Industrial Espionage and Police Investigation

Chang-Moo Lee[1]

Department of Police Administration (Criminal Justice), Hannam University
Daejeon 306-791, Korea
jbalanced@gmail.com

Abstract

Industrial espionage has been worsening. Only the tip of iceberg has been identified and moreover a small number of the cases have been prosecuted. To control industrial espionage requires new and stronger countermeasures. Among law enforcement agencies, the police are primarily responsible for preventing and controlling industrial espionage in terms of size and covering area. However, the police have many problems to be solved. The police have few experts on industrial espionage. The lack of budget and insufficient equipment contribute to hinder effective investigation. The lack of coordination among the investigation agencies and the absence of international cooperation system are also regarded as the problems to be solved. For the effective investigation for the police, therefore, it is necessary to train experts on industrial espionage. The special recruitment of outside specialists could contribute to improve the level of police investigation. Securing budget and cutting edge equipment are indispensable for effective investigation. Finally, the police should design a strategy to prove guilty and to prevent the concealment of the illegal gains from industrial espionage.

Keywords: *Industrial Espionage, Industrial Security, Police Investigation, Police Countermeasures, Trade Secret, Industrial Technology*

1. Introduction

In recent years, scientific technology has played a pivotal role in determining the national competitiveness. The economic power of the country is said to depend upon scientific technology. As the importance of scientific technology grows, industrial espionage has emerged as a new threat to many companies as well as the national interest. The industrial technology can be leaked to other countries, which could result in a serious damage not only to the company but also to the entire industry of the country [4]. The economic loss could reach over billions of U.S. dollars, while causing a fatal damage to the competitiveness of the country. Industrial espionage must be a very perplexing problem to be solved. Traditional legal remedies are largely ineffective to protect industrial technology [7, 8].

Industrial espionage has been worsening, in addition, which requires new and stronger countermeasures to control it. Several law enforcement agencies are responsible for preventing and controlling industrial espionage, including the police, the prosecutors' office, and the intelligence agencies. These agencies are playing their specific roles in curbing industrial espionage, while lots of leaking attempts of scientific technology have been

[1] Corresponding author: Chang-Moo Lee, Ph.D

uncovered. With regard to industrial espionage, only the tip of iceberg has been identified and moreover a small number of the cases have been prosecuted.

It is necessary, therefore, to reinforce the law enforcement agencies primarily dealing with industrial espionage. Particularly the police should be changed to meet such needs, since the police occupy the important position among the law enforcement agencies in terms of the size and covering area. There have been, however, few researches to explore such an issue particularly focusing upon the police. The purpose of this study is to identify the problems of the law enforcement agencies dealing with industrial espionage, specially focusing on the police, and to suggest the effective countermeasure of the police for the prevention and control of industrial espionage.

2. The Significance of Police Investigation

2.1. The Strength of the Police for Investigating Industrial Espionage

The police have showed noticeable performances in identifying the cases of industrial espionage. The police recorded 84 cases in 2011, compared to 46 cases of NIS [3]. Such a result can be explained by the scale of the Police in that the Police are operating the largest unit exclusively responsible for industrial espionage among the law enforcement agencies.

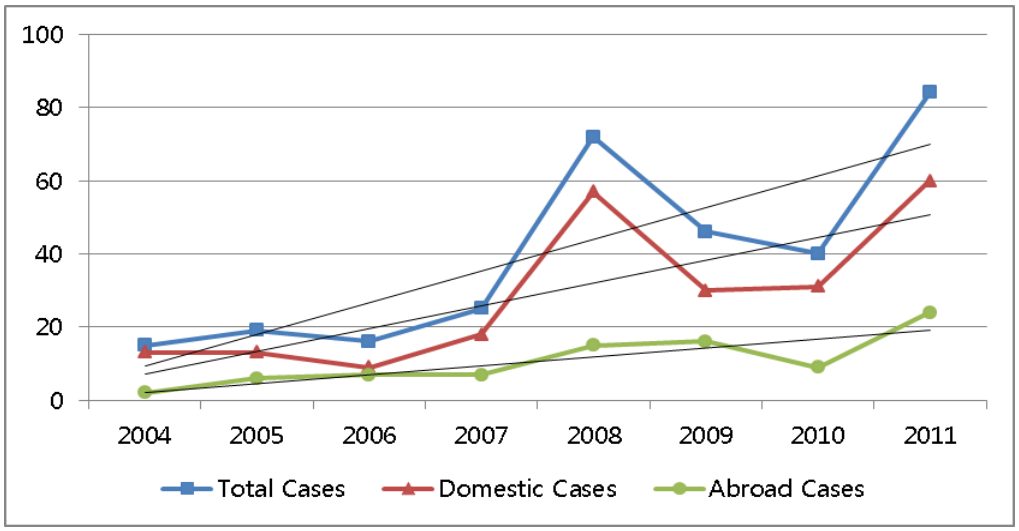
With lots of investigators, thus, the police could operate more easily than other agencies to identify and investigate industrial espionage cases. The police are also operating the investigation by each metropolitan police agency. The 16 metropolitan police agencies nation-wide have special investigation units exclusively covering industrial espionage, while other law enforcement agencies' investigations are concentrated on Seoul and its vicinity area.

Table 1. The Police Arrests of Industrial Espionage

	Total	2004	2005	2006	2007	2008	2009	2010	2011	2012.9
Total Cases	416	15	19	16	25	72	46	40	84	99
Domestic Cases	313	13	13	9	18	57	30	31	60	82
Abroad Cases	103	2	6	7	7	15	16	9	24	17

Source: Korean National Police Agency, 2012.

As shown in Table 1 and Figure 1, the police arrests of industrial espionage have steadily grown since 2004 when the police began to investigate industrial espionage. In 2008 and 2011, however, the police arrests increased rapidly more than two times than 2007 and 2010 mainly due to the expansion of the investigation units. As of September 2012, total arrests recorded 99 that exceeded those of 2011.



Source: Korean National Police Agency, 2012.

Figure 1. Trends in the Police Arrests of Industrial Espionage

The intelligence and foreign affairs section of the police has about 5,000 members which can compete with the NIS in terms of gathering information. The field officers of the section contact with frequently company employees, which would make them get the inside information about the company. These activities might increase the possibilities of identifying industrial espionage, along with an additional crime prevention effect.

The police also have advantageous points with regard to investigation. They have trained investigation experts who are specialized in digital forensics. The recent leakage cases of industrial technology show the characteristics of utilizing electronic devices, which requires digital forensics expertise for investigation. The cyber crime squad of the police has been recognized for its ability using state-of-the-art techniques.

2.2. The Current Police Investigation System against Industrial Espionage

The economic crime squads of each police station had dealt with ordinary leakage cases of industrial technology, while abroad cases had been under the investigation team of the foreign affairs section. Confronted by the problems of redundancy and expertise, the industrial espionage investigation squad was created to deal only with the leakage cases of industrial technology in 5 Metropolitan Police Agencies such as Seoul, Kyunggi, Busan, Incheon, Kyungnam on July 29, 2010, followed by the establishment of the squad in Daegu, Ulsan, Chungbuk Metropolitan Police Agency. There are currently 8 industrial espionage investigation squads operating in South Korea. The Kyunggi squad is the largest with 10 investigators, followed by Seoul and Busan. The industrial espionage investigation supporting team was established under the National Police Agency on February 1, 2011 to coordinate the industrial espionage investigation of the local squads. It plays a role of a control tower.

Table 2. The Police Investigation Units against Industrial Espionage in 2011

Metropolitan Agency	Seoul	Busan	Daegu	Incheon	Ulsan	Kyunggi	Chungbuk	Kyungnam	Total
Number of Investigator	10	8	4	4	3	12	3	3	47

Source: Korea National Police Agency, 2012.

The industrial espionage investigation squads of the Metropolitan Police Agencies have their own specific investigation system according to local industry cluster. For instances, the Seoul squad is specialized in a precision instrument, while the Incheon squad is focusing on automobile, the Kyunggi squad on semiconductors, the Kyungnam squad on shipbuilding, and the Daegu squad on fiber industry.

Since the industrial espionage investigation squad was established, its performance has been said to be positive. First, the period of investigation has shortened from one year to three months because of intensive investigation of the squads exclusively responsible for industrial espionage. Second, the arrests of industrial espionage have rapidly increased from 40 in 2010 to 84 in 2011.

With regard to crime prevention, in addition, the police have maintained a close relationship with companies. The police held a workshop in 2011 on industrial security at which they informed the CEOs of 230 companies operating in China of techniques to prevent the leakage of industrial technology and effective countermeasures as well as local law [3].

The area on which the police place a special emphasis is digital forensics to strengthen the capabilities of the investigation for industrial espionage [9]. The investigation team of the police have little problem in identifying the company which have utilized the technology leaked by industrial spies. However, it is difficult to find evidence of how to leak the secret of the company, which requires the techniques of digital forensics. This is why the police order the investigators of industrial espionage to get the education of digital forensics at least once a year. The police also acquired the budget only for the investigation of industrial espionage, which would be spent for the purchase of digital forensics instrument, the specialization education of investigators, and the building of reporting system.

3. The Problems of the Police Investigation

3.1. The Lack of Experts on Industrial Espionage

Industrial espionage is white-collar crime and hi-tech crime. The state-of-the-art technology is one of the key characteristics of industrial espionage, for which the police need the experts on Information Technology and the inside culture of business. Unfortunately, there are few experts on such areas in the police, which prevent the police from performing effective investigation of industrial espionage. The police investigation of industrial espionage usually relies on the information provided by NIS.

To solve the problem, the police created a course of ‘industrial espionage investigation’ in 2006 and began to have the police investigators get a professional training of industrial espionage including security management, investigation techniques for industrial espionage, evidence gathering, etc. This course has several problems. First, the course is a short term program of only two weeks. The 70 hour training in two weeks is too short to be effective for

the training of the experts on industrial espionage. The expert training for industrial espionage investigation squad was carried out for just one day. Second, the course also has unnecessary programs such as knowledge experience (4 hours) and physical training (4hours) [5]. Finally, the course is open exclusively for the police officers of security and foreign affairs, which blocks an opportunity for the officers of other sections.

3.2. The Budget Crunch and Poor Equipment

The police secured a budget on industrial espionage investigation in 2012 for the first time, but the full amount supported by NIS was cut in the same year. The budget assigned to industrial security was slashed without a plausible explanation. This shows a lack of interest and understanding of the police investigation of industrial espionage. Such lack of understanding is, furthermore, working as a barrier to the development of the police investigation of industrial espionage.

It is suggested that the problem of industrial espionage investigation is attributable to inadequate equipment, particularly digital forensics instruments. It is an outdated method to use external data storage devices such as USB to leak industrial technology. Currently a cellular phone is preferred to leak the information by taking a picture of the file to be leaked appearing on the computer screen [2]. Mobile digital forensics equipment is much more expensive than computer digital forensics one, which makes the purchase of the equipment difficult.

3.3. The Lack of Coordination among the Agencies

As pointed out repeatedly, industrial espionage is hard to be detected and prosecuted because of its expertise and complexity. It is required to have the expert witness to prove a guilty of a suspect. It also takes much time to arrest the person who is responsible for leaking due to the difficulty of detecting the crime. The functions of industrial security to combat leaking secrets are dispersed, which hampers the systematic response to the crime. The duplicated functions also cause unnecessary competition among agencies. Redundancy and inefficiency are the major problems due to the lack of coordination. The insufficient communication among the agencies blocks the interchange of criminal information.

3.4. The Lack of International Cooperation System

There are international agreements protecting trade secrets. They include PCPIP (Paris Convention for the Protection of Industrial Property), TRIPs (Trade-Related Aspects of Intellectual Property Rights) agreements, and NAFTA (North American Free Trade Agreements) [1]. However, these agreements have no legal power to regulate. Thus it is difficult for investigation agencies to deal with leaking trade secrets to other countries in conspiracy with foreigners. It is also hard to recover trade secrets leaked to other countries, subsequently causing a tremendous damage to the company that had the secrets stolen. Although extradition agreement exists between two countries concerned, it is not easy to arrest a fugitive who fled the country. It goes without saying for the persons who fled to the country with no extradition agreement.

4. The Effective Countermeasures for the Police Investigation

4.1. Training of Experts on Industrial Espionage

The investigation of industrial espionage requires a professional and specialized knowledge and expertise. The training of investigators should be, thus, strengthened to meet such a level of expertise. There is only the Police Training Institute which provides training for industrial espionage experts. The training period of 70 hours seems to be short and the curriculum does not provide detailed and professional knowledge on industrial espionage. To improve the ability of industrial espionage investigators, therefore, the expert course of industrial espionage should be changed. It should be elaborated and have more working-level programs including the cases of other advanced countries. The training period should be increased and the investigators should receive commissioned education at the external professional education center including universities and research institutes.

The special employment of outside specialists is also a method to improve the level of industrial espionage investigation. Currently the police are operating the special recruitment program in several areas such as foreign affairs, martial arts, commando, and cybercrime analysis, while there is no program associated with industrial security. Investigation of industrial espionage requires a specialized knowledge and techniques that could not be acquired in a short period of training. That is why the special recruitment of outside specialist is needed for effective investigation of industrial espionage.

4.2. Securing Budget and Equipment

Training of industrial security experts and commissioned education need the increase of budget. Securing necessary equipment also requires budgetary increase. The importance of the police investigation of industrial espionage should be emphasized through various media to attract the attention of the public. Such attention could put a political burden on the national assembly members and the ministry of strategy and finance by which budget could be increased. In the IT environment changing day-by-day, cutting edge equipment such as mobile digital forensics equipment should be acquired for effective investigation. The purchase of such items should be considered as investment to respond to industrial espionage.

4.3. Increasing Efforts to Prove Guilty

The arrest of industrial spies does not guarantee a conviction because of several factors such as the lenient judgment of the court on the cases of industrial espionage and ambiguous definition of trade secret. The police should design a strategy to prove guilty, and also prevent the concealment of the illegal gains from industrial espionage in the process of investigation. Thus the police should study the cases concerning industrial espionage and the trends of the judgments of the court. The Supreme Court decided that trade secrecy must not be recognized to prove misappropriation. Therefore, the police should focus on proving misappropriation rather than trade secrecy. It would be a good strategy to investigate intensively the blameful activity of the suspect to prove trade secrecy, since the court tends to recognize trade secrecy when the suspect's activity is likely to be blamed. In addition, the application of confiscation in the early stage of investigation could prevent the suspect from concealing the illegal gains, and bring about crime prevention effect on the potential criminals.

5. Summary and Conclusion

With regard to industrial technology, prevention is more important than arrest and punishment. The leaks of trade secrets or industrial technology bring about an irreversible damage to the company, since there are few methods to recover the damage and loss. However, the present condition of industrial security could be worrisome. Most of companies do not meet a minimum level of security. Industrial technology is slipping away without knowing the seriousness of the present situation. This provides a pretext for the police to strengthen industrial espionage investigation.

However, the police do not have sufficient experts on industrial espionage. The budget crunch and poor equipment are serious problems to be solved for effective investigation. The police also have troubles in industrial espionage investigation due to the lack of coordination among the investigation agencies and the absence of international cooperation system.

For the effective countermeasures for the police, therefore, it is necessary to train experts on industrial espionage. The special recruitment of outside specialists could be a solution to improve the level of police investigation. This is because specialized knowledge and techniques for effective investigation of industrial espionage could not be acquired in a short period of training. Securing budget and cutting edge equipment are also needed for effective investigation. In addition, the police should design a strategy to prove guilty and to prevent the concealment of the illegal gains from industrial espionage.

Acknowledgements

This paper has been supported by 2012 Hannam University Research Fund.

References

[1] A. Crane, “In the Company of Spies: When Competitive Intelligence Gathering Becomes Industrial Espionage”, Business Horizons, vol. 48, no. 3, **(2006)**, pp. 233-240.
[2] P. Hunton, “A Rigorous Approach to Formalizing the Technical Investigation Stages of Cybercrime and Criminality Within a UK Law Enforcement Environment”, Digital Investigation, vol. 7, no. 3-4, **(2011)**, pp. 105-113.
[3] Korean National Police Agency, Korean National Police Agency 2012 White Paper, Seoul: KNPA, **(2012)**.
[4] C. -M. Lee, “Industrial Security”, Seoul: Pakyoungsa, **(2012)**.
[5] H. -S. Lee, “A Study on the Activation Plan of Industry Security by Police”, The Police Science Journal, vol. 7, no. 1, **(2012)**, pp. 41-61.
[6] NIS (National Intelligence Service), Current Trends in High-Tech Industry Protection, vol. 10, **(2009)**.
[7] H. Snyder and A. Crescenzi, “Intellectual Capital and Economic Espionage: New Crimes and New Protections”, Journal of Financial Crime, vol. 16, no. 3, **(2009)**, pp. 245-254.
[8] W. A. Stadler, “The Quiet Threat: Fighting Industrial Espionage in America”, Security Journal, vol. 25, **(2012)**, pp. 90-93.
[9] O. Thonnard, L. Bilge, G. O. Gorman, S. Kiernan and M. Lee, “Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat”, Research in Attacks, Intrusions, and Defenses, vol. 7462, **(2012)**, pp. 64-85.