility of information collected by cooperators can be verified.

4.6.2. Improvement of humint in normative aspects

First of all, it is the best way to improve the status of intelligence officers. Public officials who perform anti-spy duties should not be suspected by the person subject to anti-spy duties, so they need to have a head of status to reach the anti-spy target. In terms of judicial control over espionage, it is not only necessary but also reasonable to stipulate that public officials in espionage agencies can assume the status. This is because the rule of law on information can be applied on the basis of clear grounds for identity theft in the real world, and the possibility of protection for public officials who are in the position of identity can be increased.

Secondly, it is the basis for cooperative management. In order for spy agencies to acquire spy intelligence, it would be the best way for intelligence officers to infiltrate the target and collect intelligence themselves, but the target group that wants to undermine national security is naturally based on closure, so internal cooperators inevitably have great significance.

However, leaving the operation of the cooperator to the judgment of the intelligence officer can result in abuse of the operation of the cooperator, and there is a possibility of reprimanding the judgment of the intelligence officer itself in the event of future problems. Therefore, it is necessary to have a legal basis for intelligence officers to operate cooperators. Similar legislation stipulates that current security business regulations can conduct background checks to investigate loyalty, sincerity, and reliability to the state for national security. This is recognized for its minimal relevance in that the purpose of legislation itself is to carry out security affairs, but it does not prescribe cooperators for those subject to the background check. Therefore, separate legislative measures are required.

To this end, it will be possible to first consider the requirements for the need to operate cooperators and the requirements for supplementation to prevent indiscriminate cooperation. In order to meet these requirements, whether or not the spy service cycle has been met can be the basis for judgment. The use of agents is a general procedure for operating a cooperator, which goes through the process of "targeting – evaluation – recruitment – management – closure".

The use of personal information (especially sensitive information) can be raised because the target selection process includes not only accessibility to that intelligence but also an assessment of the person himself. Articles 15 and 24 of the current Personal Information
Protection Act restrict the collection of personal and sensitive information, but may be treated exceptionally if consent is obtained from the information entity or permitted by law. Therefore, if a basic law to regulate anti-spy affairs is enacted and a stipulation for the operation of cooperators is established, it can be seen as having all the conditions for the cooperative operation system under the legislative system.

Third, it is necessary to verify the reliability of intelligence collected through cooperators. Not only is the information provided by the collaborator itself suspected of being reliable, but there is also the possibility of a double agent intentionally infiltrated by the other party, so the debriefer should doubt the reliability and double agent of the information he provides[26]. In order to verify reliability, an entity may first consider the right to verify facts or request data to be submitted, the review of financial transaction details, etc. In other words, it may be necessary to inquire about public officials or construction organizations and request them to report necessary matters or send documents to them, or to receive information on transactions of financial institutions by a specific person.

The Criminal Procedure Act, which is a follow-up procedure for such matters, prescribes inquiries to public offices, etc. by means of arbitrary investigation. Pursuant to Article 199(2) of the Criminal Procedure Act, an investigative agency may request public officials or other construction organizations to report necessary matters concerning the investigation or execution of a sentence, and in such cases, there shall be no restrictions on matters to be inquired. In addition, Article 4 of the "Act on Real-name Financial Transactions and Secrets" prohibits prosecutors or law enforcement officers from requesting financial institutions to provide transaction information for investigation without the consent or warrant of judges. And such procedures are likely to be viewed as arbitrary investigation[27].

Such procedures are prescribed in the investigation process, but there are currently no such procedures in the pre-procedure of espionage. In the case of espionage, the violation of the law(national security and national interests) has not occurred in reality, but the possibility or risk of infringement is very high, and there is a high possibility of infringement of the basic rights of the people. Therefore, it is necessary to stipulate in the regulations of the law how to verify the reliability of the arbitrary investigation procedures such as the inquiry of public officials, the request for financial transaction information, and the request system for the provision of communication facts[28]. Although the Criminal Procedure Act, the Financial Real Name Transaction and Confidentiality Act, and the Communications Secrets Act may be considered, these laws are basically based on criminal or law violations, so there is room for systematic confusion. Therefore, it is a reasonable choice in the legislative system to prescribe such inquiries, etc. of public offices in the new statutes.

4.7. Block political access to counter-intelligence

One of the most difficult aspects of the academic approach to anti-spy activities in our society was the politicization of counter-intelligence. As the so-called controversy over politicizing information is inevitable, espionage is bound to become an area of intelligence gathering on domestic politics, and some argue that overcoming this phenomenon is the direction of espionage[29]. Of course, this is a recognition from the dark side of Korean society where Korean intelligence agencies were involved in domestic politics, and it is a valid point.

Therefore, the most important issue in improving anti-spy activities in the future is to overcome the politicization of such counter-intelligence and not only institutional improvement but also to form a national consensus.

5. Outro

Forming a new mechanism for internal and external environment is changing rapidly and national security information and conversion is requested aware of. In other words, a new
level of information in the most contentious battlegrounds to say that the era of war. Nevertheless, we stay in the 20th century Cold War is the sense of security incidents and don’t get out of a fixed idea that “anti-espionage = North”. In addition, our overall criminal justice system is still a state that threatens the safety crimes investigation according to a changing global environment, and response system is weak or dictionary. Role of the intelligence agencies or other systematic investigation of efforts for improvements in performance while enjoying a shortfall. Anti-espionage counter new paradigm established in an era of change is now urgently requested.

In response, this study reexamined the current security criminal law system in Korea, especially the current status and problems of the anti-spy business regulations, which are the basis for the performance of anti-spy operations. Based on this, to establish a new anti-spy paradigm in response to the era of transformation, the government highlighted the necessity of enacting a basic law on anti-spy affairs and reviewed specific problems and improvement measures to be included in the law. In summary, the main points are to be replaced by conclusions.

The first is the expansion of the concept and scope of the anti-spy. In other words, if the Framework Act on Anti-Spy is enacted, the concept of anti-spy should be set as an active and active anti-spy concept, not a passive or passive anti-spy concept, to diversify anti-spy operations and respond to both traditional and non-traditional threats. In addition, the government proposed the expansion of spy agencies to cope with the diversification of security threats due to changes in the information environment.

Second, he pointed out existing problems and made some forward-looking suggestions regarding the smooth performance of anti-spy operations. The most important confirmation here is the stipulation of the means of collection and verification of anti-spy information. The method of collecting anti-spy intelligence can be distinguished in legal and realistic ways, and the factual methods such as collecting human information, technical information, and public source information are problematic. In particular, legal grounds and reliability, such as undercovering the identity or operating an informant, are problematic in the intelligence officer’s performance of specific espionage tasks. In order to dispel this, it was confirmed that there was a need to establish a basis that the spy agency could impersonate its identity in specific tasks, a legal basis that the spy agency could operate a cooperative, and a stipulation that could verify the reliability of the information collected by the cooperator.

The last thing I want to emphasize is the establishment of people’s strong will and awareness of national security, and the establishment of consensus on the improvement of the security and criminal justice system in response to the changed times. This is because the ideology and values of liberal democracy that we have achieved through blood and sweat, and the world-class economy, welfare, and happiness can never exist without the Republic of Korea. Therefore, the government should not neglect to establish policies, institutional reform, and strengthen public relations activities to the public.

6. Reference
6.1. Journal article
[4] Kim YK. A Study on Legal/Systemic Modification and Improvement for Effective Counte-


### 6.2. Thesis degree


### 6.3. Books


6.4. Additional reference


7. Appendix

7.1. Authors contribution

<table>
<thead>
<tr>
<th>Initial name</th>
<th>Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td>WP</td>
</tr>
<tr>
<td></td>
<td>- Set of concepts ✔</td>
</tr>
<tr>
<td></td>
<td>- Design ✔</td>
</tr>
<tr>
<td></td>
<td>- Getting results ✔</td>
</tr>
<tr>
<td></td>
<td>- Analysis ✔</td>
</tr>
<tr>
<td></td>
<td>- Make a significant contribution to collection ✔</td>
</tr>
<tr>
<td></td>
<td>- Final approval of the paper ✔</td>
</tr>
<tr>
<td></td>
<td>- Corresponding ✔</td>
</tr>
<tr>
<td></td>
<td>- Play a decisive role in modification ✔</td>
</tr>
<tr>
<td></td>
<td>- Significant contributions to concepts, designs, practices, analysis and interpretation of data ✔</td>
</tr>
<tr>
<td></td>
<td>- Participants in Drafting and Revising Papers ✔</td>
</tr>
<tr>
<td></td>
<td>- Someone who can explain all aspects of the paper ✔</td>
</tr>
</tbody>
</table>