International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 09 - Issue 08 || August 2023 || PP. 01-15

Knowledge Development Trajectories of the Cybercrime Identification Domain: An Academic Study Based on Citation and Main Paths Analysis

Fei-Lung Huang[1], Kai-Ying Chen[2], Wei-Hao Su[3]

[1]*College of Management Ph.D. Candidate,*

National Taipei University of Technology,

[2]*Professor of the Department of Industrial Engineering and Management,*

National Taipei University of Technology

[3]*Assistant Professor, Department of Industrial Engineering and Management,*

National Taipei University of Technology

Correspondence: (WEI-HAO SU) jackiesu1969@yahoo.com.tw, Tel.: +886-2771-2171(EXT: 2358)

Abstract: This study explores the development of cybercrime research by conducting main path analyses. Cybersecurity and cybercrime are ever-growing global concerns, and the key message from many of the relevant authorities is that we are a long way from a cyberspace that is trustworthy or secure. Studies were selected from the Scopus database, and the Main Path software was used to analyze the trajectory of cybercrime research. The most influential journals were selected according to their *g*-indices and *h*-indices. Studies with identical topics were then grouped into clusters. Wordle was used to identify the keywords in each cluster that were presented in a word cloud and serve a reference for cluster naming. The five largest clusters were "effect of the routine activity theory on cybercrime," "effect of police–community partnerships on cybercrime," "effect of network communication technology on cybercrime," "effect of Internet users' concept of security on cybercrime," and "effect of write print identification technology on cybercrime." Thereafter, the trajectories of each cluster were identified, and suggestions for future research were provided.

Keywords: information security; cyber security; citation analysis; cluster analysis; computer crime; cybercrime; main path analysis

1. Introduction

The Internet provides tremendous convenience. However, online anonymity has given rise to cybercrime, which is much more difficult to manage than conventional crime. Cybercrime can manifest in many forms, such as selling prohibited items, hacking, spreading viruses, and committing fraud. Many studies have been conducted to identify cybercriminal patterns. This study employed a main path analysis to comprehensively review cybercrime studies and explain the evolution of cybercrime and trends in cybercrime research.

A literature review was conducted to analyze the trajectory of cybercrime studies. A main path analysis and a cluster analysis were performed to achieve the following goals:

1. Clarify the trajectory of cybercrime studies through a main path analysis and identify relevant studies on cybercrime in various periods.
2. Identify the key topics of cybercrime studies through a cluster analysis.
3. Identify the differences in cybercrime research and key topics between various periods.

1.1. Identifying Core Academic Literature

1.1.1. Cybercrime

Cybercrime refers to any harmful online behaviors that violate the law through programming, encryption, and decoding. These harmful behaviors include selling prohibited items, hacking, spreading viruses, and committing fraud. Cybercrimes are committed for many reasons. Many crimes have a profit motive, and cybercrime provides greater benefits with fewer risks. Moreover, cybersecurity and data protection measures have lagged behind the rapid development of the Internet and information and communication technology. People also only see the benefits of the Internet and often overlook security concerns. Finally, lawmakers have not enacted timely and effective regulations against cybercrime. Current legal systems have failed to properly address cybercrime despite the need to create appropriate litigation systems.

1.1.2. Types of Cybercrime

Cybercrime is complex and diverse. One common type of cybercrime is selling prohibited items; cybercriminals can easily exploit online, impersonal transactions [1]. Many items sold on the Internet are prohibited or restricted, such as bootleg software, forged documents, weapons, stolen goods, and drugs. Another type of cybercrime is cyber fraud. Cybercriminals can create dummy accounts and trick consumers into transferring money for unusable or nonexistent goods. Some criminals use counterfeit credit cards to defraud online authorizations, whereas others charge fees for services that were originally free. Additionally, hacking is a major cybercrime. Cybercriminals can destroy a network's firewall; illegally invade websites, homepages, or email accounts; and open encrypted or unencrypted files to steal or leak files. Some hackers directly harm their victims through threats and extortion. Cybercriminals can spread aggressive or destructive computer viruses over the Internet to damage other computer facilities and files or, in extreme cases, paralyze an entire network, resulting in massive economic losses. Finally, cybercriminals can violate personal privacy, often by selling personal data or surveilling users' online activities.

1.1.3. Cybercrime Prevention Strategies

Appropriate and timely strategies are required for preventing cybercrime. Criminal legislation against cybercrime must be improved and account for the openness of the Internet and the covert nature of cybercrimes. Cybercrime must be accurately defined and related regulations must be stipulated. Cyberattacks against the government or society, malicious online sabotage, and online financial attacks must be punished. Moreover, cybercriminal legislation must protect the legitimate rights and interests of Internet users and prevent and punish cybercrime. Network defense technology (e.g., encryption, authentication, network monitoring, and security inspection) and equipment (e.g., routers, firewalls, and servers) must be improved through research, development, and investment. Network user management must be strengthened to enhance the defensive capacity of a network, and network security protection and supervision systems must be reinforced to prevent users from committing cybercrimes. Such systems can be strengthened by improving file backups, creating a warning system for network intrusions, performing regular security checks, and mitigating the abuse of security loopholes. Cybersecurity can also be strengthened by reinforcing international judicial exchange and collaboration. However, countries differ in their legal norms, ethics, values, and ideologies on cybercrime. Thus, countries also differ in their standards for cybercrime. The legal system and moral education related to the Internet must also be strengthened. Cybercrime cases must be discussed openly, and Internet users must be educated on the values, everyday use, and social norms of the Internet. Such actions can improve users' online behavior and self-discipline and reduce the probability of cybercrimes

1.2. Literature on Main Path Analyses

Many studies have conducted main path analyses or key-route main path analyses for a literature review on science or technology. Verspagen; Fontana *et al.* [2]; and Consoli and Mina [3] employed main path analyses to identify the trajectory of technology. Bekkers and Martinelli [4] and Lucio Arias and Leydesdorff [5] conducted a main path analysis to investigate changes in technology. Bhupatiraju *et al.* [2]; Calero Medina and Noyons [6]; Colicchia and Strozzi [6]; Harris *et al.* [8]; Chuang *et al.* [9]; Yan *et al.* [10]; and Su *et al.* [11] performed main path analysis to review literature in various disciplines. Li [12] conducted a main path analysis to simplify a massive number of patent verdicts. Li [13] also performed a main path analysis to identify key verdicts and observe trends in patent rights abuse from 1916 to 2016.

2. Materials and Methods

2.1. Data Source

In this study, a search was conducted on Scopus by using the keyword "cybercrime" on January 31, 2021. A total of 4261 articles were identified. Studies were removed if they were duplicates; had unknown authors; or had missing data for the authors, title, and year of publication. Ultimately, 4126 studies were analyzed.

2.2. Main Path Analysis

A main path analysis is used to process large quantities of cited data and investigate trends in an academic discipline. The main path is the largest weight of several paths from the literature source vertex (i.e., the start vertex) to the convergence vertex (i.e., the end vertex). The three most common methods for calculating the main path are the search path count (SPC), search path link count (SPLC), and search path note pair (SPNP). According to the suggestion by Liu and Lu [9], the present study applied global main path and key-route main path analyses in an empirical literature review and revealed that SPLC was superior to both SPC and SPNP in identifying knowledge diffusions in the main path analysis. In SPLC, one path from a network is selected, and the number of possible paths from the source vertex to the end vertex in the path is calculated. Thereafter, the

number of possible paths from the end vertex of the selected path to the convergence vertex is calculated. The product of the two calculations is then found and used to identify the weight of all the possible paths (Figure 1).

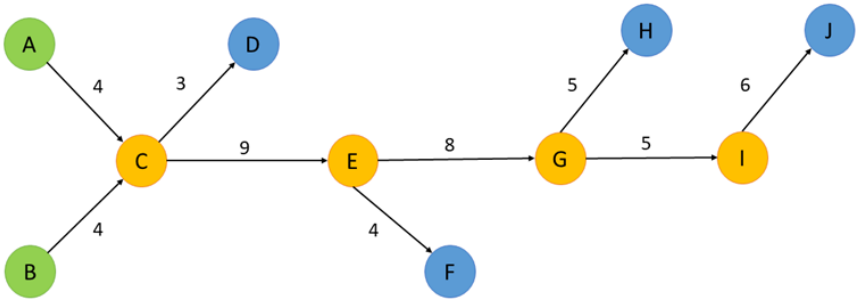


Figure 1 Weight calculation in SPLC.

2.3. Basic Statistics Analysis of Journals and Authors

The statistics for the journals and articles aggregated from Web of Science were exported. The journal statistics included the journal names, publication periods, and journal *g*- and *h*-indices. The author statistics included the author names, publication periods, and author *g*- and *h*-indices.

The *g*-index is the highest number of citations that a study received with a minimum of g^2 times. The *h*-index indicates that *h* of all the studies that an author has published were cited no fewer than *h* times.

In this study, the *g*-indices were given higher priority than the *h*-indices when evaluating the impact of the journals on the academic field and the contributions from authors. Consequently, the 20 most influential journals and the 20 most influential authors on cybercrime research were identified.

2.4. Growth Curve Analysis

The cumulative number of crime prevention studies on Scopus was determined and subsequently imported into Loglet Lab 4 to create a prediction curve for the growth of crime prevention studies. The *y*-axis was the cumulative number of crime prevention studies published, and the *x*-axis was the publication year. The curve was used to predict the development stages of crime prevention research.

2.5. Cluster Analysis

A cluster analysis was performed to divide the studies into clusters based on their characteristics or discipline. Each cluster was named according to the keywords. Edge-betweenness clustering was performed according to the following steps:

1. Calculate the betweenness in the network. Select two random nodes. The total number of shortest paths that pass through the two nodes is the number of edges between the two nodes.
2. Remove the paths with the highest betweenness.
3. If one or more clusters are separated from the citation network, calculate the modularity of the clusters. If no clusters are separated, repeat Steps 1 and 2 until all the paths are removed. Modularity is then used to compare the strength of the correlation between the nodes within a cluster and between clusters.
4. Identify the clustering with the highest modularity (i.e., the optimal clustering).

2.6. Data Mining

The content of each cluster title was imported into Wordle to calculate the frequency in which each word appeared in a large body of text. The results were incorporated in a word cloud, and the prepositions and definite articles were excluded. Thus, the frequency ranking of relevant keywords in each cluster was obtained, and each cluster was named according to its keywords.

3. Results

3.1. Data Statistics

On December 31, 2020, 4261 studies were retrieved from Scopus. Studies were removed if they were duplicates; had unknown authors; or had missing data for the author names, title, or year of publication. Ultimately, 4126 studies were analyzed.

Microsoft Excel was used to organize the individual number of annually published studies and the cumulative number of annually published studies from 1998 to 2021 (Figure 2). The blue and orange bars in Figure 2 represent the individual and cumulative numbers of annually published studies, respectively. The number of cybercrime studies increased at a slow annual rate from 2000 to 2010, after which hundreds of studies were

published each year. The individual number of publications peaked in 2019. Thus, cybercrime studies have developed gradually, and these studies have recently garnered widespread attention.

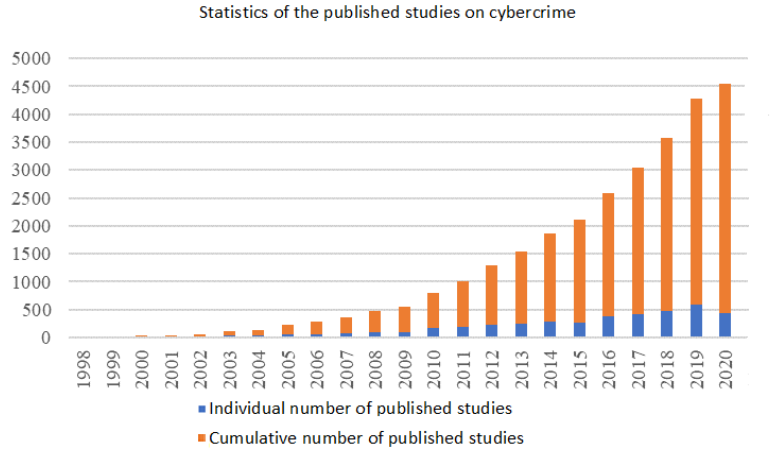


Figure 2 Bar chart on the cumulative growth of published cybercrime studies.

3.1.1. Crime Prevention Journals

The *g*-indices were used to identify the 20 most influential journals on cybercrime research. The journals with equal *g*-indices were ranked according to their *h*-indices (Figure 3). The most influential journal on cybercrime research was *Computers and Security*, followed by *Digital Investigation*, *International Journal of Cyber Criminology*, *Deviant Behavior*, and *IEEE Security and Privacy*.

Computers and Security is currently considered the most integrated and authoritative journal on cybercrime research. The journal addresses the needs of managers and experts in cybersecurity by publishing studies from professionals and scholars and providing suggestions for management.

Digital Investigation primarily publishes research based on cybercrime data analyses. The *International Journal of Cyber Criminology* is an international nonprofit journal that focuses on research on cybercriminal behavior and cybercrime prevention strategies. *Deviant Behavior* provides comprehensive research findings on criminal behavior. *IEEE Security and Privacy* publishes practical and theoretical insights on cybersecurity and privacy in addition to case studies on information security.

g-index Rank	Journal	Total papers	Papers after 2000	g-index	h-index	Active years
1	Computers And Security	38	36	31	14	1998~2020
2	Digital Investigation	34	34	24	13	2004~2019
3	International Journal Of Cyber Criminology	59	59	20	12	2012~2020
4	Deviant Behavior	19	19	19	8	2009~2020
5	Ieee Security And Privacy	31	31	19	10	2003~2019
6	Lecture Notes In Computer Science	91	91	19	11	2003~2020
7	Network Security	35	35	18	6	2002~2020
8	Crime, Law And Social Change	18	18	17	11	2000~2020
9	Ieee Access	17	17	15	8	2016~2020
10	Computer Law And Security Review	34	34	14	7	2009~2019
11	Computers In Human Behavior	13	13	13	8	2014~2020
12	Computer	24	24	13	7	2012~2018
13	Ecrime Researchers Summit, Ecrime	16	16	13	5	2011~2019
14	American Journal Of Criminal Justice	11	11	11	7	2012~2020
15	Acm International Conference Proceeding Series	59	59	11	5	2008~2020
16	Lecture Notes Of The Institute For Computer Sciences, Social-Informatics And Telecommunications Engineering	13	13	11	5	2009~2012
17	Policing	12	12	11	3	2006~2020
18	Cyberpsychology, Behavior, And Social Networking	10	10	10	7	2011~2018
19	Journal Of Contemporary Criminal Justice	10	10	10	7	2010~2020
20	Computer Fraud And Security	45	45	10	5	2002~2020

Figure 3 Top 20 journals for cybercrime research.

3.2. Academic Literature and the Overall Development Trajectory of Cybercrime

Figure 4 illustrates the global main path analysis results on cybercrime studies. The green and blue nodes represent the source and convergent vertices of the studies, respectively. Each node represents a study and is connected to another node by an arrow, which indicates the direction of knowledge flow. Each node features a string of text codes that contain the first uppercase letter of the first author's and corresponding authors' names and numbers representing the year of publication. Studies with the same uppercase letters and numbers are distinguished and sorted using lowercase letters in alphabetical order.

The global main path is the path with the highest total weight in the citation network and features 10 nodes, which are described in this section.

According to Kshetri [14], cybercriminals, cybercrime victims, and law enforcement agencies mutually reinforce each other, which results in a vicious cycle of cybercrime. In that study, a cost–benefit analysis on cybercrime was performed from the perspectives of the victims and perpetrators to clarify the motivations of

cybercriminals. Suggestions were provided to prevent Internet users from being targeted by hackers. Gordon and Ford [15] explored the breadth of cybercrime and defined both cybercrime and crimeware. Two types of cybercrime were classified, namely technical cybercrime and cybercrime with a more human element. Two case studies were examined to explain the use of crimeware in both types of cybercrimes.

Van Wilsem [16] examined the latent factors for digital and conventional crime. Previously, routine activity theory was applied to associate both cyber activities and outdoor activities with digital and conventional crime, respectively. However, an examination of the investigation data from victims revealed that activities in real life and the virtual world are interconnected. At the time of the study, the routine activity theory required verification by using new methods to ensure its credibility and use in relevant research. Van Wilsem explored the latent factors for hacker attacks and the relationship between hacker attacks and cyberbullying. The results suggested that low self-control among users is a latent factor for hacker attacks. Moreover, the cumulative number of cases of users falling victim to both digital and conventional crime has increased. According to Williams [17], cyber fraud is currently the most prevalent form of crime in Europe. This finding was based on an analysis that used routine activity theory to investigate cyber fraud and online identity theft.

According to Leukfeldt [18], Internet forums are hotspots for cybercriminals, and more attention should be given to the ability for cybercriminals to meet and develop cybercriminal networks. Moreover, the effect of cybercriminal networks on the cybercriminals' capability to commit crime requires further investigation. Leukfeldt argued that social ties play a critical role in the origin and development of most criminal networks, and such ties are often forged on Internet forums. Bijlenga [19] conducted five case studies in the Netherlands to explore how cybercriminals use their expertise in information and communication technology to commit crimes.

Expanding on the findings by Bijlenga [19], Kruisbergen [20] analyzed the use of information technology by organized criminals to launder money and investigated the financial expenditures and revenues for both conventional and digital crimes. The results revealed that criminals strongly prefer cash and often convert digital currencies into cash for transactions. Weulenkranenbarg [21] conducted a comprehensive study on hackers in non–English-speaking countries such as the Netherlands and analyzed the personal characteristics of hackers, their social networks, and their motives for committing crimes. Lavorgna [22] contended that cybercrime and organized cybercrime must be distinguished by using more accurate terms.

The global main path revealed the trajectory of mainstream cybercrime research. The source vertex indicated that early studies on cybercrime focused on common types of cybercrime, whereas later studies examined the correlation between the behaviors of cybercrime victims and their likelihood of becoming victims. Since 2017, studies have focused on the use of communication technology in various cybercrimes.

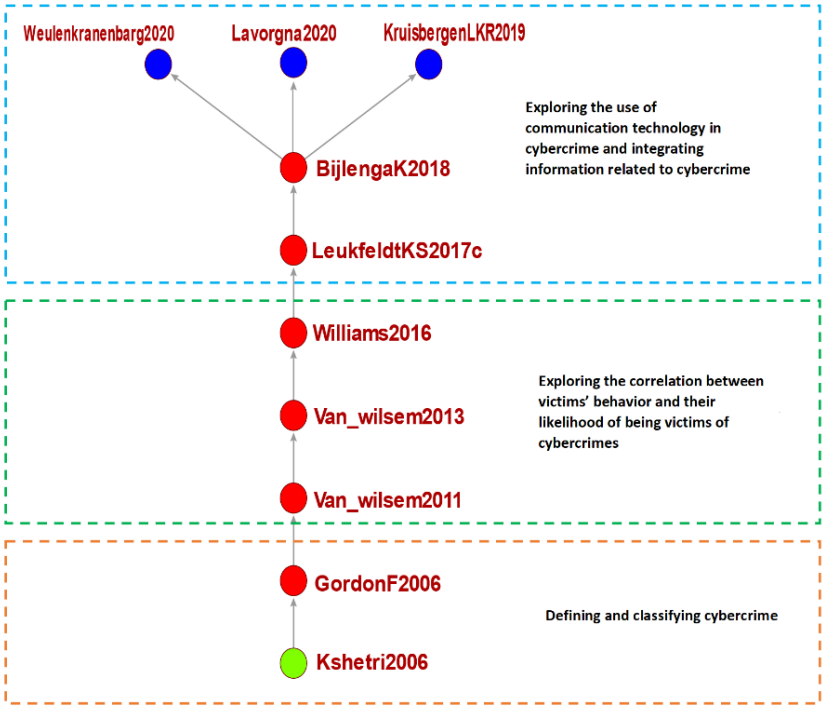


Figure 4 Global main path.
Figure 4 The relational diagram for the global main path of academic studies

4. Discussion

4.1. Development Trajectory of Cybercrime and Clusters

Because the global main path alone does not provide a comprehensive view of cybercrime research development, a key-route main path analysis was created to identify influential studies that may have been overlooked. As shown in Figure 5, the interrelationship between multiple paths revealed the development trajectories of cybercrime research across various periods.

A total of 17 studies were identified on the key-route main path. As demonstrated in Figure 5, all 10 studies on the global main path (Figure 4) were also included on the key-route main path, indicating that most of the studies on the global main path influenced cybercrime research considerably. Seven of the studies on the key-route main path were not found on the global main path. The seven studies are briefly described in the following.

Grabosky [23] argued that although digital and computer communication technology has brought more convenience, it has also provided opportunities for crime. Therefore, Internet users must possess knowledge on cybercrime to lower their likelihood becoming victims.

Choo [24] investigated how conventional organized criminals, organized cybercriminals, and politically and ideologically organized criminals use information and communication technology to break laws and monitor the Internet. The results indicated that as digital technology becomes more prevalent, evidence collection and handling procedures by law enforcement officers have become increasingly complicated. New policies must be enacted to contain criminal behavior, and more comprehensive research is required on online organized crime.

According to Choo [25], because criminals are eager to obtain personal and confidential information from Internet users, they are willing to resort to extreme measures, rendering cybercrime even more complicated than before. The routine activity theory was applied to devise measures for investigating and punishing cybercrime and reducing the likelihood of cybercrime where possible.

Since 2016, cybercrime studies have applied routine activity theory. Leukfeldt [26] examined whether this theory could be used to analyze cybercrime. Therefore, Leukfeldt explored the effects of values, visibility, accessibility, and Internet surveillance authority in cybercrime cases on cybercrime victimization. The results revealed that visibility is a critical factor for cybercrime victimization, whereas the other three factors are not significantly correlated with victimization.

Howell [27] examined whether the routine activity theory could be used to analyze website defacement by testing the relationship between the structural characteristics of a given country and the frequency of website defacement in that country. The results indicated that countries with greater Internet surveillance authority were less likely to experience website defacement. Howell also analyzed the effect of Internet surveillance authority on political and recreational website defacement and found that although recreational website defacement is significantly affected by Internet surveillance authority, political website defacement is not.

Howell [28] recorded data of various cybercrimes to provide a reference for future research and focused particularly on hacker attacks. Howell also recorded which studies used the cybercrime data and examined the advantages and limitations of such data. Such information can enable future studies to clarify the relationship between patterns of cybercrime victimization and the macroscopic framework of cybercrime.

Penkins [29] used data from multiple sources to assess whether the routine activity theory could be used to explain national malspam attacks. The results revealed that corruption, political freedom, gross domestic product, and Asian countries are significantly correlated with a high number of malspam victims. However, Internet monitoring authority increased the frequency of malspam attacks. The study provided a theoretical and policy discussion on the phenomenon.

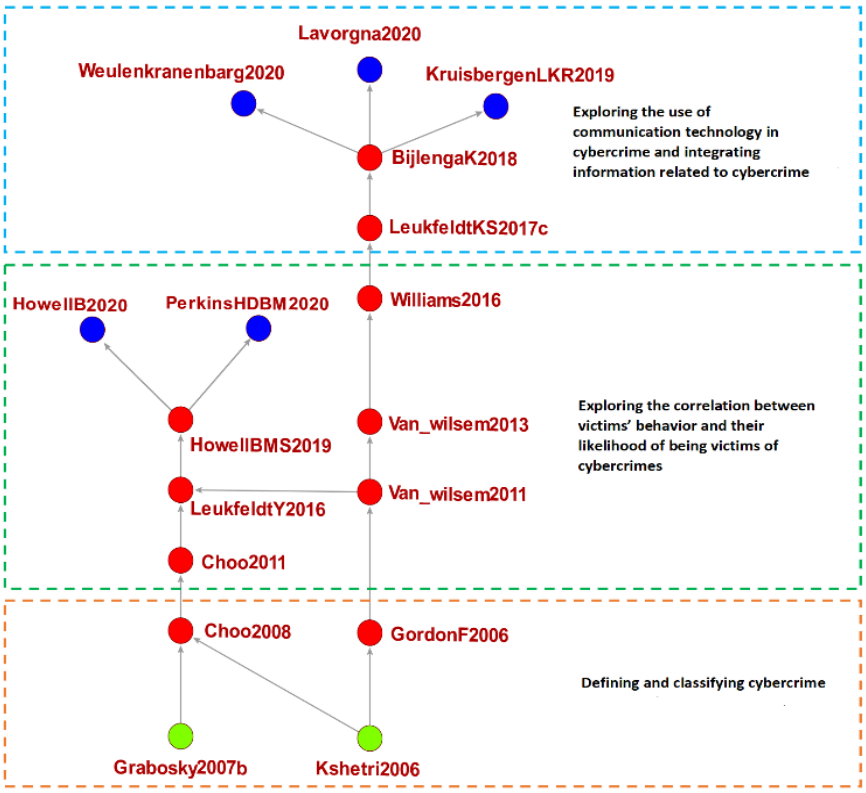


Figure 5 Key-route main path

4.2. Cluster Analysis on Cybercrime Studies

After the global main path analysis, the cybercrime studies were divided into 20 clusters to identify the key research topics. The titles of the five largest clusters were entered in Wordle to obtain the keywords. The five clusters were named "effect of the routine activity theory on cybercrime," "effect of police–community partnerships on cybercrime," "effect of network communication technology on cybercrime," "effect of Internet users' concept of security on cybercrime," and "effect of writeprint identification technology on cybercrime."

Figures 6 presents the information related to the five clusters. The information consists of the research topic, number of studies, keywords, trajectory, and word cloud. In the table, keywords are listed sequentially according to the frequency of their appearance in the cluster titles, and the numbers in the parentheses represent their average frequency. For example, in the first keyword in the first cluster, "Routine (0.20)," the keyword "routine" appeared in titles 0.20 times on average. Keyword sequencing can clarify the research trends of each cluster. According to the research trajectory diagram, all five clusters suggested that the number of publications for each research topic increased.

Figures 6 lists the information related to the five clusters, including research topic, number of studies, keywords, trajectory, and word cloud. Keywords are listed sequentially according to the frequency of their appearance in the cluster titles, and the numbers in the parentheses represent their average frequency. For example, in the first keyword in the first cluster, "Crime (0.33)," the keyword "crime" appeared in the titles 0.33 times on average. Keyword sequencing can clarify the research trends of each cluster. According to the research trajectory diagram, all five clusters suggested that the number of publications for each research topic increased.

The studies were further analyzed to determine the main path in each cluster and identify the research trajectory on each main path (Figures 7–11).

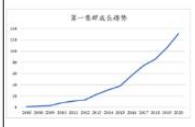
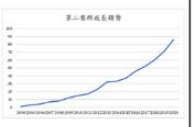
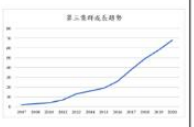
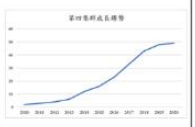
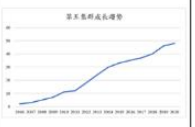
RESEARCH TOPICS	First cluster (131 studies) Effect of the Routine Activity Theory on Cybercrime	Second cluster (86 studies) Effect of Police–Community Partnerships on Cybercrime	Third cluster (68 studies) Effect of Network Communication Technology on Cybercrime	Fourth cluster (49 studies) Effect of Internet Users' Concept of Security on Cybercrime	Fifth cluster (48 studies) Effect of Writeprint Identification Technology on Cybercrime
1	Routine (0.20)	Cybercrime (0.20)	Networks (0.14)	Security (0.27)	Writeprints (0.14)
2	Activities (0.15)	Policing (0.20)	Cybercrime (0.14)	Users (0.13)	Approach (0.14)
3	Examining (0.10)	Partnerships (0.13)	Social (0.14)	Cyber (0.13)	Authorship (0.14)
4	Theory (0.10)	Software (0.07)	Phishing (0.14)	Study (0.07)	Supervised (0.14)
5	Cybercrime (0.10)	PPPs (0.07)	Virtual (0.07)	Education (0.07)	Interactive (0.07)
6	Victimization (0.10)	Policing (0.07)	Study (0.07)	Industry (0.07)	Empirical (0.07)
7	Malware (0.10)	Empirical (0.07)	Convergence (0.07)	Information (0.07)	Language (0.07)
8	Valuations (0.05)	Source (0.07)	Digital (0.07)	Research (0.07)	Forensic (0.07)
9	Assessing (0.05)	Approach (0.07)	Organized (0.07)	Organisations (0.07)	Mining (0.07)
10	Datasets (0.05)	Space (0.07)	Exploratory (0.07)	Challenges (0.07)	Identification (0.07)
Developmental Trajectory					
Word cloud					

Figure 6 Research topics

4.2.1. Effect of the Routine Activity Theory on Cybercrime

The first cluster featured 131 studies on the routine activity theory. As depicted in Figure 7, the main path consisted of eight studies published from 2005 to 2020 that explore the effect of the routine activity theory on cybercrime.

Yar [30] examined whether the theory is applicable to cybercrime; however, the study identified problems related to the theory's practicality. Therefore, Holt [31] examined cyber harassment to further explore the effect of routine activity theory on cybercrime.

Reyns [32] applied the routine activity theory to analyze cyberstalking and revealed that online exposure to risk, online proximity to motivated offenders, online guardianship, online target attractiveness, and online deviance are key factors for cyberstalking. According to Holt [33], studies on malware have been scant. Therefore, the study examined malware victimization by using various type of crime detection methods and the routine activity theory. Holt [34] collected data from an open database for malware infection and applied the routine activity theory to examine the relationship between malware attacks and a country's digital and political infrastructure. The results revealed that countries with high-tech infrastructure and political freedom are particularly vulnerable to malware attacks. Howell [27], Howell [28], and Perkins [29] investigated the relationship between victim behavior and the likelihood of victimization. In the present study, all three studies were on the key-route main path, indicating that they influence cybercrime studies considerably.

Figure 7 illustrates how studies published from 2005 to 2009 explored the practical limitations of the routine activity theory, whereas studies published from 2011 explored the applicability of the theory to explain cybercrime behavior.

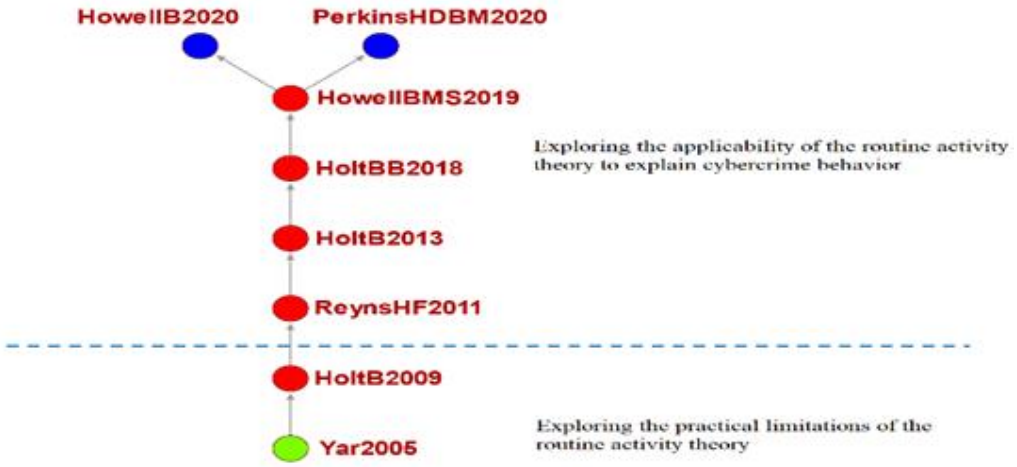


Figure 7 Main path analysis of the first cluster (i.e., the effect of the routine activity theory on cybercrime).

4.2.2. Effect of Police–Community Partnerships on Cybercrime

The second cluster featured 86 studies on police–community partnerships. As shown in Figure 8, the main path consisted of seven studies published from 2007 to 2020 that explored the effect of police–community partnerships on cybercrime.

Jones [35] contended that individuals, the government, and enterprises should modify the source code of open-source software to mitigate security loopholes. Wall [36] explored the methods of maintaining order in the real world and the Internet by focusing on Internet behavior and policing. Levi [37] examined the relationship between information security and assurance in the United Kingdom and British policing.

Huey [38] investigated the motivations and behaviors of Internet watchdogs, who track and identify information related to cybercriminals. Some nongovernment organizations work with police and share their evidence with criminal justice agencies. Huey found that Internet watchdogs can reduce cybercrime. Harkin [39] maintained that Internet monitoring and management authorities experience three major problems regarding cybercrime. First, the higher rate of cybercrime is associated with higher workloads. Second, the management authority's recourses are insufficient for solving cases of cybercrime. Third, the management authority's skills are insufficient to address sophisticated cybercrime. Nowacki [40] employed Maguire's theory to measure the organizational variables related to context, complexity, and control. A regression analysis was then performed to test whether these variables were associated with the case-handling methods used by police organizations. The results revealed that these variables were correlated with the case-handling methods. Paek [41] examined whether law enforcement supports public–private partnerships (PPPs) when policing cyberspace. A PPP refers to the partnership between a nongovernment organization and a government agency. The study revealed that law enforcement officers supports adoption of PPPs to prevent cybercrime.

As shown in Figure 8, the studies published from 2007 to 2013 primarily focused on how the police and the public cooperate to maintain order in cyberspace. Since 2018, studies have primarily explored the challenges that police face when handling cybercrime cases.

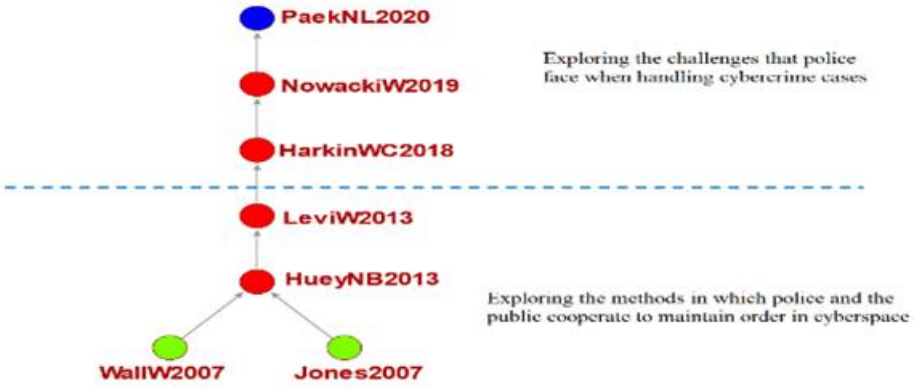


Figure 8 Main path analysis of the second cluster (i.e., the effect of police–community partnerships on cybercrime).

4.2.3. Effect of Network Communication Technology on Cybercrime

The third cluster featured 68 studies on network communication technology. As shown in Figure 9, the main path consisted of six studies published from 2012 to 2020 that explored the effect of network communication technology on cybercrime.

Soudjin [42] proposed offender convergence settings, which refers to places where cybercriminals gather and conduct activities such as information exchange and illegal trading. Regarding hacker attacks, Soudjin argued that cybercriminals can not only hack accounts and steal property but also transfer money to other accounts without leaving any traces. This study also proposed policy-related suggestions. Leukfeldt [43] analyzed phishing in Amsterdam, or the act of using real-world social networks to steal information from victims.

Leukfeldt [18], Bijlenga [19], Kruisbergen [20], and Lavorgna [22] explored the use of communication technology in cybercrime by collecting data from criminal cases. All four studies were on the global main path, which indicated that they have substantially influenced cybercrime research.

Figure 9 displays the studies published from 2012 to 2014, which mainly analyzed the common types of cybercrime through research reports. Studies published from 2017 onward have focused more on the use of network communication technology in cybercrime.

Figure 9 Main path analysis of the third cluster (i.e., the effect of network communication technology on cybercrime).

4.2.4. Effect of Internet Users' Concept of Security on Cybercrime

The fourth cluster featured 49 studies on Internet users' concept of security. As depicted in Figure 9, the main path consisted of five studies published from 2011 to 2019 and aimed to explore the effect of Internet users' concept of security on cybercrime.

Choo [25] examined the use of the routine activity theory to reduce cybercrime and reinforce methods of cybercrime investigation and punishment. Mani [44] examined the information security and risk management standards adopted by the real estate industry in South Australia. Mani found that people did not understand the true scale of cybercrime and its effects on the real estate industry. Moreover, Mani argued that employees should be trained on information security maintenance regularly to respond to more sophisticated cybercrime. Imgraben [45] indicated that most smartphone users are indifferent toward personal data theft and do not understand its risks and consequences. Imgraben suggested that an educational program that helps users understand cybercrime methods and countermeasures can be adopted to change users' attitudes and behaviors toward smartphone use.

Renaud [46] contended that a government should inform people on how to protect themselves online; those who do adhere to the government's advice must bear the consequences. Venter [47] reported that a minority of university-educated male South Africans know about cybersecurity and that the educational policy in South Africa increases the vulnerability of the young female population to cybercrime. To mitigate this risk, cybersecurity should be incorporated into school curricula starting from elementary school. Moreover, people should learn cybercrime prevention techniques, and the gender imbalance in cybersecurity education must be eliminated.

Figure 10 shows the studies published from 2011 to 2014 that investigated the correlation between Internet user behavior and their likelihood of victimization. Studies published from 2018 onward explored government countermeasures against cybercrime.

Figure 10 Main path analysis of the fourth cluster (i.e., the effect of Internet users' concept of security on cybercrime).

4.2.5. Effect of writeprint Identification Technology on Cybercrime

The fifth cluster featured 48 studies on writeprint identification technology. As depicted in Figure 10, the main path consisted of six studies published from 2006 to 2020 that explored the effect of writeprint identification technology on cybercrime.

Jiexun [48] indicated that writeprint identification mitigates the difficulties of fingerprint collection during cybercriminal investigations. Writeprint identification is used to determine a person's identity through their

writing style. Several combinations of writing features are generated for high-accuracy identity verification. Iqbal [49] introduced an innovative data mining method that captures the written records of suspects and models their writing characteristics and frequency. Criminals can consequently be identified, and their writing can be used as strong legal evidence.

Iqbal [50] analyzed the writing styles in the emails of anonymous criminals. Compared with conventional investigation methods, Iqbal's method was more effective when investigating cases with minimal information. Furthermore, suspects can be grouped according to their writing styles to identify criminals more easily at the start of an investigation.

Pearl [51] proposed a new supervised machine learning model to detect the acts of cybercriminals. The model extracts the criminals' writeprint from written texts to identify their criminal behaviors. This method yields high-accuracy and high-practicality in detecting criminal behavior. Villar-Rodriguez [52] extracted language features from text messages through natural language processing, which can detect language features with high accuracy. Mbaziira [53] indicated that both natural language processing and deception detection discourse are highly effective in detecting fake reviews and scams.

Figure 11 presents the studies published from 2006 to 2010 that investigated the effect of writeprint identification on police efficiency in cybercriminal investigations. Studies published from 2012 onward explored the effectiveness of smart technology in writeprint identification.

Figure 11 Main path analysis of the fifth cluster (i.e., the effect of writeprint identification on cybercrime).

4.3. Growth Curve Analysis of Cybercrime Research

Cybercrime research has grown annually, and a total of 4126 studies have been published. Currently, a total of 7674 scholars have investigated cybercrime. In this study, a growth curve analysis was conducted to examine the maturation period of cybercrime studies.

In Fig. 11, the dotted line represents the estimated cumulative number of studies published, and the solid line and dots are the actual cumulative numbers. The inflection point of the growth curve occurred in 2017, and cybercrime research is expected to plateau by 2047, at which point the cumulative number of studies published is estimated to be 4126.

Currently, cybercrime research has surpassed the inflection point of its growth period and is expected to grow slowly. Cybercrime research is expected to fully develop in approximately 30 years.

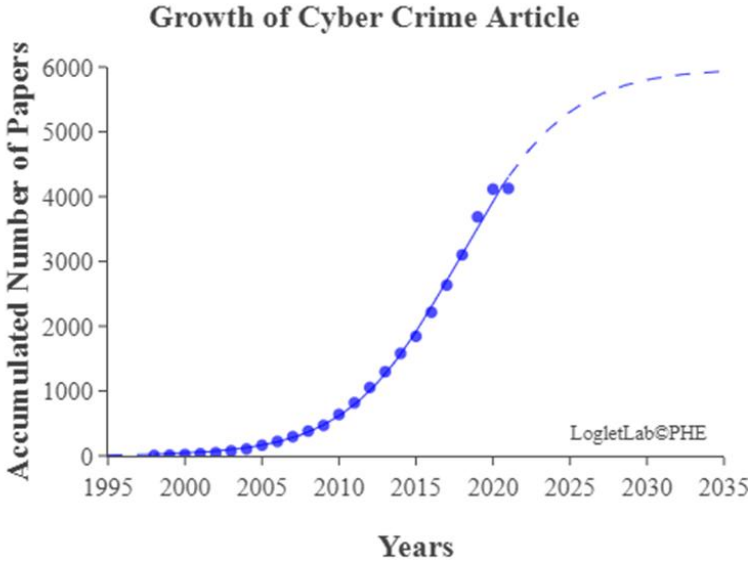


Figure 12 Growth curve of cybercrime studies.

5. Conclusions

Currently, 4126 studies have been published on cybercrime. The cumulative number is expected to reach 5990 by 2033, when cybercrime research is expected to plateau. Cybercrime research to fully develop in 15 years.

This study performed a global main path analysis to identify the research main path with the highest total weight. A key-route main path analysis was then conducted to observe the interactions and relationships between research paths. The results indicated that early cybercrime studies focused on exploring the common types of cybercrime, the studies during the middle period focused on the correlation between victims' behavior and their likelihood of victimization, and the most recent studies integrated data on the use of communication technology in cybercrime and various types of cybercrime.

Cluster analysis and data mining were performed to identify the five largest clusters of cybercrime studies. Various research fields related to cybercrime were then analyzed. The five clusters were named "effect of the routine activity theory on cybercrime," "effect of police–community partnerships on cybercrime," "effect of network communication technology on cybercrime," "effect of Internet users' concept of security on cybercrime," and "effect of writeprint identification technology on cybercrime." Finally, the developmental contexts and research focuses of each cluster were identified according to their global main path.

1. Effect of the routine activity theory on cybercrime: Early studies focused on the practical limitations of the routine activity theory, whereas recent studies have examined whether the theory can explain cybercrime behavior.
2. Effect of police–community partnerships on cybercrime: Early studies focused on cooperation between police and the public in maintaining order in cyberspace, whereas recent studies have explored the challenges police face when handling cybercrime cases.
3. Effect of network communication technology on cybercrime: Early studies mainly analyzed the common types of cybercrime through research reports, whereas recent studies have focused on the use of network communication technology in cybercrime.
4. Effect of Internet users' concept of security on cybercrime: Early studies focused on the correlation between Internet users' behavior and their likelihood of victimization, whereas recent studies have explored the governments countermeasures against cybercrime.
5. Effect of writeprint identification on cybercrime: Early studies investigated the effect of writeprint identification on the police efficiency in cybercriminal investigations, whereas recent studies have explored the effectiveness of smart technology in writeprint identification.

According to the results of the global main path analysis, key-route main path analysis, and cluster analysis, the topics of cybercrime research vary but are related. Studies discussing the "correlation between victims' behavior and their likelihood of victimization" and the "use of network communication technology in various types of cybercrime" can be found in the clusters "effect of the routine activity theory on cybercrime," "effect of Internet users' concept of security on cybercrime," and "effect of network communication technology on cybercrime." Thus, these studies have influenced cybercrime research considerably.

This study was an integrative study, whose structure and methodology can be used to explore trends in research topics and explain the key implications of technological management.

Author Contributions: Conceptualization and methodology, F.-L.H. and K.-Y.C.; data curation, F.-L.H. and W.-H.S.; writing—original draft preparation, K.-Y.C; writing—review and editing, W.-H.S.; supervision, K.-Y.C.; project administration, K.-Y.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable

Informed Consent Statement: Not applicable

Data Availability Statement: Not applicable

Acknowledgments:
Fei-Lung Huang: College of Management Ph.D. Candidate, National Taipei University of Technology

Kai-Ying Chen: Professor of the Department of Industrial Engineering and Management, National Taipei University of Technology. He focuses on the fields of Manufacturing Automation and Electronic Business, Manufacturing Execution System, and Application of Radio Frequency Identification.

Wei-Hao Su: Assistant Professor of the Department of Industrial Engineering and Management, National Taipei University of Technology. He focuses on Technology and Innovation Management, Management of Technology, Managing Innovation in Organizations, and New Venture Creation.

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

References

[1]. Cybercrime. Available online: https://en.wikipedia.org/wiki/Cybercrime(accessed on 01 December 2021)
[2]. Fontana, R.; Nuvolari, A.; Verspagen, B. Mapping technological trajectories as patent citation networks: an application to data communication standards. *Econ. Innov. New Technol.* **2009**, *18*, 311–336. https://doi.org/10.1080/10438590801969073
[3]. Consoli, D.; Mina, A. An evolutionary perspective on health innovation systems. *J. Evol. Econ.* **2009**, *19*, 297–319. http://doi.org/10.1007/s00191-008-0127-3
[4]. Bekkers, R.; Martinelli, A. Knowledge positions in high-tech markets: trajectories, standards, strategies and true innovators. *Technol. Forecast. Soc. Change* **2012**, *79*, 1192–1216. https://doi.org/10.1016/j.techfore.2012.01.009
[5]. Lucio-Arias, D.; Leydesdorff, L. Main¬Path Analysis and Path-Dependent Transitions in HistCite™-based Historiograms. *J. Assoc. Inf. Sci. Technol.* **2008**, *59*, 1948–1962. https://doi.org/10.1002/asi.20903
[6]. Calero-Medina, C.; Noyons, E.C. Combining mapping and citation network analysis for a better understanding of the scientific development: the case of the absorptive capacity field. *J. Informetr.* **2008**, *2*, 272–279. https://doi.org/10.1016/j.joi.2008.09.005
[7]. Colicchia, C.; Strozzi, F. Supply chain risk management: a new methodology for a systematic literature review. *Supply Chain Manag. Int. J.* **2012**, *17*, 403–418. https://doi.org/10.1108/13598541211246558
[8]. Harris, J.K.; Beatty, K.E.; Lecy, J.D.; Cyr, J.M.; Shapiro, R.M, II. Mapping the multidisciplinary field of public health services and systems research. *Am. J. Prev. Med.* **2011**, *41*, 105–111. https://doi.org/10.1016/j.amepre.2011.03.015
[9]. Chuang, T.C.; Liu, J.S.; Lu, L.Y.; Tseng, F.M.; Lee, Y.; Chang, C.T. The main paths of eTourism: trends of managing tourism through internet. *Asia Pac. J. Tour. Res.* **2017**, *22*, 213–231. https://doi.org/10.1080/10941665.2016.1220963
[10]. Yan, J.; Tseng, F.M.; Lu, L.Y. Developmental trajectories of new energy vehicle research in economic management: main path analysis. *Technol. Forecast. Soc. Change* **2018**, *137*, 168–181. https://doi.org/10.1016/j.techfore.2018.07.040
[11]. Lin, P.Y.; Chen, K.Y.; Cheng, C.Y.; Su, W.H.; Lu, L.Y. The academic development trajectories of the lean production based on main path analysis method. *Processes* **2022**, *10*, 1495–1518. https://doi.org/10.3390/pr10081495
[12]. Li, M. Research on the key citation paths of U.S. federal circuit judgments using main path analysis. *Presence* **2012**.
[13]. Li, J. A survey of the development track and trend of patent abuse theory: a viewpoint of main path analysis. *Presence* **2016**.
[14]. Kshetri, N. The simple economics of cybercrimes. *IEEE Secur. Priv*. **2006**, *4*, 33–39. https://doi.org/10.1109/MSP.2006.27
[15]. Gordon, S.; Ford, R. On the definition and classification of cybercrime. *J. Comput. Virol*. **2006**, *2*, 13–20. http://doi.org/10.1007/s11416-006-0015-z
[16]. Van Wilsem, J. Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *Eur. J. Criminol.* **2011**, *8*, 115–127. http://dx.doi.org/10.1177/1477370810393156
[17]. Williams, M.L. Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. *Br. J. Criminol.* **2016**, *56*, 21–48. https://doi.org/10.1093/bjc/azv011
[18]. Leukfeldt, E.R.; Kleemans, E.R.; Stol, W.P. Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *Br. J. Criminol.* **2017**, *57*, 704–722. https://doi.org/10.1093/bjc/azw009

[19]. Bijlenga, N.; Kleemans, E.R. Criminals seeking ICT-expertise: an exploratory study of Dutch cases. *Eur. J. Crim. Policy Res.* **2018**, *24*, 253–268. https://doi.org/10.1007/s10610-017-9356-z
[20]. Kruisbergen, E.W.; Leukfeldt, E.R.; Kleemans, E.R.; Roks R.A. Money talks money laundering choices of organized crime offenders in a digital age. *J. Crime Justice* **2019**, *42*, 569–581. https://doi.org/10.1080/0735648X.2019.1692420
[21]. WeulenKranenbarg, M. Global voices in hacking (multinational views). *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Palgrave Macmillan: Cham, Switzerland, 2020; pp.771–792
[22]. Lavorgna, A. Organized crime and cybercrime. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Palgrave Macmillan: Cham, Switzerland, 2020; pp. 117–134.
[23]. Grabosky, P. Requirements of prosecution services to deal with cyber crime. *Crime, Law Soc. Chang.* **2007**, *47*, 201–223.http://doi.org/ 10.1007/s10611-007-9069-1
[24]. Choo, K.-K.R. Organised crime groups in cyberspace: a typology. *Trends Organ. Crime* **2008**, *11*, 270–295. http://doi.org/10.1007/s12117-008-9038-9
[25]. Choo, K.-K.R. The cyber threat landscape: challenges and future research directions. *Comput. Secur.* **2011**, *30*, 719–731. https://doi.org/10.1016/j.cose.2011.08.004
[26]. Leukfeldt, E.R.; Yar, M. Applying routine activity theory to cybercrime: a theoretical and empirical analysis. *Deviant Behav.***2016**, *37*, 263–280. https://doi.org/10.1080/01639625.2015.1012409
[27]. Howell, C.J.; Burruss, G.W.; Maimon, D.; Sahani, S. Website defacement and routine activities: considering the importance of hackers valuations of potential targets. *J. Crime Justice* **2019**, *42*, 536–550. https://doi.org/10.1080/0735648X.2019.1691859
[28]. Howell, C.J.; Burruss, G.W. Datasets for analysis of cybercrime. *The Palgrave Handbook of International Cybercrime and Cyber deviance*, Palgrave Macmillan: Cham, Switzerland, 2020; pp. 207–219. https://doi.org/10.1007/978-3-030-74837-1_12
[29]. Perkins, R.C.; Howell, C.J.; Dodge, C.E.; Burruss, G.W.; Maimon, D. Malicious spam distribution: a routine activities approach. *Deviant Behav.***2020**, *43*, 1–17. https://www.x-mol.com/paperRedirect/1340000824559583232
[30]. Yar, M. The novelty of cybercrime: an assessment in light of routine activity theory. *Eur. J. Criminol.* **2005**, *2*, 407–427. http://dx.doi.org/10.1177/147737080556056
[31]. Holt, T. J.; Bossler, A.M. Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behav.* **2009**, *30*, 1–25. https://psycnet.apa.org/doi/10.1080/01639620701876577
[32]. Reyns, B.W.; Henson, B.; Fisher, B.S. being pursued online: applying cyber life style-routine activities theory to cyberstalking victimization. *Crim. Justice Behav.* **2011**, *38*, 1149–1169. https://psycnet.apa.org/doi/10.1177/0093854811421448
[33]. Holt, T. J.; Bossler, A.M. Examining the relationship between routine activities and malware infection indicators. *J. Contemp. Crim. Justice* **2013**, *29*, 420–436. https://doi.org/10.1177%2F1043986213507401
[34]. Holt, T.J.; Burruss, G.W.; Bossler, A.M. Assessing the macro-level correlates of malware infections using a routine activities framework. *Int. J. Offender Ther. Comp. Criminol.* **2018**, *62*, 1720–1741. https://doi.org/10.1177%2F0306624X16679162
[35]. Jones, B.R. Comment: virtual neighborhood watch: open source software and community policing against cybercrime. *J. Crim. L. Criminol.* **2007**, *97*, 601–629. https://www.jstor.org/stable/40042835
[36]. Wall, D.S.; Williams, M. Policing diversity in the digital age: maintaining order in virtual communities. *Criminol. Crim. Justice* **2007**, *7*, 391–415. http://dx.doi.org/10.1177/1748895807082064
[37]. Levi, M.; Williams, M.L. Multi-agency partnerships in cybercrime reduction: mapping the UK information assurance network cooperation space. *Inf. Manag. Comput. Secur.* **2013**, *21*, 420–443. http://doi.org/10.1108/IMCS-04-2013-0027
[38]. Huey, L.; Nhan, J.; Broll, R. Uppity civilians and cyber-vigilantes: the role of the general public in policing cyber-crime. *Criminol. Crim. Justice* **2013**, *13*, 81–97. https://doi.org/10.1177%2F1748895812448086
[39]. Harkin, D.; Whelan, C.; Chang, L. The challenges facing specialist police cyber-crime units: an empirical analysis. *Police Pract. Res.* **2018**, *19*, 519–536. https://doi.org/10.1080/15614263.2018.1507889
[40]. Nowacki, J.; Willits, D. An organizational approach to understanding police response to cybercrime. *Policing Int. J.* **2019**, *43*, 63–76. https://doi.org/10.1108/PIJPSM-07-2019-0117
[41]. Paek, S.Y.; Nalla, M.K.; Lee, J. Determinants of police officers' support for the public-private partnerships (PPPs) in policing cyberspace. *Policing Int. J.* **2020**, *43*, 877–892. http://doi.org/10.1108/PIJPSM-06-2020-0088
[42]. Soudijn, M.R.J.; Zegers, B.C.H.T. Cybercrime and virtual offender convergence settings. *Trends Organ. Crime* **2012**, *15*, 111–129. http://dx.doi.org/10.1007/s12117-012-9159-z

[43]. Leukfeldt, E.R. Cybercrime and social ties: Phishing in Amsterdam. *Trends Organ. Crime* **2014**, *15*, 231–249. http://dx.doi.org/10.1007/s12117-014-9229-5
[44]. Mani, D.; Choo, K.-K.R.; Mubarak, S. Information security in the South Australian real estate industry: a study of 40 real estate organisations. *Inf. Manag. Comput. Secur.* **2014**, *22*, 24–41. https://doi.org/10.1108/IMCS-10-2012-0060
[45]. Imgraben, J.; Engelbrecht, A.; Choo, K.-K.R. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behav. Inf. Technol* .**2014**, *33*, 1347–1360. https://doi.org/10.1080/0144929X.2014.934286
[46]. Renaud, K.; Flowerday, S.; Warkentin, M.; Cockshott, P.; Orgeron, C. Is the responsibilization of the cyber security risk reasonable and judicious? *Comput. Secur.* **2018**, *78*, 198–211. https://doi.org/10.1016/j.cose.2018.06.006
[47]. Venter, I.M.; Blignaut, R.J.; Renaud, K.; Venter, M.A. Cyber security education is as essential as the three R's. *Heliyon* **2019**, *5*, e02855. http://dx.doi.org/10.1016/j.heliyon.2019.e02855
[48]. Jiexun, L.I.; Zheng, R.; Chen, H. From fingerprint to writeprint. *Commun. ACM*. **2006**, *49*, 76–82. http://dx.doi.org/10.1145/1121949.1121951
[49]. Iqbal, F.; Hadjidj, R.; Fung, B.C.M.; Debbabi, M. A novel approach of mining write-prints for authorship attribution in e-mail forensics. *Digit Investig*. **2008**, *5*, S42–S51. http://doi.org/10.1016/j.diin.2008.05.001
[50]. Iqbal, F.; Binsalleeh, H.; Fung, B.C.M.; Debbabi, M. Mining writeprints from anonymous e-mails for forensic investigation. *Digit Investig*. **2010**, *7*, 56–64. http://doi.org/10.1016/j.diin.2010.03.003
[51]. Pearl, L.; Steyvers, M. Detecting authorship deception: a supervised machine learning approach using author writeprints. *Lit. Linguistics Comput.* **2012**, *27*, 183–196. http://dx.doi.org/10.1093/llc/fqs003
[52]. Villar-Rodriguez, E.; Del Ser, J.; Bilbao, M.N.; Salcedo-Sanz, S. A feature selection method for author identification in interactive communications based on supervised learning and language typicality. *Eng. Appl. Artif. Intell*. **2016**, *56*, 175–184. http://dx.doi.org/10.1016/j.engappai.2016.09.004
[53]. Mbaziira, A.V.; Murphy, D.R. An empirical study on detecting deception and cybercrime using artificial neural networks. In Proceedings of the 2nd International Conference on Compute and Data Analysis, Association for Computing Machinery: New York, NY, United States, 2018; pp. 42–46. https://doi.org/10.1145/3193077.3193080