International Journal of Cybersecurity Intelligence & Cybercrime

Volume 6 | Issue 1 Article 2

3-31-2023

Research Trends in Cybercrime and Cybersecurity: A Review Based on Web of Science Core Collection Database

Cybercrime, Cybersecurity, Collaboration Network, Research topics, Web of Science

Recommended Citation

Wu, L., Peng, Q., & Lemke, M. (2023). Research trends in cybercrime and cybersecurity: A review based on Web of Science core collection database. International Journal of Cybersecurity Intelligence and Cybercrime, 6(1), 5-28.

Wu et al. (2023). *International Journal of Cybersecurity Intelligence and Cybercrime, 6*(1), 5-28.

Research Trends in Cybercrime and Cybersecurity: A Review Based on Web of Science Core Collection Database

Ling Wu*, Ph.D., Prairie View A&M University, U.S.A.
Qiong Peng, Ph.D.,Northeastern University, U.S.A.
Michael Lemke, Ph.D.,University of Houston-Downtown, U.S.A.

Keywords: Cybercrime, Cybersecurity, Collaboration Network, Research topics, Web of Science

Abstract:
Studies on cybercrime and cybersecurity have expanded in both scope and breadth in recent years. This study offers a bibliometric review of research trends in cybercrime and cybersecurity over the past 26 years (1995-2021) based on Web of Science core collection database. Specifically, we examine the growth of scholarship and the expanded scope of subject categories and relevant journals. We also analyze the research collaboration network based on authors' affiliated institutions and countries. Finally, we identify major topics within the fields, how each topic relates to – and diverges from – one another, and their evolution over time. Overall, we illustrate the scientific landscape of cybercrime and cybersecurity scholarship by quantitatively synthesizing major components of existing literature. This study offers actionable insights to help researchers identify key research resources, establish/expand collaboration networks, and investigate emerging research topics in this increasingly important domain in criminology and criminal justice.

Introduction

Technological advances have brought significant improvements for society, but they have also generated new criminal opportunities (Kubic, 2001; Rebovich & Byrne, 2022). Cybercrime and cybersecurity issues have increased exponentially in recent years, leading to the formation of a new line of scientific inquiry (Bossler & Berenblum, 2019; Herath et al., 2022). Given that cybercrime and cybersecurity contain both human and technological dimensions, researchers in these areas need to take an interdisciplinary approach; unfortunately, literature in these areas is very limited and compartmented. Social scientists – primarily criminologists – most often examine the prevalence and dynamics of cybercrime by applying and testing traditional criminological theories. Conversely, computational scientists – predominately computer scientists – explore myriad topics in cybercrime and cybersecurity research, but they have traditionally focused on technical aspects of these areas (Brands & Van Doorn, 2022).

For both novice and established researchers in the fields, a holistic understanding of the scientific landscape is needed to chart future research. It provides potential synergies between social scientists and computational scientists by testing theory using computational modeling. This process also sets a foundation for future collaborative and interdisciplinary research. The current study utilizes a bibliometric method to examine global trends of cybercrime and cybersecurity research in the past 26 years. Bibliometrics presents a great advantage in synthesizing scientific activity in a domain as it offers a transparent, systematic, and

*Corresponding author
Ling Wu, Ph.D., Department of Justice Studies, Prairie View A&M University, 100 University Dr, Prairie View, TX 77446, U.S.A.
Email: liw@pvanu.edu

and reproducible process (Li et al., 2017; Wu et al., 2022).

The purpose of this study is to examine multiple aspects of this scientific landscape, including the state of existing research, major citations, research collaboration networks, as well as popular themes and emerging topics based on a review based on Web of Science core collection database. Web of Science is the oldest, most popular and respected research database in the world (Birkle et al. 2020). More specifically, we first examine the general trend of publications over time and the productivity of scholarly works across countries, institutions, journals, and subject categories. It offers researchers – in particular, those new to the fields – a starting point via which to explore key research resources and directions. We then visualize research collaboration networks and identify the major players and clusters in international and institutional collaboration networks, respectively. Doing so provides researchers with guidance for establishing or expanding their own collaboration networks. Researchers can also reexamine theoretical contexts for their future research based on the most cited works in the fields as pinpointed in this study. Finally, we identify important topics and/or subtopics within the existing cybercrime and cybersecurity literature, and analyze trends presented by these topics through comparing their popularity over time. This helps scholars not only understand the evolution of topics in the fields, but also proactively plan potential future research directions.

Literature Review

Cybercrime is often used as an umbrella term, encompassing a range of criminal activities that take place over the internet or within a computer system by taking advantage of flaws in complex information systems or infrastructures (Finklea & Theohary, 2012; Phillips et al., 2022). The rapid expansion of online business and services, financial transactions, telecommuting, and social media platforms have all contributed to unprecedented criminal opportunities in cyberspace (Ye & Leipnik, 2013; Ye et al., 2019). Direct information regarding the scope and prevalence of cybercrime remains limited (DeTardo-Bora & Bora, 2016), but cybersecurity market growth is anticipated to grow by 12-15% yearly through 2025 (Morgan, 2019). Cybercrime and cybersecurity issues victimize individuals and organizations at all levels and are detrimental to privacy, personal safety, financial health, and national security (Curtis & Oxburgh, 2022). Cybercrime is also rapidly becoming the world's most costly form of crime. The 2020 Internet Crime Complaint Center (IC3) report issued by Federal Bureau of Investigation (FBI), the lead U.S. federal agency for cybercrime investigation, revealed a total loss of $4.2 billion from 791,790 complaints filed by cybercrime victims, which represented a substantial increase in the number of complaints and estimated loss as compared with the 2019 report (FBI, 2021). The global COVID-19 pandemic worsened data breaches in workspaces as well as scams against individuals and organizations exploiting the situations in the pandemic (Panda Security, 2020). The cyberspace chaos ushered in by the pandemic culminated in high-profile ransomware attacks paralyzing major U.S. energy infrastructures (Wade, 2021). These far-reaching consequences of cybercrimes and security issues suggest the urgency to understand their dynamics and improve policies in cybercrime detection, investigation, and more importantly, prevention (Collier et al., 2022; Gottschalk & Hamerton, 2022).

The number of criminological studies on cybercrime has increased over the past two decades, largely due to the surge in cybercrime incidents. Unlike traditional crime, cybercrime has the ability to impact virtual space and cause tremendous tangible and intangible damage (Jaishankar, 2007, 2015; Moneva et al., 2022; Yar, 2005). Cybercrime was examined first as "computer-related crime" or "high technology crime" in

legal and social science fields (Carroll & Schrader, 1995; Coutorie, 1995). Jaishankar (2007) proposed the concept of cyber criminology, defined as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space" (p.1). As a subfield of criminology, it has since entered the academic arena of criminal justice. Various forms of courses and degree programs in cybercrime and cybersecurity are offered by criminal justice departments in U.S. higher education institutions. Most recently, cybercrime and cybersecurity have been seen as preferred areas of specialization in criminal justice academic job advertisements. There are now several journal and book publications in the fields, including the International Journal of Cyber Criminology, devoted to the study of cybercrime through a social science lens.

This line of inquiry by criminologists was largely pursued under the "old wine in new bottles" framework (Grabosky, 2001). Researchers attempted to use traditional criminological theories to examine behavioral dynamics in cyber offending and victimization. Technological evolution created more opportunities for people to exploit for criminal purposes. Still, cybercrime is largely considered a reflection or redirection of crime from physical space in virtual space, given that most crimes committed in person can be translated into cyberspace (Wall, 2001). Even though offenders may adjust their modi operandi to fit for cyber environments, the general criminality does not change intrinsically (Holt & Bossler, 2014). As a whole, these studies have typically demonstrated that traditional criminological theories and their components are applicable in virtual environments (Taylor et al., 2019).

These classical criminological theories revisited in cybercrime literature included, but not limited to, routine activities theory, self-control theory, strain theory, learning theory, and neutralization theory (Bossler & Berenblum, 2019). Utilizing surveys, experiments, existing data, and ethnographies (Payne & Hadzhidimova, 2020), criminologists have studied a wide range of cybercrimes, as summarized by a four-category typology: Cyber-trespass, cyber-deception/theft, cyber-porn and obscenity, and cyberviolence (Payne & Hadzhidimova, 2020; Wall, 2001). Altogether, the existing criminological literature has generated valuable information on cyber-offending and its dynamics. It has expanded our knowledge of the prevalence of cybercrime and the impacts of technology on different offending behaviors (Holt & Bossler, 2014). It has also concluded that no clear general theory of cybercrime can provide a universal explanation for all offenses in cyberspace. Instead, more empirical evidence has been found to support crime-specific theoretical approaches (Payne & Hadzhidimova, 2020). In a nutshell, criminologists have played an important role in shaping our understanding of the mechanisms, risks, and consequences of cybercrime, as well as viable preventive strategies (Payne & Hadzhidimova, 2020).

As a new subfield within criminal justice, the majority of existing cybercrime research used a "zoom in" approach to examine a specific type of crime by testing a particular criminological theory. Conversely, a "zoom out" approach and outward thinking can facilitate future research in cybercrime and cybersecurity. This is because research is needed to understand how the larger criminal justice system responds to cybercrime at all levels (Holt & Bossler, 2014). More importantly, true interdisciplinary research in cybercrime and cybersecurity is needed through close collaboration between computational and social scientists.

In recent years, new theories have been proposed for explaining cybercrime due to a dissatisfaction with traditional theoretical frameworks. Space transition theory (Jaishankar, 2008) and irrational coping theory (Halder & Jaishankar, 2015) are prominent examples. Researchers have also proposed new subfields in cybercrime research. Cyber victimology, for instance, was introduced as "the study of forms of online victimization, its impact on victims, and responses of society and systems" (Jaishankar, 2015). However, the

overall breadth of cybercrime and cybersecurity research by criminologists is still by and large very narrow. This line of inquiry needs to be expanded to embody all major components of criminal justice system, such as law enforcement, courts, and corrections (Holt & Bossler, 2014). The rationale for expanding such inquiry is provided below.

First, cybercrime is arguably one of the most critical challenges facing law enforcement today. The elusive nature of cybercrime translates into a need for high levels of expertise in investigating cybercrime and security issues. Further, cybercrime and cybersecurity demand unique knowledge in law enforcement service and management, from responding to calls for service, arrest and apprehension, investigation, to evidence collection and preservation (Nodeland et al., 2019; Stambaugh et al., 2001). Explorations of these areas are very limited in existing literature, even though they are critical for guiding policy to increase police capabilities for handling and preventing cybercrime (Bossler & Holt, 2012). Similarly, interactions between cybercriminals or cyber victims and the justice process are extremely understudied (Smith et al., 2004; Abu-Ulbeh et al., 2021). Such information is pivotal for developing better policies for processing criminals and serving victims in all stages of the justice system, including prosecution, adjudication, sentencing, corrections, and reentry. Therefore, there is a need to broaden the horizon of cybercrime and cybersecurity research – even within the discipline of criminal justice.

Second, cybercrime and cybersecurity are widely recognized as interdisciplinary fields, encompassing criminology, victimology, sociology, psychology, computer science, information management, and data science, among others (Jaishankar, 2018). Computer scientists have acknowledged that cybercrime and cybersecurity have a pronounced human dimension, along with a technological dimension (Gordon & Ford, 2006). Similarly, criminologists believe that cybercrime should be addressed as an interdisciplinary topic because the nature of cybercrime is "a technological problem, a crime problem, a social issue, a business concern" (Payne & Hadzhidimova, 2020). Criminologists also realized the importance for social scientists to seek an effective way to collaborate with computational and technology specialists (Bossler, 2017). However, current cybercrime and cybersecurity research is very compartmentalized, and therefore separately conducted by social scientists (predominantly criminologists) and computational scientists (predominantly computer scientists). On one hand, cyber criminology is still to some extent marginalized and neglected by mainstream criminology, and some conventional criminologists may not necessarily acknowledge cyber criminology as a distinct discipline. Similarly, other conventional criminologists may have no interest or expertise in technologies/methods and laws/policies related to cyber forensics and information security. Many conventional criminologists are "digital immigrants,": People born before 1985 who adopted digital technology later in life (Prensky, 2001). In such cases, limited exposure to technology could have hindered efforts to research cybercrime (Holt et al., 2015). On the other hand, computer scientists have traditionally focused little on the human element of cybercrime due to limited social science exposure or training. In both cases, barriers can be created due to the lack of a "common language" (Holt, 2017) or different epistemic values, research methods, and standards of evidence between social and computer scientists (Hofman et al., 2021). In addition, a practical challenge to true interdisciplinary collaboration is a lack of funding opportunities for interdisciplinary teams and joint grant-seeking efforts by such teams. Internal and external grants jointly applied for, and secured by, social scientists and computational scientists are pivotal to warrant such collaboration. Only when both criminologists and computer scientists begin to embrace an outward mindset and operate outside their silos can they start to build a collaborative relationship. Otherwise, cybercrime and cybersecurity research will continue to exist in separate silos, thus missing out on the opportunity to meaningfully integrate key insights.

Fortunately, there are signs that research in this area is becoming less compartmentalized. Next-generation criminologists may bring cybercrime research to new heights, as these "digital natives" – researchers born after the rise of digital technologies – master holistic knowledge of theory and technology (Jaishankar, 2010; 2018). It is also envisioned that the field of cyber criminology will become more integrated within conventional criminology. At the same time, computational scientists are beginning to dabble in the social science realm. Tapping the unprecedented amount of digital social data – particularly unstructured data – produced in recent years requires methods and practices derived from computer science (Edelmann et al., 2020). This exploration may lead to the emergence of a "computational social science" field that will attract both social scientists and computer scientists. While the computational revolution is still unfolding, research on collecting and analyzing social data and drawing funding has become more important than ever (Lazer et al., 2009). Altogether, this builds a solid foundation for future interdisciplinary collaboration on cybercrime and cybersecurity research.

In summary, the core of cyber criminology involves the examination of offending and victimization in cyberspace from a behavioral theoretical perspective (Jaishankar, 2010; Ngo & Jaishankar, 2017). However, social scientists do not necessarily have the expertise in relevant technologies and thus they need assistance from computational scientists (Bossler, 2017). Cybercrime and cybersecurity are therefore fields drawing on a variety of disciplines, including computer science, information technology, electrical engineering, criminology, criminal justice, sociology, philosophy, law, psychology, and others. Given the very fragmented state of current scholarship, a clearer picture of the entire cybercrime and cybersecurity landscape is needed to guide future research and facilitate novel interdisciplinary collaborations.

Data and Method

The dataset used in this study is collected from Science Citation Index Expanded (SCIE) and Social Science Citation Index (SSCI) publications in the Web of Science Core Collection database. The publication search strategy is: Title= (cyber$crime* OR cyber$security*) OR Abstract= (cyber$crime* OR cyber$security*) OR Author Keywords= (cyber$crime* OR cyber$security*). Each publication that contains any of these keywords and their variants (with *) in the title, abstract, or keyword list is included. For each publication, published year, title, authors and their institutional affiliations, keywords, and cited references were collected. The time frame of the search was set as "until now" (the data collection date was September 19, 2021). The search query resulted in a total of 3,815 records. Among them, 180 records are excluded from the current study due to the lack of critical information, such as the published year. As a result, this bibliometric study examined 3,635 cybercrime and/or cybersecurity publications between 1995 and 2021. Synonymous terms from the keyword pool were standardized as to improve the author keyword analysis results.

Bibliometric analysis incorporates both quantitative and visual analytics to summarize trends in selected research fields. Such analysis can "reveal temporal dynamics of scholarly works, spatial and institutional distributions of publications, academic collaborations, and major research trends" (Li et al., 2017, p. 385). Furthermore, bibliometric network analysis, such as co-word analysis (Ding et al. 2001), co-citation analysis (He & Hui, 2002), co-authorship analysis (Glänzel & Schubert, 2005), and co-publication analysis (Schmoch & Schubert, 2007), can shed light on relationships between keywords, as well as relationships between other identifiers in the literature, including country of origin, research institution, and

author (Peng & Ye, 2021). We use the R package "Bibliometrix" (Aria & Cuccurullo, 2017) and VOSviewer (Van Eck & Waltman, 2010) to perform the bibliometric analysis. The "Bibliometrix" package is a tool for quantitative research in scientometrics and bibliometrics. It can build data matrices for co-citation, co-author, and co-word analysis as well as perform all main bibliometric methods of analysis.

VOSviewer is a software tool for visualizing scientific landscapes by constructing and mapping bibliometric networks within the scientific literature. Natural language processing functionality is built in the VOSviewer package, which enables a researcher to create co-occurrence networks based on textual data extracted from a body of scientific literature. This software package also includes state-of-the-art techniques for network layout and network clustering. VOSviewer can be used to visualize bibliometric networks that are formed by a set of items together with links between the items. Items in a bibliometric network can be scientific publications, journals, researchers, institutional affiliations, countries, or keywords, along with other identifiers (e.g., citations). These items can then be linked through different metric measurements, such as co-authorship, co-occurrence, bibliographic coupling, citation, or co-citation. A network map typically includes only one type of item, as well as a single type of link measurement chosen by researchers.

Node, link, and cluster are three core features to view a network map. First, an item is represented by a node and its label in a network map. The size of a node is determined by the weight of the item, so the heavier the weight of an item, the larger the node of the item. For some items, the label may not be displayed to avoid overlapping labels. Second, a link is a connection or a relation between two items in a network. Each pair of items in a network has only one link, as represented by a curved line between them. The thickness of this line indicates the strength of the link, while the distance between two items approximately indicates their relatedness. Therefore, a thicker line represents a stronger the link between two items, while a shorter distance means that the two items are more related to each other when compared with other pairs of items. Third, the clustering technique in VOSviewer assigns items to clusters by maximizing the quality function, after the relatedness of items has been determined. Different clusters are shown in different colors, and they are non-overlapping. Each item is assigned to only one cluster, and the color of that item is determined by the cluster to which the item belongs. At the same time, clusters do not necessarily exhaustively cover all items in a map, so there may be items that do not belong to any cluster. Based upon these analytical functions in VOSviewer, the current research generates different network maps in the hope of providing multiple angles through which to examine the current scientific landscape of cybercrime and cybersecurity research.

Results

Characteristics and Patterns of Existing Publications

Key characteristics of the 3,635 publications related to cybercrime and/or cybersecurity identified during the literature search are shown in Figure 1 and Table 1. The annual number of publications increased from 1 in 1995 to 780 in 2020, illustrating an upward growth trajectory. The number of publications in the first nine and half months of 2021 totaled 741. As such, the overall growth rate shows significant acceleration since 2016, and over 80% of all cybercrime and cybersecurity studies were published in the last six years of the study period.

Table 1. *Scientific Output Descriptors, 1995-2021*

PY	TP	AU	AU/TP	NR	NR/TP	TC	TC/TP
1995	1	1	1.000	0	0.000	1	1.000
1999	2	2	1.000	0	0.000	0	0.000
2000	10	11	1.100	97	9.700	39	3.900
2001	9	10	1.111	3	0.333	18	2.000
2002	12	12	1.000	30	2.500	26	2.167
2003	22	29	1.318	147	6.682	139	6.318
2004	27	38	1.407	83	3.074	304	11.259
2005	23	27	1.174	66	2.870	58	2.522
2006	31	41	1.323	375	12.097	253	8.161
2007	24	33	1.375	300	12.500	232	9.667
2008	35	57	1.629	526	15.029	1131	32.314
2009	23	40	1.739	488	21.217	551	23.957
2010	39	98	2.513	1033	26.487	1444	37.026
2011	55	124	2.255	1825	33.182	1421	25.836
2012	69	133	1.928	1714	24.841	1305	18.913
2013	109	244	2.239	3875	35.550	2078	19.064
2014	102	234	2.294	4092	40.118	1833	17.971
2015	110	255	2.318	3933	35.755	1443	13.118
2016	203	561	2.764	8746	43.084	3182	15.675
2017	246	689	2.801	9902	40.252	4009	16.297
2018	400	1233	3.083	18456	46.140	4851	12.127
2019	562	1912	3.402	28082	49.968	5289	9.411
2020	780	2787	3.573	43742	56.079	3224	4.133
2021	741	2744	3.703	43426	58.605	717	0.968

Note: *PY: publication year; TP: number of publications; AU: number of authors; TC: total citation count; NR: number of cited references; AU/TP, NR/TP, and TC/TP: average number of authors, references, and citation per paper

The cybercrime and cybersecurity research fields has also attracted more scholars, as evidenced by the steadily increasing number of authors (AU) over time; specifically, these numbers increased from only one scholar in 1995 to 2,744 scholars in 2021 (Table 1). Not only are more scholars involved in the fields today, but their involvement has increasingly centered on collaborative works. The authorship per publication (AU/TP) increased threefold over the study period to reach an average of 3.7 authors per publication by 2021. This rising trend in authorship might be partially explained by the fact that modern scientific inquiries have become more complex and thus require collaboration within a discipline or across different disciplines. Together, these results suggest that scholarly interests and frequencies of collaboration are on the rise across cybercrime and cybersecurity research. In addition, the average number of quoted references in each publication (NR/TP) has increased from 0 in 1995 to 58.6 in 2021. Such growth in quoted references indicates an expansion of the accumulated knowledge base in the cybercrime and cybersecurity fields. Thus, throughout the past 26 years, and in particular across the most recent six years, the cybercrime and cybersecurity research fields have boomed. This, in turn, has attracted more researchers to the fields, fostered more collaboration, and built a consistently stronger scientific knowledge base for future research.

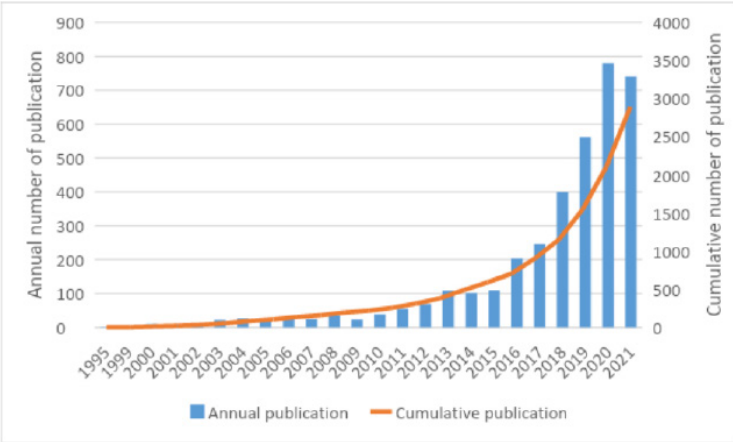


Figure 1. Growth of publication outputs, 1995-2021

Distribution of Publications among Subject Categories and Journals

Due to multidisciplinary interests of cybercrime and cybersecurity research, scholars may target a wide range of journals to publish their works. To identify major publication channels utilized by researchers, a journal productivity measure was adopted for cybercrime and cybersecurity literature, as calculated by the total number of articles in the database published in a particular journal. Table 2 summarizes and ranks the 20 most productive journals of cybercrime and cybersecurity literature. The top 20 journals listed below have different focuses and audiences; nevertheless, they serve as primary venues for cybercrime and cybersecurity scholarly articles. IEEE Access has not only produced the largest number of publications (TP, 220), but also the highest number of total citations (TC, 2,094), as compared with other journals. Six out of the 20 journals were Social Science Citation Index (SSCI) journals: Computer Law & Security Review, Crime Law and Social Change, Security Journal, Communications of the ACM, Deviant Behavior, and Journal of Contemporary Criminal Justice. The remaining Science Citation Index Expanded (SCIE) journals fell under a variety of Web of Science Core Collection Categories, but, by and large, were related to the computer science category. When ranking journal productivity by the average number of citations per publication (TC/TP), Transactions on Smart Grid (SCIE, 39.16) and Deviant Behavior (SSCI, 34.73) emerged at the top the list. One unique journal, however, is Energies (under "Energy & Fuels" category), which is neither a computer science journal nor a social science journal. The reason it features cybercrime and cybersecurity research may be related to the fact that cyber-attacks expose critical energy infrastructure to a range of adversaries, as evidenced by recent ransomware attacks against critical U.S. pipelines. Thus, new solutions to improve the resiliency and security of energy infrastructure are desperately needed, and hence prioritized in the related discipline (Onyeji et al., 2014)

Table 2. *The 20 Most Productive Journals in Cybercrime and Cybersecurity Research*

Journals	Core Collection categories (Index)	TP (%)	TC (%)	TC/TP
IEEE Access	Engineering, Electrical & Electronic | Telecommunications | Computer Science, Information Systems (SCIE)	220(6.05)	2,094(6.24)	9.52

Computers & Security	Computer Science, Information Systems (SCIE)	176(4.84)	1,221(3.64)	6.94
IEEE Security & Privacy	Computer Science, Information Systems | Computer Science, Software Engineering (SCIE)	109(3.00)	545(1.63)	5.00
Sensors	Instruments & Instrumentation | Chemistry, Analytical | Engineering, Electrical & Electronic (SCIE)	64(1.76)	180(0.54)	2.81
Computer	Computer Science, Hardware & Architecture | Computer Science, Software Engineering (SCIE)	60 (1.65)	472(1.41)	7.87
Applied Sciences-basel	Engineering, Multidisciplinary | Materials Science, Multidisciplinary | Chemistry, Multidisciplinary | Physics, Applied (SCIE)	53(1.46)	166(0.50)	3.13
Computer Law & Security Review	Law (SSCI)	49(1.35)	312(0.93)	6.37
IEEE Transactions on Smart Grid	Engineering, Electrical & Electronic (SCIE)	44(1.21)	1,723(5.14)	39.16
Electronics	Physics, Applied | Computer Science, Information Systems | Engineering, Electrical & Electronic (SCIE)	43(1.18)	460(1.37)	10.70
Future Generation Computer Systems the International Journal of Escience	Computer Science, Theory & Methods (SCIE)	43(1.18)	646(1.95)	15.02
Crime Law and Social Change	Social Sciences, Interdisciplinary | Criminology & Penology (SSCI)	38(1.05)	542(1.62)	14.26
Security Journal	Criminology & Penology (SSCI)	32(0.88)	194(0.58)	6.06
Communications of the ACM	Computer Science, Hardware & Architecture | Computer Science, Theory & Methods | Computer Science, Software Engineering (SSCI)	30(0.83)	201(0.60)	6.70
Deviant Behavior	Criminology & Penology | Psychology, Social | Sociology (SSCI)	30(0.83)	1042(3.11)	34.73
Journal of Contemporary Criminal Justice	Journal of Contemporary Criminal Justice	30(0.83)	428(1.28)	14.27
Security and Communication Networks	Telecommunications | Computer Science, Information Systems (SCIE)	29(0.80)	100(0.30)	3.45
Computers in Human Behavior	Psychology, Experimental | Psychology, Multidisciplinary (SSCI)	28(0.77)	396(1.18)	14.14
Energies	Energy & Fuels (SCIE)	26(0.72)	128(0.38)	4.92
IEEE Transactions on Information Forensics and Security	Engineering, Electrical & Electronic | Computer Science, Theory & Methods (SCIE)	25(0.69)	235(0.70)	9.40
ACM Computing Surveys	Computer Science, Theory & Methods (SCIE)	23(0.63)	359(1.07)	15.61

Note: *TP: number of publications; TC: total citation count; TC/TP: average number of citations per paper

Geographic and Institutional Distribution of Publications

The current study collected information on authorship of each publication, as well as each author's institutional affiliation. This facilitated the construction of a co-occurrence matrix of co-authors' institutional affiliations and their located countries. Next, authors' geographic distributions and collaboration networks were visualized. Figure 2 shows the top ten countries that produced the most cybercrime and cybersecurity research, as measured by the total number of publications by authors' affiliated institutions (TP). Of the ten countries displayed in Figure 2, four were in Europe, three were in Asia, two were in North America, and one was in Australia. This suggests that cybercrime and cybersecurity is a global phenomenon that draws scholarly attention worldwide. Scholars from the United States produced the largest share of publications (1,474), followed by the United Kingdom (386) and China (300).

We further divided all publications into two groups: 1) the domestic collaborative research (IP), in which all authors' institutional affiliations are within a single country; and 2) the international collaborative research (CP), in which at least one author was affiliated with an institution located in a different country. Comparing IP and CP in Figure 2 revealed that cybercrime and cybersecurity publications in the United States were mainly produced through researchers' collaboration across institutions within the United States, while the United Kingdom approximately equally split the share of domestic collaborative research and international collaborative research. Countries with a higher percentage of international collaborations as compared to their domestic collaborations were Australia (61%), China (61%), South Korea (54%), and Italy (54%).

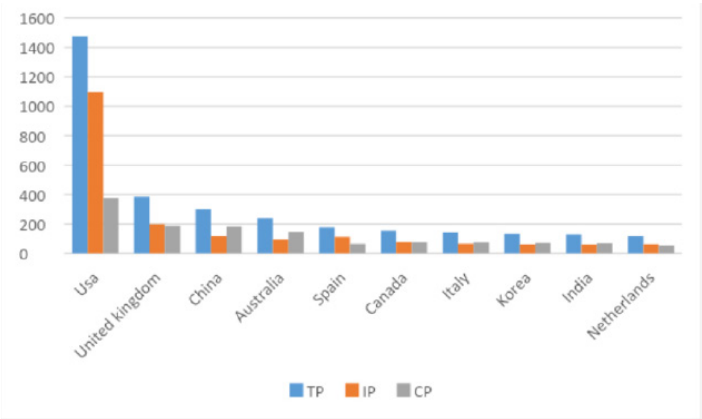
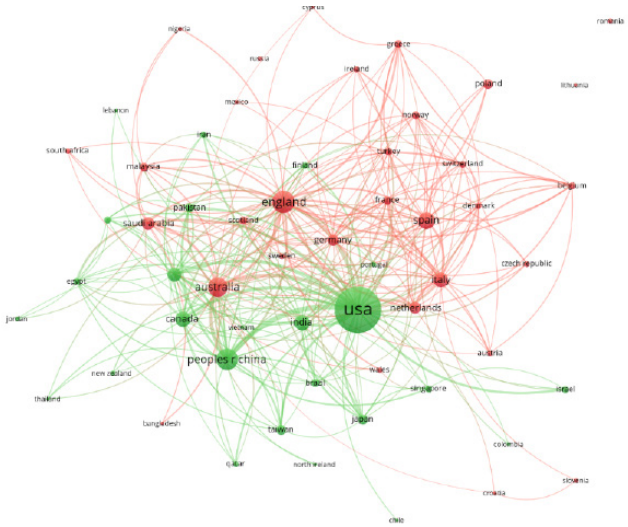


Figure 2. Top Ten Countries with Most Scholars' Affiliated Institutions
Note: *TP, total publications; IP, number of publications by authors affiliated with institutions within a single country; CP, number of internationally collaborative publications

Figure 3 visualizes the collaboration network among 63 countries based on co-authorship analysis utilizing VOSviewer software. Each node and label represent a country, in which the node size indicates a country's importance in the entire network as measured by its productivity or the number of publications produced. Identical to the result as shown in Figure 2, Figure 3 confirms that the United States was the most

productive and influential country in cybercrime and cybersecurity research. The other three relatively large nodes are United Kingdom, China, and Australia, indicating these three nations also produced large numbers of papers with co-authorships.



*F*igure 3. Collaboration Network Across Countries

Co-authorship analysis enabled the study of the most productive countries' collaboration network, as plotted in Figure 3. China and USA are linked by the thickest line in the map, which suggests that co-authorship between China and USA had the highest frequency among all co-authorships between any two countries. For example, the line between India and USA is shorter than the line between India and any other country. This suggests that, in a publication authored by a scholar from India, it was relatively more likely to see the academic involvement of researchers from the U.S. Figure 3 also identifies two main clusters of collaborations represented by two colors (green and red). European countries tended to cluster together and fell into the red cluster, while Asian and North American countries fell into the green cluster. This suggests that countries from the same continent tended to collaborate more with one another than with countries from distant continents. Note that the U.S. is at the center of the collaboration network situated near where the two clusters merge. It illustrates that U.S. researchers conducted an enormous amount of collaborative research with researchers from various countries in both clusters.

Institutional Collaboration Network

Table 3 ranks the top 15 productive higher education institutions, based on the number of publications produced by each institution. Ten institutions were based in the United States, and the other five were based in Australia and Europe. The table shows that Michigan State University published the largest number of articles (87) over the period examined, followed by the University of South California (35), Carnegie Mellon University (34), and Deakin University (34). In addition to the productivity of each institution, citation counts and rates of its academic outputs were also calculated as a means to measure each institution's

academic impact and influence (Harnad, 2009). Michigan State University had the largest number of total citations for its publications, but the University of North Carolina had the highest rate of citations per publication.

Table 3. *Top 15 Institutions Based on The Total Publications and Citations*

Rank	Institution	Number of publications	Number of citations
1	Michigan State University	87	1370
2	University of South Florida	35	254
3	Carnegie Mellon University	34	288
4	Deakin University (Australia)	34	394
5	The University of Texas at San Antonio	31	319
6	Indiana University	29	234
7	University of Maryland	28	507
8	University of Wisconsin	28	422
9	Purdue University	27	182
10	University of Murcia (Spain)	27	229
11	University of Oxford (UK)	27	272
12	University of North Carolina	26	824
13	University of Virginia	25	309
14	Delft University of Technology (Netherlands)	24	305
15	Vrije Universiteit Amsterdam (Netherlands)	23	276

Figure 4 visualizes the collaboration network across 60 top institutions that produced the most cybercrime and cybersecurity research. In other words, these institutions have the most active researchers in cybercrime and cybersecurity community. Each node and label represent a research institution, in which the node size indicates the institution's importance in the entire network as measured by its productivity or the number of publications produced. Identical to the result of Table 3, we can see that Michigan State University, shown as the largest node in the network, was clearly the most productive research institution in the fields.

For example, among all lines associated with Michigan State University, the thickest line connects the node University of South Florida. This suggests that scholars in Michigan State most frequently collaborated with scholars in University of South Florida as compared to other institutions. It is possible that two nodes are very close to each other in distance but linked by a rather thin curved line. The institutions located at the periphery of the map may have closely collaborated with certain other institutions, but their collaboration networks were typically much more limited compared to the institutions situated at more centered positions of the map. For example, Huazhong University of Science & Technology in China had rather strong collaboration with Queensland University of Technology in Australia, as indicated by a relatively thick line between the two; however, other than Queensland University, Huazhong University had no other collaborative partner in this entire network system.

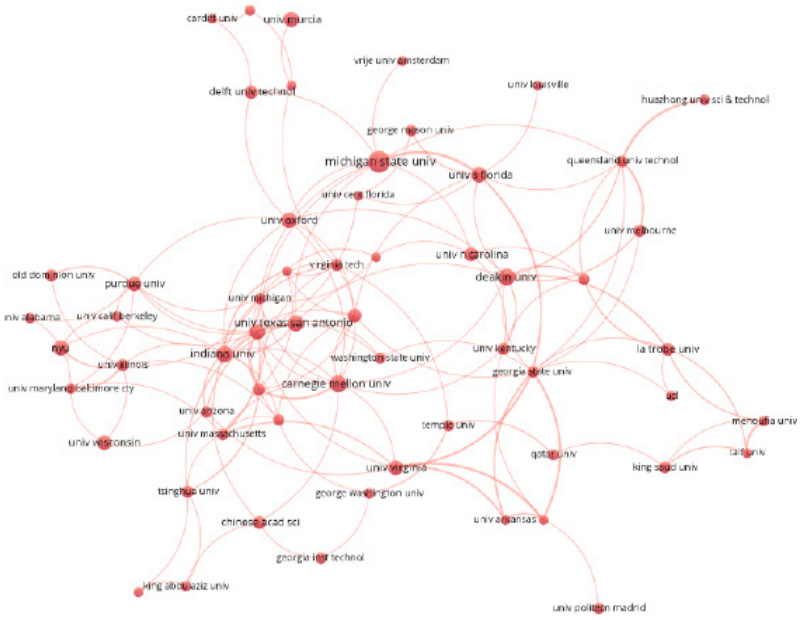


Figure 4. Institutional Collaboration Network

Most Cited Publications

Table 4. *The 10 Most Cited Research Articles/books*

Rank	Author(s)	Year	Title	Journal/Publisher
1	Cohen & Felson	1979	Social change and crime rate trends: A routine activity approach	American Sociological Review
2	Holt & Bossler	2009	Examining the applicability of lifestyle-routine activities theory for cybercrime victimization	Deviant Behavior
3	Wall	2007	Cybercrime: The transformation of crime in the information age	Polity
4	Bossler & Holt	2009	On-line activities, guardianship, and malware infection: An examination of routine activities theory.	International Journal of Cyber Criminology
5	Yar	2005	The novelty of 'cybercrime' an assessment in light of routine activity theory	European Journal of Criminology
6	Holt & Bossler	2014	An assessment of the current state of cybercrime scholarship	Deviant Behavior
7	Buczak & Guven	2016	A survey of data mining and machine learning methods for cyber security intrusion detection	IEEE Communications Surveys & Tutorials
8	Gottfredson & Hirschi	1990	A general theory of crime	Stanford University Press
9	Bossler & Holt	2010	The effect of self-control on victimization in the cyberworld	Journal of Criminal Justice
15	Ngo & Paternoster	2011	Cybercrime victimization: An examination of individual and situational level factors	International Journal of Cyber Criminology

All quoted references across each of the 3,635 publications included in the current study were analyzed. Table 4 lists the top ten most cited works by cybercrime and cybersecurity researchers. Nine out of ten publications were journal articles or books written by criminologists, with the exception of Buczak & Guven (2016). Two publications on classical criminological theories – routine activity theory (Cohen & Felson, 1979) and self-control theory (Gottfredson & Hirschi, 1990) – were well-established before the cyberage but have been revisited by cybercrime and cybersecurity researchers in recent years. This may suggest that routine activity theory and self-control theory are either among the most tested theories or most commonly used theoretical frameworks across the cybercrime and cybersecurity literature. This criminologist-dominated pattern was also evident across the top 30 most-cited works (not listed here due to space limitations). All but three of the top 30 most-cited publications were works from criminologists; more specifically, two publications discussed cybersecurity from computer science methodological perspectives, data mining and machine learning methods for cyber security intrusion detection (Buczak & Guven, 2016) and anomaly detection (Chandola et al., 2009), while the third publication discussed employee compliance through the lens of a business organization's information security policy (Bulgurcu et al., 2010). In all, this suggests that criminologists play an important role in leading the theoretical direction of the cybercrime and cybersecurity fields. Criminological thinking and research remain "central to the search for answers to the astounding questions of law and order in the twenty-first century cyber space" (Ndubueze, 2017, p. 70).

Keyword Analysis

Keyword Network Analysis

Keywords are scientific terms that present an ideal summary of a study as they often reflect the primary topics and subtopics addressed in the publications, including the most important techniques used. The keywords supplied by authors in the existing literature provided a simplified profile of the main contents of publications. All synonymous keywords in the original keyword pool were standardized to improve the keyword network visualization results. Top 90 high-frequency keywords were identified among all unique keywords included in 3,635 publications. We then examined the co-occurrence relationships among these top 90 high-frequency keywords and visualized co-word networks using VOSviewer software.

The map in Figure 5 shows the distribution of keywords across all areas of cybercrime and cybersecurity research. The map represents the relational network of 90 major keywords.. Two keywords are linked by a thicker line, if these two keywords are more frequently used as keywords simultaneously in each publication. Inter-keywords distance indicates the relatedness of any two keywords, as measured by their co-occurrence likelihood. The closer two keywords are located to each other, the two corresponding topics (or subtopics) are more intellectually related.

As shown in Figure 5, the 90 most frequent keywords were grouped into three theme clusters: the cybersecurity cluster, at the center (green); the cybercrime cluster, at the bottom right (blue); and the machine learning cluster, at the bottom left corner (red). The group of keywords closely associated with cybercrime were generally related to human behaviors or conditions, such as deterrence, awareness, personality, fear appeals, routine activities, behavior, victimization, and fraud. Some topics belong to the cybercrime cluster, but are also relatively closely related with cybersecurity, included health, trust, decision-making, impact, technology, and information. The cybersecurity cluster contained major substantive

or methodological areas to deal with cybercrime challenges, such as software, systems, model, framework, design, management, and others. The machine learning cluster included keywords about technologies and methods we applied in cybersecurity, such as deep learning, prediction, data mining, feature extraction, intrusion detection, etc. Machine learning cluster is closely tied into and inextricably intertwined with the cybersecurity cluster.

This topic-based analysis reflects the earlier discussion of the current state of cybercrime and cybersecurity scholarship in the literature review. There is very little study focusing on the interaction between cybercrime and cybersecurity and the justice process (Smith et al., 2004). Therefore, this study provides further justification for the need to expend cybercrime and cybersecurity research to all major components in criminal justice system, such as law enforcement, courts, and corrections (Holt & Bossler, 2014). There is thus a need to broaden the horizon of cybercrime and cybersecurity research even within the discipline of criminal justice. In addition, even though the cybercrime and cybersecurity clusters were linked with each other, the research topics in both groups were relatively separated, as indicated by a rather clear separation of the cybercrime and cybersecurity clusters in the map.

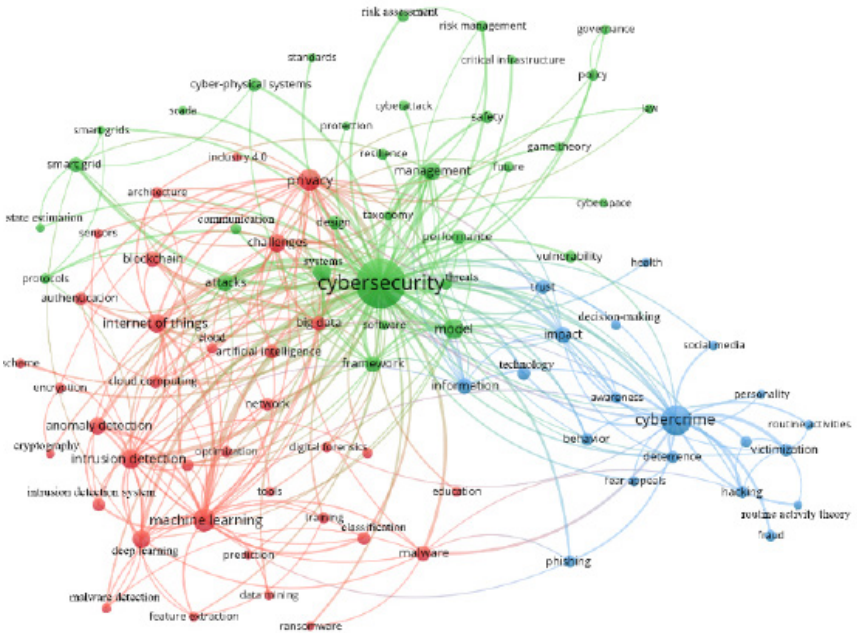


Figure 5. Co-occurrence Network of Top 90 High-frequency Keywords

Temporal Evolution of Keywords

Research in certain fields may evolve over time as topics, sub-topics, and techniques advance. Thus, examining the temporal change of keywords can provide a glimpse of how a research field changes over time.

To examine the temporal evolution of keywords, the 40 most frequently used keywords among all 3,635 publications between 1995 and 2021 were ranked (Table 5). To identify specific popular topics and subtopics within the cybercrime and cybersecurity fields, the general keywords "cybercrime" and "cybersecurity," which were initially used to retrieve all publications, as well as their synonymous keywords from ranking, were excluded. The timeframe was then divided into three consecutive periods: 1995-2011, 2012-2016, and 2017-2021. In each period, the 40 high-frequency keywords were re-ranked to represent the relative popularity of each topic or subtopic in the cybercrime and cybersecurity fields. The frequency of most keywords has increased over time, likely in correlation with the growth of the number of publications that contain a specific keyword (N) in the corresponding period. However, this growth is largely due to the expansion of cybercrime and cybersecurity literature in general.

These 40 high-frequency keywords were viewed as a proxy of 40 major topics and subtopics within the fields of cybercrime and cybersecurity. A comparison of how each keyword is utilized in literature over time can therefore illustrate the momentum of different topics in cybercrime and cybersecurity research, including their emergence, increase in popularity, or decrease in popularity. In the first period, 21 topics and subtopics later seen across cybercrime and cybersecurity research were not seen at all. As shown in Table 5, these 21 keywords were not ranked because they were simply not included in any publication. Interestingly, some of these previously neglected topics and subtopics emerged in the second period. As seen in the frequency (N) and rank (R), thirteen new keywords appeared in publications during this period. Despite the fact that these topics or subtopics started to emerge, scholarly attention in these areas was very limited. A typical example is the subtopic of deep learning: It was only used as a keyword in one publication in this period, and therefore it earned a very low absolute rank (495th) among all keywords. In the third period, eight topics became the most recent additions to the cybercrime and cybersecurity literature, including blockchain, artificial intelligence, training, intrusion detection system, feature extraction, decision making, tools, and Covid 19.

In cases in which the ranking of a keyword consistently rose over the most recent two periods, the trend of the keyword was labeled as "rising" to note that the keywords occurred with increasing relative popularity in scholarly articles. Table 5 identifies 23 keywords that have risen in popularity over the past 10 years. The most noticeable rising subtopic is "deep learning (DL)," which saw a dramatic jump in popularity – rising from 495th place in the second period to sixth place in the third period. Similarly, the rank of "machine learning (ML)" rose from 45th place in the second period to third place in the most recent period. This dramatic jump in rankings was likely due to the recent development of DL and ML methods and applications in cybersecurity. DL is a type of ML, and both are a subset of artificial intelligence. The aim of these areas is to train machines with the ability to automatically learn and act based on previous experience. The main difference between DL and ML is in their feature extraction and classification method. Different from ML, DL does not necessarily need to establish structured data to classify the objects but process unstructured data through different layers of neural networks. Due to the significantly increased popularity of ML and DL, topics related to ML/DL methodologies such as "training", "feature extraction", and "classification" also emerged as "rising" new additions to cybercrime and cybersecurity fields. In all, topics and subtopics– machine learning, Internet of Things, deep learning, intrusion detection, and blockchain – are now among the most popular topics or subtopics today.

As shown in Figure 5 and Table 5, among 40 high-frequency keywords, six topics were closely and directly related to cybercrime and criminology, including "deterrence", "victimization", "phishing", "policing",

Table 5. T*emporal Evolution of The 40 High-frequency Keywords*

Keywords	Gross (1995-2021)		Period one (1995-2011)		Period two (2012-2016)		Period three (2017-2021)		Trend
	N	**R**	**N**	**R**	**N**	**R**	**N**	**R**	
Machine learning	195	1	1	232	4	45	190	3	Rising
Internet of Things	123	2	0	NaN	6	21	117	5	Rising
Deep learning	110	3	0	NaN	1	495	109	6	Rising
Privacy	87	4	1	272	16	5	70	10	
Intrusion detection	85	5	2	49	6	22	77	8	Rising
Malware	78	6	3	17	14	8	61	13	
Blockchain	74	7	0	NaN	0	NaN	74	9	Rising
Anomaly detection	67	8	2	23	3	53	62	12	
Smart grid	65	9	5	9	7	19	53	15	
Artificial intelligence	58	10	0	NaN	0	NaN	58	14	Rising
Hacking	56	11	1	188	15	7	40	23	
Cloud computing	53	12	4	10	5	25	44	18	
Phishing	51	13	0	NaN	5	34	46	17	Rising
Big data	48	14	0	NaN	5	24	43	20	Rising
Cyber physical systems	43	15	0	NaN	2	126	41	21	Rising
Risk assessment	37	16	2	69	3	75	32	26	
Risk management	36	17	3	21	3	76	30	29	
Digital forensics	34	18	2	38	5	28	27	31	
Training	34	19	0	NaN	0	NaN	34	24	Rising
Intrusion detection system	33	20	0	NaN	0	NaN	33	25	Rising
Authentication	32	21	0	NaN	1	325	31	27	Rising
Network security	31	22	3	19	3	68	25	37	
Resilience	31	23	0	NaN	2	235	29	30	Rising
Victimization	29	24	2	77	0	NaN	27	33	
Fraud	28	25	3	16	5	30	20	48	
Data mining	27	26	3	15	1	486	23	39	
Feature extraction	27	27	0	NaN	0	NaN	27	32	Rising
Protocols	27	28	0	NaN	1	898	26	35	Rising
Policing	26	29	2	64	8	15	16	68	
Game theory	25	30	0	NaN	3	59	22	43	Rising
Ransomware	25	31	0	NaN	1	910	24	38	Rising
Sensors	24	32	0	NaN	1	964	23	41	Rising
Decision making	23	33	0	NaN	0	NaN	23	40	Rising
Risk	23	34	1	281	8	16	14	85	
Tools	23	35	0	NaN	0	NaN	23	42	Rising
Deterrence	22	36	1	145	4	44	17	59	
Encryption	22	37	0	NaN	2	152	20	47	Rising
Classification	21	38	1	101	0	NaN	20	46	
Covid 19	21	39	0	NaN	0	NaN	21	45	Rising
Cryptography	21	40	0	NaN	2	119	19	49	Rising

(*N, the number of publications that contain a specific keyword in the corresponding period; R, the absolute rank of keywords. "NaN" value in rank means no such author keyword in any publication in the corresponding period.)

"malware", and "digital forensic". Among these six topics, the only topic considered as "rising" is the "phishing" keyword, which belongs to the cybercrime cluster but was also linked with the cybercrime and cybersecurity clusters. Even though the "malware" and "digital forensic" topics were essentially related to cybercrime, these two topics were automatically grouped into machine learning cluster based on overall network constellation. Similar to most topics related to cybercrime, "policing" was not considered as a rising topic. Even through the number of articles that included "policing" as a key term increased throughout all periods, the relative rank of this keyword did not increase recently. Altogether, these findings suggest that, in general, most topics related to all three clusters continuously and increasingly attracted scholarly attention and contributions from social and computational scientists. However, topics related to cybersecurity and machine learning appeared to outpace their counterparts related to cybercrime.

Figure 6 visualizes the temporal evolution of the 90 high-frequency keywords over the recent five years (2017-2021). Similar to Figure 5, these 90 keywords included in all publications are visualized using VOSviewer software. However, in contrast to Figure 5, the color of each node in Figure 6 does not distinguish its theme cluster, but rather serves as a temporal indicator corresponding to the continuous color bar scaled between 2017 (in warmer, yellow color) and 2021 (in cooler, purple color). More specifically, the nodes in warmer colors represent the most recent popular topics and subtopics, while the nodes in cooler colors correspond to popular topics in earlier years. When three theme clusters are considered in whole, the machine learning cluster was obviously the most recent sought-after areas of study, followed by the cybersecurity and cybercrime clusters, respectively. Topics within each theme cluster also show temporal variation in popularity. For example, in the cybercrime cluster, "social media", "victimization", "deterrence" and "fear appeals" were relatively newer popular topics compared to "routine activity", "hacking," and "fraud." Similarly, in the machine learning cluster, "intrusion detection" and "optimization" were slightly older topics compared with the topics in yellow color.

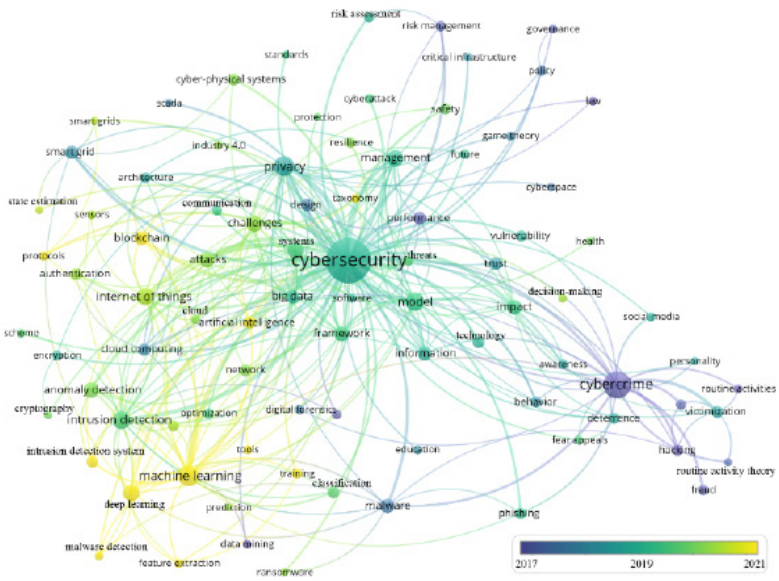


Figure 6. Temporal Evolution of The Most Frequently Used Keywords in The Recent 5 Years

Attention should be paid towards nodes in yellow color, which are topics and subtopics which have enjoyed the highest relative level of scholarly attentions recently. Yellow nodes include "machine learning", "deep learning", "training", "blockchain", "feature extraction", "artificial intelligence." This further validates the results presented in Table 5. In addition, even though machine learning, deep learning, and blockchain are all relatively large nodes in the yellow cluster, ML and DL are linked by a thicker and much shorter line, while blockchain is located at a distance with the former two. This suggests a strong intellectual linkage between ML and DL, but not necessarily between ML/DL and blockchain.

Conclusion and Discussion

Research interests in cybercrime and cybersecurity has exploded in recent years (Gangwar & Narang, 2022). This study utilized a bibliometric method to examine global trends of cybercrime and cybersecurity research over the past 26 years. The purpose of this study was to comprehensively depict this scientific landscape in the hope of providing multiple perspectives to examine the cybercrime and cybersecurity scholarship. As the title of this paper emphasizes, this research aimed to depict such trends in the most popular and comprehensive database (Web of Science) largely used by criminologists and (computational) social scientists.

We first examined the general trend across 3,635 publications over time, and the productivity of scholarly works across countries, institutions, journals, and subject categories. Results show that the cybercrime and cybersecurity are emergent and booming research fields as indicated by the fast and consistent growth trajectory of related publications. The fields continue to draw new researchers, facilitate collaboration across related fields, and foster the growth of a scientific knowledge base for future research. This study offers researchers – especially those new to the fields – a starting point through which to explore key resources and directions. For example, novice researchers may be unaware of the volume or scope of key publishing venues, especially given the absence of the terms "cybercrime" and "cybersecurity" in the titles of the most productive journals in these domains.

We then identified research collaboration networks and the major players and clusters in these collaboration networks. The results suggest that cybercrime and cybersecurity research has grown on a global scale. As Jaishankar (2010) pointed out, "cyberspace has defied the boundaries and has made geography irrelevant," as it does for cybercrime and cybersecurity research. The international collaboration network map suggests that the United States is the main hub for international collaborative research, even though most U.S.-based research involves domestic collaboration. The institutional collaboration network map identifies major institutions with which the most active cybercrime and cybersecurity researchers hold affiliations, such as Michigan State University. The map also clearly shows the collaboration network among these top-producing institutions. Both international and institutional collaboration networks are clustered. Scholars who are interested in future collaboration opportunities may wish to reference our visualization results for international and institutional collaboration networks to build and expand their own research networks or to join an existing network accessible to them either socially or geographically.

Our research also identified the most cited works in cybercrime and cybersecurity fields allowing scholars to rethink theoretical and methodological contexts for their future research. This study found that the theoretical contexts are largely dominated by the criminologist perspective because criminologists have

produced the majority of the top-cited works. This further confirms that criminologists play an important role in leading the theoretical direction of the cybercrime and cybersecurity fields. Admittedly, it is likely that such influence stems from a small group of criminologists because cybercrime is a rather new area in criminal justice and criminologists specializing in the fields are limited in number. Given recent calls for novel theoretical development, particularly in criminology (Lemke et al. 2022), the findings reported here may be leveraged to introduce needed theoretical heterogeneity in the cybercrime and cybersecurity fields.

In addition, we identified all important topics and subtopics within cybercrime and cybersecurity literature based on a network analysis of high-frequency keywords. Such analysis not only identified major topics and subtopics in cybercrime and cybersecurity fields, but also charted a linkage or co-occurrence pattern among these topics. Scholars intending to explore one specific topic can simultaneously consider those nearby topics and subtopics and those linked with a thicker line in the network map, as the latter may be intellectually related to the former as reflected in existing literature. In so doing, researchers can potentially transcend the siloed configuration of current scholarship by identifying new collaborators based on overlapping research interests that would otherwise be latent.

Finally, the scholarly interests and collective attention paid to specific topics may change over time. Once heavily studied, some topics may lose popularity among researchers, while other emergent topics may gain momentum moving forward. Visualization of the temporal evolution of keywords can help scholars get a better sense of the rise or decline in trends for specific research topics. This study identified 23 topics and subtopics that have risen in popularity over the past ten years. Eight topics became the most recent additions to the cybercrime and cybersecurity literature, including blockchain, artificial intelligence, training, intrusion detection system, feature extraction, decision making, tools, and Covid 19. In all, topics and subtopics– machine learning, Internet of Things, deep learning, intrusion detection, and blockchain – are among the most popular subtopics today.

Although this study had several strengths, there were also a few limitations. Most notably, the Web of Science core collection database that this study was based on may not include some relevant computer science papers. Thus, despite the relatively large number of articles included in this study, it is possible that the findings reported here may be somewhat altered with the inclusion of missing articles. Of note, the authors are currently planning a follow-up study to specifically examine such trends in the computer science database. Additionally, the rapidly changing landscape of cybercrime and cybersecurity research may indicate that literature reviews may become obsolete within a relatively short period of time. However, the timeframe of the current study is quite recent, as it includes articles as recent as 2021; thus, the methodology employed here likely maximizes its contemporary relevance. Finally, as is the case with bibliometric methods in general (Wallin, 2005), the findings reported here are methodology-dependent and potentially sensitive to the approach employed by the authors. The authors' combined methodological and content expertise lend support to the validity of the research design decisions that were made in this review.

Despite these limitations, it is our hope that the findings presented here will not only help scholars understand the changing landscape of cybercrime and cybersecurity research, but they could also provide scholars with a strong knowledge base as they set out to plan their own research and collaboration. As the state of cybercrime and cybersecurity science continues to grow and evolve, it is critical to continue to conduct and report studies such as the one reported here that holistically map the empirical landscape. By

doing so, both established and novice researchers can better identify publishing venues, establish novel interdisciplinary collaborations, and stay abreast of emerging topics and subtopics, with potentially transformative impacts on cybercrime and cybersecurity science as a whole.

Reference

Abu-Ulbeh, W., Altalhi, M., Abualigah, L., Almazroi, A. A., Sumari, P., & Gandomi, A. H. (2021). Cyberstalking victimization model using criminological theory: A systematic literature review, taxonomies, applications, tools, and validations. *Electronics*, *10*(14), 1670.

Aria, M., & Cuccurullo, C. (2017). Regular article bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, *11*(4), 959-975.

Birkle, C., Pendlebury, D. A., Schnell, J., & Adams, J. (2020). Web of Science as a data source for research on scientific and scholarly activity. *Quantitative Science Studies*, *1*(1), 363-376.

Bossler, A. M. (2017). Need for debate on the implications of honeypot data for restrictive deterrence policies in cyberspace. *Criminology & Public Policy*, *16*(3), 681-688.

Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. Policing: *An International Journal of Police Strategies and Management*, *35*(1), 165-181.

Bossler, A. M., & Berenblum, T. (2019) Introduction: new directions in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495-499.

Brands, J., & Van Doorn, J. (2022). The measurement, intensity and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior*, *127*, 107082.

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153-1176.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *Management Information Systems Quarterly*, *34*(3), 523-548.

Carroll, M. W., & Schrader, R. (1995). Computer-related crimes. *American Criminal Law Review*, *32*(2), 183 -211.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, *4 1*(3), 1-58.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588-608.

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2022). Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. *Policing and Society*, *32*(1), 103-124.

Coutorie, L. (1995). The future of high-technology crime: A parallel Delphi study. *Journal of Criminal Justice, 23*(1), 13-27.

Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal*, 0032258X221107584.

DeTardo-Bora, K. A., & Bora, D. J. (2016) Chapter 8: Cybercrimes: An overview of contemporary challenges and impending threats. In J. Sammons, (Eds.), *Digital forensics: Threatscape and best practices* (pp. 119-132). Syngress. ISBN: 978-0128045268

Ding Y, Chowdhury, G. G, & Foo, S. (2001). Bibliometric cartography of information retrieval research by using co-word analysis. *Information Processing & Management*, *37*(6), 817–842.

Edelmann, A., Wolff, T., Montagne, D., & Bail, C. A. (2020). Computational Social Science and Sociology. *Annual Review of Sociology*, *46*, 61-81.

FBI (2021). Internet Crime Report 2020. Federal Bureau of Investigation. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

Finklea, K. M., & Theohary, C. A. (2012). Cybercrime: Conceptual issues for congress and U.S. law enforcement. *Journal of Current Issues in Crime, Law & Law Enforcement, 5*(1/2), 1-27.

Gangwar, S., & Narang, V. (2022). A survey on emerging cyber crimes and their impact worldwide. In *research anthology on combating cyber-aggression and online negativity* (pp. 1583-1595). IGI Global.

Glänzel, W., & Schubert, A. (2005). Analyzing scientific networks through co-authorship. In F. Moed et al. (Eds.), *Handbook of quantitative science and technology research* (pp. 257-276).

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*(1), 13-20.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies, 10*(2), 243-249.

Halder, D., & Jaishankar, K. (2015). Irrational coping theory and positive criminology: A frame work to protect victims of cyber crime. In N. Ronel & D. Segev (Eds.), *Positive criminology* (pp. 276 -291). Routledge.

Harnad, S. (2009). Open access scientometrics and the UK Research Assessment Exercise. *Scientometrics, 79*(1), 147-156.

He, Y., & Hui, S. (2002). Mining a web citation database for author co-citation analysis. *Information processing & Management, 38*(4), 491-508.

Herath, T. B., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: a systematic literature review. *Journal of Cybersecurity and Privacy, 2*(1), 1-18.

Hofman, J.M., Watts, D. J., Athey, S., Garip, F., Griffiths, T. L., Kleinberg, J., Margetts, H., Mullanathan, S., Salganik, M. J., Vazire, S., Vespignani, A., & Yarkoni, T. (2021). Integrating explanation and prediction in computational social science. *Nature, 595*, 181-188.

Holt, T. J. (2017). Situating the problem of cybercrime in a multidisciplinary context. In Y. J.

Holt (Ed.), *Cybercrime through an interdisciplinary lens* (pp.1-16).

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40.

Holt, T., Bossler, A. M., & Spellar, S. K. (2015). *Cybercrime and digital forensics: An introduction*. New York, NY: Routledge.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology, 1*(1), 1-6.

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmallager & M. Pittaro, (Eds.), *Crimes of the Internet* (pp.283-301). Prentice Hall.

Jaishankar, K. (2010). The future of cyber criminology: Challenges and opportunities. *International Journal of Cyber Criminology, 4*(1&2), 26-31.

Jaishankar, K. (2015). "*Cyber crime victimization: New wine into old wineskins?*", Keynote Speech at the 15th World Society of Victimology Symposium, July 5-9, 2015, at Perth, Australia, organized by Victim Support, Angelhands Inc. and supported by Australian Institute of Criminology.

Jaishankar, K. (2018). Cyber criminology as an academic discipline. *International Journal of Cyber Criminology, 12*(1), 1-8.

Kubic, T. T. (2001). *The FBI's Perspective on the Cybercrime Problem Rouse*. Washington, 2001. Retrieved from https://archives.fbi.gov/archives/news/testimony/the-fbis-perspective-onthe-cybercrime-problem

Lazer, D., Pentland, A., Adamic, L., Aral, S., Barabasi, A. L., Brewer, D., Christakis, N., Contractor, N., Fowler, J., Gutman, M., Jebara, T., King, G., Macy, M., Roy, D., & Van Alstyne, M. (2009). Computational social science. *Science, 323*(5915), 721-723.

Lemke, M. K., Wolf, D. A., & Drake, S. A. (2022). A call for complex systems and syndemic theory in firearm violence research. *American Journal of Preventive Medicine, 62*(3), 459-465.

Li, Q., Wei, W., Xiong N., Feng D., Ye, X., & Jiang, Y. (2017). Social media research, human behavior, and sustainable society. *Sustainability, 9*(3), 384-394.

Moneva, A., Leukfeldt, E. R., Van De Weijer, S. G., & Miró-Llinares, F. (2022). Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective. *Computers in Human Behavior, 126*, 106984.

Morgan, S. (2019). *Global cybersecurity spending predicted to exceed $1 trillion from 2017-2021*. Retrieved from https://cybersecurityventures.com/cybersecurity-market-report/.

Ndubueze, P. N. (2017). *Cyber Criminology and Technology-Assisted Crime Control: A Reader*. Ahmadu Bello University Press Ltd.

Ngo, F. T., & Jaishankar, K. (2017). Commemorating a decade in existence of the International Journal of Cyber Criminology: A research agenda to advance the scholarship on cyber crime. *International Journal of Cyber Criminology, 11*(1), 1-9.

Nodeland, B., & Belshaw, S., & Saber, M. (2019). Teaching cybersecurity to criminal justice majors. *Journal of Criminal Justice Education, 30*(1), 71-90.

Onyeji, O., Bazilian, M., & Bronk, C. (2014). Cyber security and critical energy infrastructure. *The Electricity Journal, 27*(2), 52-60.

Panda Security (2020). 43 COVID-19 Cybersecurity Statistics. Panda Security. Retrieved from https://www.pandasecurity.com/mediacenter/news/covid-cybersecurity-statistics.

Payne, B. K., & Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research: An examination. *International Journal of Cyber Criminology, 14*(1), 81-105.

Peng, Q., & Ye, X. (2021). Research trends in social media/big data with the emphasis on data collection and data management: A bibliometric analysis. In A. Nara & M Tsou (Eds.), *Empowering Human Dynamics Research with Social Media and Geospatial Data Analytics* (pp. 47-63). Springer.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences, 2*(2), 379-398.

Prensky, M. (2001). Digital natives, digital immigrants. From on the horizon. *MCB University Press, 9*(5), October 2001.

Rebovich, D., & Byrne, J. M. (Eds.). (2022). *The new technology of financial crime: new crime commission technology, new victims, new offenders, and new strategies for prevention and control*. Routledge.

Schmoch, U., & Schubert, T. (2007) Are international co-publications an indicator for quality of scientific research? *Scientometrics, 74*, 361-377.

Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial*. Cambridge University Press.

Stambaugh, H., Beaupre, D. S., Icove, D. J., Baker, R., Cassaday, W., & Williams, W. P. (2001). *Electronic Crime Needs assessment for state and local law enforcement*. National Institute of Justice Research Report. Retrieved from https://www.ojp.gov/pdffiles1/nij/186276.pdf.

Taylor, R. W., Fritsch, E. J., Liederbach, J., & Holt, T.J. (2019). *Digital crime and digital terrorism*. 3rd Pearson Prentice Hall.

Van Eck, N. J., & Waltman, L. (2010) Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics, 84*, 523–538.

Wade, M. (2021). Digital hostages: Leveraging ransomware attacks in cyberspace. *Business Horizons, 64*(6), 787-797.

Wall, D. S. (2001). Cybercrimes and the internet. In D. S. Wall, (Eds.) *Crime and the Internet*. (pp. 1–17). New York, NY: Routledge.

Wallin, J. A. (2005). Bibliometric methods: Pitfalls and possibilities. *Basic & Clinical Pharmacology & Toxicology, 97*(5), 261-275.

Wu, L., Peng, Q., Lemke, M., Hu, T., & Gong, X. (2022). Spatial social network research: A bibliometric analysis. *Computational Urban Science, 2*(1), 1-13.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427.

Ye, X., & Leipnik, M. (2013). Comparison of the characteristics of small business in China and the US. *Perspectives on Global Development and Technology, 12*: 661-679.

Ye, X., Lian, Z., She, B., Qin, C., & Kudva, S. (2019). Spatial and big data analytics of e-market transaction in China. *GeoJournal*