2018 3(1) 1-6
Submission: 2018/05/10, Peer review: 2018/05/20, Accepted: 2018/05/25, Published: 2018/06/30

International journal of justice & law

Publication state: Japan
ISSN: 2423-8767

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

Corresponding author
E-mail: pws7897@naver.com

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

http://dx.doi.org/10.22471/law.2018.3.1.01

Criminal LAW Proposals for the Protection of Industrial Security Technologies in KOREA

Park Woong-shin

Sungkyunkwan University, Seoul, Republic of Korea

Abstract

In this paper, we have examined the issues to be considered for the protection of industrial security technology from a criminal law perspective. Infringement of industrial security technology is a field that can threaten the existence and security of the state as well as impeding national competitiveness, and it is common to discuss it in the national security area. Furthermore, the threat of national security has diversified, and the effective control over industrial security technology is getting more difficult. Therefore, this study distinguishes two important areas to be considered for protection of industrial security technology.

First of all, although industrial security technology belongs to the field of protection, it is confirmed that unconditional protection is moving toward a hyperconnected society, and that there is no reality at the moment. Secondly, it pointed out that criminal punishment is at the forefront of protection of industrial security technology, especially that the creation of new crime should be judiciously cautious. In the concrete criminal procedure, it prevents prevention of intentional leakage of sensitive industrial security technology.

In order to proactively protect the industrial security technology, it is necessary to consider how to institutionalize information sharing among the related organizations involved in the protection of industrial security technology. In addition, the protection of industrial security technology can be limited only by the efforts of the public sector. Therefore, we examined the possibility of utilizing the private investigator. Finally, we assume that the industrial security technology is traded in the dark net, which is newly emerging as a crime market.

[Keywords] ***Justice & Law, Industrial Security, Balance of Protection and Utilization, Dark Net, Symbolic Criminal Law***

1. Intro

Security is an abbreviation of security and means etymological freedom from threats. In particular, national security means that the state, which is a political community, is free from external threats. At one time, there were times when national security itself was perceived as the basic purpose of the state. And there was also a time when such national security was traditionally aimed at securing the nation's existence and security in the military and diplomatic aspects of international relations.

However, with the progress of economicization, globalization, and informationization, it is necessary to make certain changes to the concept of national security. The non-state actors alienated from the international order have not only become the dominant players in international relations due to the progress of globalization and informationization, but also the times when rapid economic development transcends the economic realm within the state, Respectively. Accordingly, the concept of national security has also been changed to a comprehensive security concept[1].

In particular, the industrial security area will be regarded as a security area that is related not only to traditional political and military areas but also to economic areas. In the past, criminal legal interest in the protection of industrial security technology has been relatively insufficient, but the criminal legal response of industrial security technology is also important in that the influence and importance of industrial security technology and the meaning of the technology are highly deteriorated. In this paper, we propose a proposal for the protection of industrial security technology from a perspective different from the conventional one though it is a criminal law view.

2. Industrial Security and Comprehensive Security as a Premise Concept

2.1. Concept of industrial security

The term "industrial security" was introduced to the public in October 2003 when the Center for Industrial Confidentiality was established at the National Intelligence Service and the importance of industrial security was emphasized[2].

In 2006, the “ENFORCEMENT DECREE OF THE ACT ON PREVENTION OF DIVULGENCE AND PROTECTION OF INDUSTRIAL TECHNOLOGY” was enacted, and industrial security technologies and security industries were specified in legal terms. In this context, industrial security in the broad sense can be seen as "any effort to protect all economic activities that produce goods and services from crime"[3].

Conventional industrial security has a wide variety of concept definitions, but generally focuses on preventing industrial technology or leakage of confidential information. However, since the concept of industrial security may lack concrete validity, it is reasonable to consider industrial activities as all kinds of activities that protect all kinds of threats.

2.2. Comprehensive security as a new challenge in industrial security

Traditionally, national security was based on military security. However, due to the end of the ideological confrontation between nations and the rise of non - state actors in accordance with the progress of information and globalization, Conflicts arise due to territorial and economic interests. In other words, the changed international situation calls for a new paradigm of national security. The recent national security paradigm is not focused on traditional ideology or military superiority but threatens and paralyzes the people, territory, sovereignty, Elements also appear as a concept of comprehensive security that can threaten national security[4].

The paradigm of this new security environment is characterized as follows. 1)As discussed above, in the setting up of the concept of security, not only from the military point of view, but also from the non-military elements such as politics, economy, society, environment and technology. 2)The fundamental change of the subject and the threatened object is that the viewpoint of security has changed from the viewpoint of the state-oriented security concept to the center of the individual and the human community[5]. 3)The emergence of transnational threats as a threat to national security is not a conventional concept of a nationality. Transnational threats are characterized by the fact that the source of the threat is done by non-state actors, while the threats by non-state actors are transcended beyond traditional borders. 4)Finally, each country in the world has reached a state where it cannot guarantee the security of the state from the threat of terrorism.

3. Current Proposals for the Protection of Industrial Security Technology

3.1. Balance of protection and utilization of industrial security technology

It is not an exaggeration to say that it is information that supports human society at the present time, which is aiming at a super connective society beyond information society. Now and in the future, in our human society, information will be the object of protection and utilization because the endless goods will

be created from the information. Industrial security technology, which is a problem in the industrial security field, is also a kind of "information", so the industrial security technology also takes a dual role of protection and utilization[6]. Especially, when the violation of various industrial security technologies is reported, our public opinion cannot deny that there is a tendency to protect the industrial security technology and to punish the violation. However, it is because industrial security technology that can directly affect the national security and putting it as a protection area is afraid that it will make a practical use to overthrow the possibility of improvement and legitimate use. The problem is that it is important to open the area of utilization boldly and set the appropriate level of protection necessary for the area of protection.

3.2. Countermeasures against the violation of industrial security technology

Therefore, it is necessary to secure the effectiveness of criminal punishment in order to protect industrial security technology. In other words, the low sentencing rate of violation of industrial security technology, the generous sentence standard, and the area remaining as legitimate gaps in the current law (eg., detecting and collecting trade secrets, criminal punishment for business secret holders due to leakage of trade secrets The problem is that it is argued that the criminalization of criminal cases should be strengthened to protect criminal protection against industrial security technology.

However, it is reasonable to argue that public awareness raises public awareness through the reinforcement of criminal punishment for violation of industrial security technology, but theoretical purity is exploited by various legal external factors(eg., political and social factors) you should be aware that there is room. Especially, in reality, when the sentence of sentencing of the court is low, the symbolic upgrade of the statutory form is likely to make our industrial security legislation a symbolic criminal law[7].

3.3. Protection of industrial security technologies in criminal proceedings

In addition, you should be concerned about the inadvertent leakage of industrial security technology from specific criminal procedures. The current Criminal Procedure Act provides the defendants and lawyers with the right to access and read documents related to the documents or evidence kept during the proceeding, as well as the documents kept by the prosecutor after filing the complaint. In other words, it can be said that the right to acquire such rights as defendant's litigation records is in need of inventory because there is a possibility that industrial security technology, which is a problem in specific facts, is exposed again. In addition, defendants are allowed to have access to the trial records. Of course, these regulations are designed to guarantee defendants' right of defense in criminal proceedings, but it is also necessary to consider restrictions on industrial security incidents and furthermore, when considering the application in national security cases. According to the Criminal Procedure Law, the judge may take protective measures to prevent the disclosure of personal information such as the names of persons involved in the case before the reading or copying when there is a possibility that the safety of the victims. It is considered to be a personal information deletion regulation for the protection of victims[8], but it can be used as a reference for preparing special rules of industrial security technology trial.

Furthermore, it is possible to consider the provision of general provisions to restrict disclosure of inappropriate information(eg., sensitive information such as industrial security technologies such as this one as well as personal information of the victim) to the public in the Criminal Procedure Act.

4. Current Proposals for the Protection of Industrial Security Technology

4.1. Proposal for proactive prevention of industrial security technology – Institutionalization of information sharing of related organizations

It will not be enough to stress the competitiveness of the nation as well as the proactive protection of sensitive industrial security technologies that can be directly linked to survival. Therefore, prevention of industrial security infringement is the best way. It is clear that the responsibility of the investigation agencies, including the National Intelligence Service, which is raised in some areas, is strengthened and the creation of a dedicated organization is effective. However, in a comprehensive security situation like now, protection against other objects of "industrial security technology" object cannot be overlooked at all. In other words, it is not necessary to reconsider the necessity of various related organizations' efforts in the present era where various security risk factors exist. In particular, the historical lessons that the greatest reason for preventing the September 11, 2001 terrorist attacks in the past was the lack of information sharing between investigative agencies and intelligence agencies suggests a direction for us[9]. In other words, an organic information sharing system of related organizations related to industrial security technology is needed[9]. The problem is not abstract information sharing and information sharing by human means but institutionalized information sharing plan[10]. Therefore, a detailed information sharing system on the types of information, types of infringement, threats, and threats to be shared by the relevant organizations such as police, prosecutors, national intelligence agencies, patent offices, It is necessary to plan for maintenance by. The abstract information sharing is likely to be a meaningless echo in reality, and the sharing of information by human cooperation also doubts its continuity.

4.2. Enhancement of private sector capacity to protect industrial security technology

In a comprehensive security situation in which various security threats exist, it is a reality that only national efforts to raise national security and industrial security are limited. Therefore, the capacity of the private sector is also required to correct the limitations of the public sector for enhancing industrial security. To this end, it is possible to come up with a plan to strengthen the security capability at the company level of the industrial security technology, and it is of course the most reliable liability. However, there is a possibility of complementing these organizational / physical security activities, and this is a private research institute system that has been discussed recently.

A private investigator means a system that investigates cases that have been commissioned by others as a private entity, not a public entity such as police or prosecutors[11]. In Korea, discussions on the introduction of civilian investigators have been conducted mainly by the police, but they have been limited in the factual area of so - However, in countries such as the United States and the United Kingdom, the private investigator system has been used for supplementing the public domain and for research and security activities to meet user needs. In other words, if the results of private investigators in these countries meet certain requirements, they will be provided for the benefit of plaintiffs or defendants at trial, or they will be ordered or delegated by the state agency or hired by government agencies to collect evidence on behalf of the public domain[12].

In addition, although the scope of private investigators in these countries is widely recognized, areas such as coping with industrial espionage, coping with copyright and trademark infringement, and investigating patent rights are also recognized[13]. Therefore, Korea should also carefully examine the introduction of civilian capacity, especially the private research institute system, in response to various industrial security risks in the new security situation.

4.3. Tracking and retrieving leaked information – Focusing on Dark net

Industrial security technologies may be violated by specific nations, but may also be violated by non-state actors. In particular, infringement by non-state actors can be assumed to be for the purpose of profit-making after infringement, and darknet is the area where such a market is emerging as the dominant market. Darknets are part of a deep web

that is intentionally hidden and cannot be accessed through a common search engine. Darknet not only protects information from unauthorized access, but also encrypts it to prevent random browsing, thus acting as a platform for Internet users who need to be anonymous. Therefore, it is easy to tempt crime because anonymity is essential, and it can be seen as the type of information circulated on the dark net.

In addition, it is not a centralized Internet site such as Naver, Daum, etc., but it is also characterized by the fact that individual actors open and operate individual sites for their purposes in the depths of the deep web. The biggest feature of Darknets is that they are not able to trade in Darknets once they are connected to Darknets, but they are introduced to the other person before the transactions or they check the creditworthiness of them in various ways[14]. In order to connect to such a dark net, special application represented by TOR(The Onion Router) should be installed[15]. It is difficult to keep track of the user's activity because the TOR protects the anonymity of the user[16] by arbitrarily transmitting the Internet Protocol(IP) address[17]. These darknets are inherently a prime example of criminal activity because of the difficulty of the jurisdiction of the state. It is also possible that the leakage of industrial security technology due to these characteristics will become a means of trading. Therefore, it is required that countermeasures against countermeasures against the distribution of industrial security technology in the dark net and how to recover it should be required.

5. Conclusion

In the above, I have traditionally looked at the issues to be considered for the protection of industrial security technologies from a criminal law perspective.

Infringement of industrial security technology is a field that can threaten the existence and security of the state as well as impeding national competitiveness, and it is common to discuss it in the national security area. Furthermore, the threat of national security has diversified, and the effective control over industrial security technology is getting more difficult. Therefore, this study distinguishes two important areas to be considered for protection of industrial security technology.

First of all, although industrial security technology belongs to the field of protection, it is confirmed that unconditional protection is moving toward a hyper connected society, and that there is no reality at the moment. Secondly, it pointed out that criminal punishment is at the forefront of protection of industrial security technology, especially that the creation of new crime should be judiciously cautious. In the concrete criminal procedure, it prevents prevention of intentional leakage of sensitive industrial security technology.

In order to proactively protect the industrial security technology, it is necessary to consider how to institutionalize information sharing among the related organizations involved in the protection of industrial security technology. In addition, the protection of industrial security technology can be limited only by the efforts of the public sector. Therefore, we examined the possibility of utilizing the private investigator. Finally, we assume that the industrial security technology is traded in the dark net, which is newly emerging as a crime market.

6. References

6.1. Journal articles

[1] Kim HJ. Proposals for the Revision of Laws to Execute Punishment on Spies of Foreign Nationality. *Hankuk University of Foreign Studies Law Review*, 40(1), 61-80 (2016).

[2] Lee CM. A Study on the Conceptual Definition of Industrial Security. *Korean Journal of Industrial Security*, 2(1), 73-90 (2011).

[5] Lee JY. National Security Environment Change and National Crisis & Emergency Management: Typology of National Crisis under the Concept of Comprehensive Security. *Crisisonomy*, 9(2), 177-198 (2013).

[8] Lee SD. A Study on Reformation of Information Protection Regulation of the Crime Victims on the Criminal Procedure Act. *Sungkyunkwan University Law Review*, 24(3), 493-515 (2013).
[10] Park KM & Park WS. A Critical Review on Intelligence Sharing System in Act on Anti-Terrorism. *The Prosecutor*, 57, 383-412 (2017).
[11] Hwang MG. Comparative Legal Study on the Legalization Subsequent Implementation of Private Investaignadtoitrs System in Japan. *Law Review*, 18(1), 271-295 (2018).
[12] Lee HS & Jo HB. A Study on Industrial Security using Private Investigation. *The Korean Association of Police Science Review*, 14(6), 257-281 (2012).

6.2. Thesis degree

[3] Park MR. Sentencing Research on Industrial Security: Focused on Sentencing Guidelines of Unfair Competition Prevention and Trade Secret Protection. Korea University, Doctoral Thesis (2016).
[6] Park WS. A Study on the Personal Information Protection in the Criminal Law. Sungkyunkwan University, Doctoral Thesis (2016).
[7] Lee WY. The Study of Problems and Ways of Improvements in the Assembly Criminal Legislation. Hanyang University, Doctoral Thesis (2012).

6.3. Books

[4] Kurt W. Radtke & Raymond Feddema. Comprehensive Security in Asia. Brill (2000).
[9] National Commision on Terrorist Attacks upon the United State. The 9/11 Commission Report. US Government (2004).
[13] Robert D. McCrie. Security Operations Management. Butterworth Heinemann (2001).
[14] Marc Goodman. Future Crimes: Inside the Digital Underground and the Battle for Our Connected World. BookLife (2016).

6.4. Additional references

[15] http://bgr.com (2014).
[16] http://www.fastcolabs.com (2014).
[17] http://content.time.com (2013).

Author
Park Woong-shin / Sungkyunkwan University Post-Doc
B.A. Sungkyunkwan University
M.A. Sungkyunkwan University
Ph.D. Sungkyunkwan University

Research field
- A Critical Review on Intelligence Sharing System in Act on Anti-terrorism, The Prosecutor, 57 (2017).
- A Study on the Problems and Improvement of the Investigation in the Act on Anti-terrorism, SKKU Law Review, 29(2) (2017).

Major career
- 2017~present. Dongseo University, Lecturer.
- 2017~present. Sungkyunkwan University, Post-Doc.