


Article

The Perceived Importance of Cybercrime Control among Police Officers: Implications for Combatting Industrial Espionage

Seung-Yeop Paek ¹, Mahesh K. Nalla ², Yong-Tae Chun ³ and Julak Lee ^{4,*} 

¹ Department of Criminal Justice, California State University, East Bay, SF-428, Hayward, CA 94542, USA; seung.paek@csueastbay.edu

² School of Criminal Justice, Michigan State University, 560 Baker Hall, 655 Auditorium Road, East Lansing, MI 48824, USA; nalla@msu.edu

³ Department of Security Management, Kyonggi University, 154-42, Gwanggyosan-Ro, Yeongtong-Gu, Suwon-Si, Gyeonggi-Do 16227, Korea; chunyongtae@naver.com

⁴ Department of Industrial Security, Chung-Ang University, 84 Heukseok-ro, Dongjak-Gu, Seoul 06974, Korea

* Correspondence: julaklee71@cau.ac.kr

Abstract: The current research explored the predictors of how police officers perceived the importance of combatting cybercrime. This is an era in which industrial security is threatened by perpetrators who use advanced techniques to steal information online. Understanding how law enforcement officers view the control of cybercrimes, especially those that steal confidential business information, can inform industrial espionage prevention and help maintain a nation's industrial competitiveness in the world market. We surveyed a convenience sample of South Korean police officers attending training at the Police Human Resources Development Institute (PHRDI) using a paper-and-pencil questionnaire. The results indicated that the officers' perceptions of colleagues' and organizational views on cybercrime control significantly impacted their attitudes. Additionally, officers' perceptions of the seriousness of online theft (in this paper, we use the terms online theft and property cybercrime interchangeably) and their computer proficiency were also found to affect their views on the importance of combatting cybercrimes. We conclude by suggesting that the police take a proactive organizational approach to prevent and respond to online property crimes through education and public awareness programs, which could positively impact the prevention of industrial espionage.



Citation: Paek, S.-Y.; Nalla, M.K.; Chun, Y.-T.; Lee, J. The Perceived Importance of Cybercrime Control among Police Officers: Implications for Combatting Industrial Espionage. *Sustainability* **2021**, *13*, 4351. <https://doi.org/10.3390/su13084351>

Academic Editors: Hwansoo Lee and Lorenzo Ardito

Received: 8 March 2021

Accepted: 13 April 2021

Published: 14 April 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: online theft; cyberespionage; industrial security; officer perceptions; South Korea

1. Introduction

The development of information and communications technologies has presented a formidable challenge to law enforcement and other security governance actors. In particular, cybercrime, a term that covers the offenses targeting both computers and/or networks and those assisted by computer technology [1–3], has become a major social issue over the past couple of decades. With the virtual environment offering myriad opportunities for illegal activities, new offenses such as hacking and malware attacks have emerged [3]. Traditional crimes are now committed by taking advantage of cyberspace's unique characteristics [1,4,5].

Today's industrial espionage can be conducted in various manners. For example, cyberspace is used as a medium through which trade secrets are illegally acquired from domestic companies to benefit international businesses. The virtual environment presents unpredictable risks to industries through increased interconnectedness and the availability of criminal opportunities which are not restricted by spatiotemporal limitations [6–9].

Any industry can fall victim to espionage, but biotechnology, information and communications technology, energy, and defense technology are some of the expected targets. Once a business is victimized, it can wreak havoc at the national level as well. For example,

a 2017 Russian cyberattack which disabled bank, transportation, and company operations worldwide cost FedEx approximately \$300 million [10]. Considering industrial espionage's negative impact on the targeted industry and subsequent damage to a nation's economic and social well-being, it is vital to establish strategic plans to prevent it. In this exploratory research, we aim to suggest prevention and response measures by examining police officers' perceptions of cybercrime control.

The Role of Police

Law enforcement can play a central role in combatting industrial espionage as the main social control agent. For the police to play their roles effectively, understanding the nature and status of industrial espionage is important, but estimating victimization is often difficult due to a lack of reporting by victims [7]. Moreover, current tools for detecting and investigating incidents, especially cyberespionage, are inadequate and have not been tailored to technological evolution [11].

Although existing literature offers insights into protecting intellectual property and trade secrets (e.g., [12,13]), there is little scholarly discourse and empirical evidence concerning industrial espionage policing. Significantly, law enforcement responses to and perceptions of cyberespionage are important research areas that can inform the control of industrial espionage in an era in which cyberspace is a medium for most business and personal activities. Considering that cyberespionage is a type of cybercrime using techniques such as hacking and malware attacks, understanding police officers' attitudes toward these offenses can lay a foundation for effective policing of industrial espionage occurring in the virtual environment. Therefore, this research examines the factors related to the importance that police officers attribute to cybercrime control.

According to the Federal Bureau of Investigation (FBI), a total of 467,361 complaints with an estimated \$3.5 billion losses were filed to the Internet Crime Complaint Center (IC3) in 2019 [14]. Considering the volume of unreported cybercrimes [15], the actual number of offenses committed in cyberspace is expected to be much higher. Based on the trend over the last five years, the number of crimes committed in cyberspace and the resulting financial losses will continue to rise. To commit espionage, techniques such as phishing are often used to lure targets [16]. The European Union Agency for Cybersecurity (2020) reports that around 63% of 2019's cyberespionage cases involved phishing [17]. Because different offense techniques (e.g., malware, hacking, phishing, etc.) can be combined to steal information in cyberspace [18], industries must understand the nature of cybercrime threats to confidential information such as intellectual property.

As the primary responders to crimes, law enforcement is expected to control illicit activities in cyberspace. Because security governance in the virtual environment requires specialized knowledge and investigative skills [19], issues that make policing cybercrime challenging have been noted in the policing and cybercrime literature, including officers' lack of awareness and interest [20,21]. Building on the existing evidence, we explore the factors that predict the importance that police officers attribute to cybercrime control. Since officers who acknowledge the problem's magnitude are more likely to be interested in resolving it [22], the results of this research can inform the practice of preventing and responding to cyberespionage.

2. Issues in Policing Cybercrime

The number of Internet users continues to rise worldwide, with an estimated digital population of 4.6 billion in 2020 [23], constituting nearly 60% of the global population. From the perspective of Routine Activities Theory [24], cyberspace offers appealing opportunities to motivated offenders by allowing them to commit crimes without the need for spatiotemporal convergence with potential victims and guardians [25,26]. This makes it difficult for law enforcement to identify offenders' locations, especially when they can maintain a degree of anonymity [27]. Additionally, emerging offenses aimed at inanimate

objects that utilize advanced technology such as automated vehicles [28] have complicated regulating cybercrimes.

A lack of available resources is another major obstacle to the effective regulation of cybercrimes [29]. This issue is linked to insufficient training and low-level knowledge about these emerging crimes and an inability to keep pace with technological developments and the offenders who have adjusted to them [30,31]. These limited resources and expertise have implications for officers' willingness to engage in cybercrime control. Evidence suggests that officers are not knowledgeable or experienced enough to perform cybercrime investigations (e.g., [32]), and they are reluctant to get involved in them [20].

To enhance industrial espionage countermeasures, Hou and Wang [33] suggest multi-agency collaborations involving private and public sector agencies. For such programs to be implemented successfully, each constituent should make unique contributions [34]. Aside from the need for training and education in public law enforcement, as mentioned earlier, businesses are not willing to report their victimization incidents to protect brand values and shareholders' assets [35]. Without active cooperation from the private sector and businesses involved in industrial espionage, the police cannot take a central role in combatting it. This is especially the case because the police are traditionally expected to handle street crimes, on which a heavy emphasis is placed. Thus, law enforcement duties are prioritized over order maintenance and service [36,37]. It has been found that officers do not support establishing cybercrime units at a local level and are unwilling to receive additional cybercrime training [20].

Furthermore, an element of the police subculture that resists changes and hinders adaptation to evolving environments [38] presents another obstacle for police response to cybercrime. For police to improve their capability of regulating illicit activities in cyberspace, effort must be invested in shifting the organizational focus. In the hierarchical and collective work environment, such change will impact management and line officers' views [39,40]. Studies show that police officers do not believe they should be the primary contact authority for cybercrimes [20,41]. This is possibly due to little emphasis placed on cybercrimes at the organizational level or low self-confidence and lack of preparedness for responding to cybercrime cases [42,43].

Based on the idea that controlling cybercrime lays a foundation for regulating cyberespionage, we assess the factors related to how law enforcement officers perceive the importance of cybercrime control. Understanding officers' attitudes is an essential step for planning, establishing, and implementing programs to combat cyberespionage.

3. Research Method

This research was carried out in the cultural setting of South Korea. The country recorded a gross domestic product exceeding \$1.6 trillion in 2019, ranking 12th globally. The South Korean economy largely relies on exports from industries such as semiconductors, displays, electronic vehicles, and telecommunications [44,45] whose intellectual properties must be protected to maintain the nation's socio-political competitiveness in the world. To combat industrial espionage, the South Korean police enforce the Prevention and Protection of Industrial Espionage Act, the Unfair Competition Prevention and Trade Secret Protection Act, and the Defense Industry Technology Protection Act. Industrial espionage investigators are also cultivated, and the Korean National Police Agency (KNPA) offers training and education courses on industrial espionage [44].

According to the KNPA [46], suspects in 581 industrial technology leakage cases were arrested from 2015 to 2019. Furthermore, a total of 155,554 incidents of information network infringement crime and information network crime were reported in 2019. Given the link between these online offenses and technology leakage, law enforcement must emphasize the property offenses committed in the virtual environment.

Because of the increasing pervasiveness of the Internet and the unique characteristics of online offenses, it is necessary to examine how police officers view cybercrimes. In particular, understanding officers' views on the importance of controlling cybercrime and

the factors that affect their perceptions can inform the practice of educating and training officers in evidence collection and investigation which are critical components of regulating the offenses [47].

3.1. Data Collection

We collected data from a convenience sample of officers attending training at the Police Human Resources Development Institute (PHRDI) in June 2014. The PHRDI is the training hub for officers of all ranks, assignments, and work locations and offers a comprehensive list of programs regularly. Using a paper-and-pencil questionnaire developed based on Bossler and Holt [20] and Holt and Bossler [41], we surveyed participants' views on the importance of policing cybercrimes. We met with each course instructor and informed them about the research purpose, survey distribution, and collection procedures.

The survey questionnaire included a wide range of items related to the perceptions of cybercrime and response strategies. For this research, how participants perceived an organizational emphasis on cybercrime and their attitudes toward their supervisors' and colleagues' views of the importance of cybercrime control were examined. Furthermore, the perceived seriousness of cybercrime and the personal capability of responding to it were explored. After being informed about the research background and ensured anonymity, 433 officers participated in the survey. A total of 362 cases were used for the analysis after 71 cases were deemed unusable due to missing information.

3.2. Measurement

The dependent variable was the perceived importance of cybercrime control. Two items, "conducting a stakeout on the computer is just as important as a traditional stakeout" and "investigating cybercrime is a priority for the police" (Spearman-Brown = 0.54), measured how respondents perceived (1 = strongly disagree; 5 = strongly agree) the importance of controlling cybercrime.

The police are a conservative collectivist organization [38–40]. The profession's chain of command also resembles that of the military, so how other members and the organization view cybercrime control are likely to affect individual officers' attitudes. Therefore, respondents were asked about the emphases their colleagues, supervisors, and organization had placed on cybercrime control (1 = strongly disagree; 5 = strongly agree).

Based on existing research on police officers' perceptions of cybercrime [20,41], officers who view cybercrime to be serious and feel confident about their computer proficiency are more likely to see cybercrime control as a critical task. To measure the perceived seriousness of property cybercrime, participants were shown six offenses (electronic theft of money, identity theft, credit card fraud, virus/malicious software, copyright infringement/piracy, and voice phishing/phishing) and were asked to indicate their seriousness (1 = not serious; 5 = very serious). In addition, computer proficiency was measured by responses to the following two items (Spearman-Brown = 0.65): "I would feel comfortable in working in the cybercrime unit at any time" and "If I receive suitable training, I am confident that I can contribute to cybercrime investigation" (1 = strongly disagree; 5 = strongly agree) (Appendix A).

3.3. Analytic Strategies

We employed Ordinary Least Squares (OLS) as the main analytic strategy. Aside from independent variables (i.e., perceptions of colleagues', supervisors', and the organization's emphasis on the need for cybercrime control, view of the seriousness of property cybercrime, and computer proficiency), socio-demographic characteristics such as gender, education level, and years of experience were included in the OLS model as control variables.

Univariate and bivariate analyses were conducted to examine each variable's characteristics and the independent variables' relationships with the outcome variable. Before proceeding to OLS, Variance Inflation Factor (VIF) values were checked to confirm no multicollinearity among the predictor variables.

4. Results

The vast majority of respondents were male (89%) with an average of 17 years of experience. About a half of participants (51%) held a four-year college degree, and the range of experience was 3 to 34 years with a mean of 17 years. As for views of the importance of controlling cybercrime, participants believed investigating cybercrime was an important task for the police ($\bar{x} = 7.75$), placing considerable emphasis on regulating illicit activities in cyberspace (Tables 1 and 2).

Table 1. Socio-Demographic Characteristics of the Participants.

	<i>n</i>	%	Range	Mean (SD)
Gender				
0 = Female	41	11.5	0–1	0.89 (0.32)
1 = Male	316	88.5		
Education Level				
1 = High school	88	24.4	1–3	2.26 (0.83)
2 = 2-year college	90	24.9		
3 = 4-year college or graduate school	183	50.7		
Years of Experience	362		3–34	17.23 (5.71)

Table 2. Descriptive Statistics of the Variables.

	<i>n</i>	Range	Mean (SD)
Dependent variable			
Importance of cybercrime control	358	3–10	7.75 (1.26)
Independent variables			
Colleagues' view on cybercrime control	361	1–5	3.71 (0.79)
Supervisor's view on cybercrime control	362	1–5	3.44 (0.83)
Organization's view on cybercrime control	356	1–5	3.46 (0.88)
Online theft seriousness	353	10–30	24.46 (3.49)
Computer proficiency	361	2–10	6.30 (1.70)

Respondents believed that their colleagues believed in the need for cybercrime control ($\bar{x} = 3.71$), supervisors showed concern for the need to control cybercrime ($\bar{x} = 3.44$), and the police as an organization placed an equal amount of emphasis on cybercrime as on street crimes ($\bar{x} = 3.46$). Officers also perceived property cybercrimes to be serious offenses ($\bar{x} = 24.46$) and reported a reasonable level of computer proficiency ($\bar{x} = 6.30$).

The bivariate correlation analysis (Table 3) found that each independent variable was positively correlated with the dependent variable. Particularly, the perception of colleagues' beliefs on the need for cybercrime control had the strongest relationship ($r = 0.47$; $p \leq 0.01$) with the dependent variable, followed by the perception of a supervisor's attitude ($r = 0.34$; $p \leq 0.01$) and organizational emphasis ($r = 0.31$; $p \leq 0.01$).

Table 3. Bivariate Relationships between Variables.

	1	2	3	4	5	6
1. Importance of cybercrime control	1					
2. Colleagues' view	0.47 **	1				
3. Supervisor's view	0.34 **	0.62 **	1			
4. Organizational view	0.31 **	0.29 **	0.28 **	1		
5. Online theft seriousness	0.21 **	0.19 **	0.05	−0.001	1	
6. Computer proficiency	0.19 **	0.12 *	0.04	0.10	0.13 *	1

* $p \leq 0.05$; ** $p \leq 0.01$.

According to the OLS analysis (Table 4), the model explained 28% of the dependent variable variance. None of the socio-demographic characteristics were related to participants' perceptions of cybercrime control's importance. On the other hand, except for

the supervisor's view, each independent variable predicted the importance respondents attributed to cybercrime control. How officers viewed their colleagues' ($\beta = 0.33$; $p \leq 0.001$) and the organization's concern ($\beta = 0.33$; $p \leq 0.001$) for controlling cybercrime affected their perceptions positively. Specifically, the more they believed their colleagues and organization showed concern for or emphasized cybercrime, the more they were likely to think that controlling cybercrimes was important. Furthermore, online theft's seriousness ($\beta = 0.15$; $p \leq 0.01$) and computer proficiency ($\beta = 0.10$; $p \leq 0.05$) were positively associated with the perceived importance of cybercrime control.

Table 4. The Perceived Importance of Cybercrime Control Among Police Officers.

All ($n = 307$)		
Variables	B (SE) ¹	β
Gender	0.22 (0.19)	0.06
Education	0.08 (0.08)	0.05
Years of experience	−0.02 (0.01)	−0.07
Colleagues' view	0.52 (0.10)	0.33 ***
Supervisor's view	0.15 (0.09)	0.10
Organizational view	0.25 (0.07)	0.17 ***
Online theft seriousness	0.05 (0.02)	0.15 **
Computer proficiency	0.07 (0.04)	0.10 *
R ² /Adjusted R ²		0.29/0.28

¹ B (SE): Unstandardized coefficient (standard error); β : Standardized coefficient. * $p \leq 0.05$; ** $p \leq 0.01$; *** $p \leq 0.001$

5. Discussion

The current research results suggested that several factors may impact individual officers' views of the importance of controlling cybercrimes. Cybercrimes continue to emerge with the increased use of technology, and cyberspace provides opportunities for committing traditional crimes by taking advantage of the unique virtual environment. Over the past decade, companies and governments worldwide have been targeted by attackers who have used different computer techniques to steal confidential information [48], suggesting the prevalence of cyberespionage.

To respond to the rapidly evolving techniques and sophisticated tools used for industrial espionage, public law enforcement must play a central role as the main social control agent. For the police to effectively perform their duties in this area, understanding how individual officers perceive the importance of controlling cybercrime is critical. Officers' attitudes toward cybercrimes, particularly property offenses, have implications for cyberespionage because officers who accept the problem's importance are more likely to be interested in countermeasures [22].

The current research found that both the perceived views of colleagues and organizational emphasis influenced officers' attitudes toward the importance of controlling cybercrime. The perceived seriousness of online theft and individual proficiency also increased officers' emphasis on fighting cybercrimes, which supported prior research suggesting the influence of officers' perceptions as first responders [20,41,49].

The findings offer the following practical implications for the police in responding to cyberespionage. The KNPA [50] report that there was a total of 3638 cases of network infringement in 2019, which included 2664, 35, and 270 cases of hacking, denial-of-service, and malware attacks, respectively. Based on 112 cases of industrial espionage in the same year and the fact that phishing and other online fraud techniques are commonly used in industrial espionage [16,17], the police should redefine their roles [51] to eradicate industrial espionage along with property cybercrimes, especially those involving cyber-trespass and cyber-deception/theft [52]. A number of scholars have suggested improving industrial espionage-related policing activities, hiring expert personnel, and training officers to enhance skills [53–55].

The recommended measures will eventually help the police participate in cyberspace security governance and cyberespionage control, but a more immediate issue requiring attention is how officers view cybercrimes. Considering the nature of the virtual environment that defies spatiotemporal limitations, solving cyberespionage cases often necessitates interagency cooperation and involves officers performing varying duties at different levels. Therefore, general officer populations must be informed about the relevance of property cybercrimes for industrial espionage. This means organizational effort is needed to help raise officers' awareness and prepare them to handle cybercrimes effectively by establishing clear guidelines and providing sufficient training [42,43].

Additionally, the public must be educated on the seriousness of cybercrimes and the need to control them to prevent industrial espionage. It has been noted that low-level awareness is a major reason for the underreporting of economic cybercrime [51]. Government programs aimed at distributing information about cybercrimes and industrial espionage should be implemented to encourage reporting of suspicious online activities related to cyber trespassing and theft. Posters and billboards containing information about the offenses and the number(s) to call for reporting can be installed in public spaces, and public service announcements could reach many citizens.

The police can emphasize industrial espionage in all officer training. Evidence collection and handling the early stages of cyberespionage, including communication with the units in charge, can improve investigational efficiency and effectiveness. Training should include educating officers on the significance of industrial espionage control and emphasize personal computer efficiency. Lastly, the KNPA can publish reports on cyberespionage statistics. At the moment, there are no statistics to estimate the prevalence of online cybercrimes in industrial espionage cases. Access to such statistics will promote the development and implementation of more practical and relevant strategies.

The results must be interpreted by taking the following limitations into account. Because of the non-probability sampling (i.e., convenience) method used, the results' generalizability is limited. Nonetheless, considering that the PHRDI is the hub for police training and education, it can be argued that the survey participants comprised a national sample. In addition, the cross-sectional survey does not allow us to examine causal relationships between the variables. For instance, officers who feel that controlling cybercrimes is important may be more likely to believe that their colleagues and the police organization also emphasize it. Moreover, those who believe in the importance of preventing and responding to cybercrimes could invest greater effort in improving necessary skills (i.e., personal computer competency) to make a positive contribution. Future research should collect a random sample and employ an analytic strategy that enhances the findings' external validity and allows examination of causal effects to establish clear temporal orders between variables.

Moreover, the time elapsed since data collection could have undermined the validity of findings. We are aware of the social, political, and economic changes that have occurred for the past seven years, including a greater degree of interconnectedness in cyberspace due to the increasing number of Internet users and ongoing advancements in information and communications technologies. These developments have resulted in multiplication of criminal opportunities and diversification of offender modus operandi in the virtual environment. Public law enforcement, however, has not been able to keep up with these changes as recent studies suggest that officers still lack adequate understanding of and skills for combatting cybercrimes [42,43]. In addition to little improvement in policing cyberspace, the police as an organization are slow to adopt innovations and are difficult to reform [38]. Therefore, we believe the data used in this research are not a serious limitation, especially when our goal is to examine officers' perceptions of cybercrime control.

6. Conclusions

We examined the correlates of police officers' perceived importance of controlling cybercrime and its implications for combatting industrial espionage. As the Internet has

become an essential part of everyday business, regulating illicit activities in cyberspace must be prioritized by the police who are the major law enforcement organization in the public sector. To regulate behaviors that could pose threats to a nation's industrial security, the police must acknowledge cybercrimes' seriousness and educate officers accordingly. Although there is extensive research conducted on cybercrime victimization and offending, there is little scholarly discourse of cyberespionage. To fill this gap, we explored the correlates of South Korean police officers' perceived importance of cybercrime control and discussed the implications for combatting industrial espionage.

We suggest that the police invest effort in redefining their missions and rethink how to police illegal online activities. Traditional crimes such as industrial espionage can now be committed online through hacking and malware attacks. Expressing concern about this issue may help shift the organizational focus, stimulating changes in officers' attitudes. Regular training and education programs may also increase officers' awareness and enhance their cyberespionage investigation skills and knowledge. Drawing from the facts that economic losses from cybercrimes continue to rise rapidly [14] and cybercrimes are now employed by politically-motivated offenders [56], countermeasures involving cross-sectoral partnerships should also be considered for effective prevention and response [49]. Furthermore, informing ordinary citizens about the importance of preventing industrial espionage and how it can be committed online and reporting procedures can supplement policies implemented at the organizational and governmental levels. Finally, future research should continue to pursue this line of research and contribute to the literature of policing industrial espionage by investigating the predictors of victimization and measuring the effectiveness of the programs implemented for industrial espionage control.

Author Contributions: Conceptualization, J.L.; methodology, S.-Y.P. and Y.-T.C.; writing—original draft preparation, S.-Y.P., M.K.N. and J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This paper was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0008703).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Measurement of Variables.

Item	Loading
Importance of Cybercrime Control	
Conducting a stakeout on the computer is just as important as a traditional stakeout	0.83
Investigating cybercrime is a priority for the police	0.83
Spearman-Brown	0.54
Kaiser-Meyer-Olkin (KMO)	0.50
Online Theft Seriousness	
Electronic theft of money	0.73
Identity theft	0.81
Credit card fraud	0.82
Virus/malicious software	0.74
Copyright infringement/piracy	0.65
Voice phishing/phishing	0.67
Cronbach's Alpha	0.83
KMO	0.86

Table A1. Cont.

Item	Loading
Computer Proficiency	
I would feel comfortable working in the cybercrime unit at any time.	0.86
If I receive suitable training, I am confident that I can contribute to cybercrime investigation.	0.86
Spearman-Brown	0.65
KMO	0.50

References

- Bossler, A.M.; Berenblum, T. Introduction: New directions in cybercrime research. *J. Crime Justice* **2019**, *42*, 495–499. [CrossRef]
- Furnell, S. Cybercrime: Vandalizing the information society. In Proceedings of the International Conference on Web Engineering, ICWE 2003, Oviedo, Spain, 14–18 July 2003; pp. 8–16.
- McGuire, M.; Dowling, S. Cyber Crime: A Review of the Evidence. Available online: <https://www.justiceacademy.org/iShare/Library-UK/horr75-chap1.pdf> (accessed on 14 January 2021).
- Brenner, S.W. Is There Such a Thing as “Virtual Crime”? *Calif. Crim. Law Rev.* **2001**, *4*, 105–111.
- Brenner, S.W. Cybercrime Metrics: Old Wine, New Bottles? *Va. J. Law Technol.* **2004**, *9*, 1–53.
- Hubbard, T.; Weber, G.L.; Steinhoff, J.C. Protecting data assets in a perilous cyber world. *J. Gov. Financ. Manag.* **2017**, *66*, 26–31.
- Button, M. Economic and industrial espionage. *Secur. J.* **2020**, *33*, 1–5. [CrossRef]
- Newman, G.; Clarke, R. *Superhighway Robbery: Preventing E-Commerce Crime*; Willan Publishing: Portland, OR, USA, 2003.
- Wagner, R.E. Bailouts and the potential for distortion of federal criminal law: Industrial espionage and beyond. *Tulane Law Rev.* **2012**, *86*, 1017–1055.
- National Counterintelligence in Cyberspace. Foreign Economic Espionage in Cyberspace. Available online: <https://fas.org/irp/ops/ci/feec-2018.pdf> (accessed on 27 February 2021).
- Luciano, L.; Baggili, I.; Topor, M.; Casey, P.; Breitingner, F. Digital forensics in the next five years. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; pp. 1–14.
- Hinduja, S.; Ingram, J.R. Self-control and ethical beliefs on the social learning of intellectual property theft. *West. Criminol. Rev.* **2008**, *9*, 52–72.
- Elliott, S.M. The Threat from Within: Trade Secret Theft by Employees. *Nat. Biotechnol.* **2007**, *25*, 293–295. [CrossRef]
- Federal Bureau of Investigation. Internet Crime Report. Available online: https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf (accessed on 15 January 2021).
- Tcherni, M.; Davies, A.; Lopes, G.; Lizotte, A. The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Q.* **2016**, *33*, 890–911. [CrossRef]
- Accenture. 2019 Cyber Threatscape Report. Available online: https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf (accessed on 26 February 2021).
- European Union Agency for Cybersecurity. ENISA Threat Landscape 2020—Cyber Espionage. Available online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage> (accessed on 26 February 2021).
- Holt, T.J.; Bossler, A.M. An assessment of the current state of cybercrime scholarship. *Deviant Behav.* **2014**, *35*, 20–40. [CrossRef]
- Hinduja, S. Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Polic. Int. J. Police Strateg. Manag.* **2004**, *27*, 341–357. [CrossRef]
- Bossler, A.M.; Holt, T.J. Patrol officers’ perceived role in responding to Cybercrime. *Polic. Int. J. Police Strateg. Manag.* **2012**, *35*, 165–181. [CrossRef]
- Lee, J.R.; Holt, T.J.; Burruss, G.W.; Bossler, A.M. Examining English and Welsh detectives’ views of online crime. *Int. Crim. Justice Rev.* **2021**, *31*, 20–39. [CrossRef]
- Skogan, W.G.; Hartnett, S.M. *Community Policing, Chicago Style*; Oxford University Press: New York, NY, USA, 1997.
- Global Digital Population as of October. Available online: <https://www.statista.com/statistics/617136/digital-population-worldwide/> (accessed on 26 February 2021).
- Cohen, L.E.; Felson, M. Social change and crime rate trends: A routine activity approach. *Am. Sociol. Rev.* **1979**, *44*, 588–608. [CrossRef]
- Grabosky, P.N. Virtual criminality: Old wine in new bottles? *Soc. Leg. Stud.* **2001**, *10*, 243–249. [CrossRef]
- Wall, D.S. Policing and the Regulation of the Internet. In *Criminal Law Review*; Walker, C., Ashworth, A., Eds.; Sweet & Maxwell: London, UK, 1998; pp. 79–91.
- Navarro, J.N.; Jasinski, J.L. Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociol. Spectr.* **2012**, *32*, 81–94. [CrossRef]
- Kennedy, J.; Holt, T.; Cheng, B. Automotive cybersecurity: Assessing a new platform for cybercrime and malicious hacking. *J. Crime Justice* **2019**, *42*, 632–645. [CrossRef]
- Goodman, M.D. Why the police don’t care about computer crime. *Harv. J. Law Technol.* **1997**, *10*, 465–494.

30. Hadlington, L.; Lumsden, K.; Black, A.; Ferra, F. A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Polic. J. Policy Pract.* **2018**. [CrossRef]
31. Holt, T.J.; Blevins, K.R.; Burkert, N. Considering the pedophile subculture online. *Sex. Abus.* **2010**, *22*, 3–24. [CrossRef]
32. Bond, E.; Tyrrell, K. Understanding revenge pornography: A national survey of police Officers and staff in England and Wales. *J. Interpers. Violence* **2018**. [CrossRef] [PubMed]
33. Hou, T.; Wang, V. Industrial espionage—A systematic literature review (SLR). *Comput. Secur.* **2020**, *98*. [CrossRef]
34. Dupont, B. Security in the Age of Networks. *Polic. Soc.* **2004**, *14*, 76–91. [CrossRef]
35. Etzioni, A. Cybersecurity in the private sector. *Issues Sci. Technol.* **2011**, *28*, 58–62.
36. Paoline, E.A., III. Taking stock: Toward a richer understanding of police culture. *J. Crim. Justice* **2003**, *31*, 199–214. [CrossRef]
37. Sparrow, M.K.; Moore, M.H.; Kennedy, D.M. *Beyond 911: A New Era for Policing*; Basic Books: New York, NY, USA, 1992; pp. 129–149.
38. Cohen, R. The force and the resistance: Why changing the police force is neither inevitable, nor Impossible. *Univ. Pa J. Law Soc. Chang.* **2017**, *20*, 105–123.
39. Manning, P.K. The police occupational culture in Anglo-American societies. In *The Encyclopedia of Police Science*; Bailey, W., Ed.; Garland Publishing: New York, NY, USA, 1995; pp. 472–475.
40. Waddington, P.A. Police (canteen) sub-culture. An appreciation. *Br. J. Criminol.* **1999**, *39*, 287–309. [CrossRef]
41. Holt, T.J.; Bossler, A.M. Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. *Am. J. Crim. Justice* **2012**, *37*, 396–412. [CrossRef]
42. Bossler, A.M.; Holt, T.J.; Cross, C.; Burruss, G.W. Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness. *Secur. J.* **2020**, *33*, 311–328. [CrossRef]
43. Burruss, G.; Howell, C.J.; Bossler, A.; Holt, T.J. Self-perceptions of English and Welsh constables and sergeants preparedness for online crime: A latent class examining constables' and analysis. *Polic. Int. J.* **2019**, *43*, 105–119. [CrossRef]
44. Lee, S.; Lee, J.; Jung, J. An exploration of the necessary competencies of professional police investigators for industrial espionage cases in South Korea. *Secur. J.* **2020**, *33*, 119–138. [CrossRef]
45. National Intelligence Service. Nation's Core Technologies. Available online: https://www.nis.go.kr:4016/AF/1_5_2.do (accessed on 28 February 2021).
46. Korean National Police Agency. Police Statistical Yearbook 2019. Available online: <https://www.police.go.kr/www/open/public/public05.jsp> (accessed on 31 January 2021).
47. Lee, S.O. A study on the effective method for the prevention of industrial secrets leakage. *Chung Ang. Law Rev.* **2019**, *21*, 39–80.
48. Center for Strategic and International Studies. Significant Cyber Incidents Since 2006. Available online: https://csis-website-prod.s3.amazonaws.com/s3fs-public/210129_Significant_Cyber_Events.pdf (accessed on 28 January 2021).
49. Paek, S.Y.; Nalla, M.K.; Lee, J. Determinants of police officers' support for the public-private partnerships (PPPs) in policing cyberspace. *Polic. Int. J.* **2020**, *43*, 877–892. [CrossRef]
50. Korean National Police Agency. Cyber Safety. Available online: <https://www.police.go.kr/eng/statistics/statisticsSm/statistics04.jsp> (accessed on 27 January 2021).
51. Akdemir, N.; Sungur, B.; Başaranel, B.U. Examining the Challenges of Policing Economic Cybercrime in the UK. *Güven. Bilim. Derg. Int. Secur. Congr. Spec. Issue* **2020**, *2020*, 113–134.
52. Wall, D. Cybercrimes and the Internet. In *Crime and the Internet*; Wall, D., Ed.; Routledge: New York, NY, USA, 2001; pp. 1–17.
53. Cho, H.D. Confrontation Capacity Strengthening Plan about Industrial Espionage in Police. *Korean Assoc. Police Sci. Rev.* **2013**, *40*, 193–213.
54. Lee, H.S. A Study on the Measure of Facilitating Industrial Security by the Police. *J. Korean Assoc. Gov. Stud.* **2012**, *4*, 173–192.
55. Hong, S. A Study on the Police Policy to Counter Industrial Espionage. *J. Inst. Police Sci.* **2015**, *10*, 65–93.
56. Lee, B.; Paek, S.Y. Phishing and Financial Manipulation. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Holt, T.J., Bossler, A.M., Eds.; Palgrave Macmillan: Cham, Switzerland, 2020; pp. 899–916.