SN

REVIEW PAPER

Check for
updates

Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis

Huong Thi Ngoc Ho[1] · Hai Thanh Luong[2] (ID)

Abstract

Research on cybercrime victimization is relatively diversified; however, no biblio-metric study has been found to introduce the panorama of this subject. The current study aims to address this research gap by performing a bibliometric analysis of 387 Social Science Citation Index articles relevant to cybercrime victimization from Web of Science database during the period of 2010–2020. The purpose of the article is to examine the research trend and distribution of publications by five main fields, including time, productive authors, prominent sources, active institutions, and lead-ing countries/regions. Furthermore, this study aims to determine the global collabo-rations and current gaps in research of cybercrime victimization. Findings indicated the decidedly upward trend of publications in the given period. The USA and its authors and institutions were likely to connect widely and took a crucial position in research of cybercrime victimization. Cyberbullying was identified as the most concerned issue over the years and cyber interpersonal crimes had the large number of research comparing to cyber-dependent crimes. Future research is suggested to concern more about sample of the elder and collect data in different countries which are not only European countries or the USA. Cross-nation research in less popu-lar continents in research map was recommended to be conducted more. This paper contributed an overview of scholarly status of cybercrime victimization through statistical evidence and visual findings; assisted researchers to optimize their own research direction; and supported authors and institutions to build strategies for research collaboration.

✉ Hai Thanh Luong
haithanh.luong@rmit.edu.au

Huong Thi Ngoc Ho
Huonghn252@gmail.com

[1] School of Journalism and Communication, Huazhong University of Science and Technology, Wuhan, Hubei, China

[2] School of Global, Urban and Social Studies, RMIT University, Melbourne, Australia

Introduction

To date, the debate of cybercrime definition has been controversial which is considered as one of the five areas of cyber criminology (Ngo and Jaishankar 2017; Drew 2020).[1] Several terms are used to illustrate 'cybercrime', such as 'high-tech crime' (Insa 2007), 'computer crime' (Choi 2008; Skinner and Fream 1997), 'digital crime' (Gogolin 2010), or 'virtual crime' (Brenner 2001). 'Cybercrime', however, has been the most popular in the public parlance (Wall 2004). A propensity considers crime directly against computer as cybercrime, while other tendency asserts that any crime committed via internet or related to a computer is cybercrime (Marsh and Melville 2008; Wall 2004). Hence, there is a distinction between 'true cybercrime' or 'high-tech' cybercrime and 'low-tech' cybercrime (Wagen and Pieters 2020). Council of Europe defines 'any criminal offense committed against or with the help of a computer network' as cybercrime (Abdullah and Jahan 2020, p. 90). Despite different approaches, cybercrime generally includes not only new types of crimes which have just occurred after the invention of computer and internet (Holt and Bossler 2014; Drew 2020) but also traditional types of crimes which took the advantages of information communication technology (ICT) as vehicle for illegal behaviors (Luong 2021; Nguyen and Luong 2020; Luong et al. 2019). Two main cybercrime categories identified, respectively, are cyber-dependent crime (hacking, malware, denial of service attacks) and cyber-enable crime (phishing, identity theft, cyber romance scam, online shopping fraud). Nevertheless, there are several different classifications of cybercrime such as cybercrime against certain individuals, groups of individuals, computer networks, computer users, critical infrastructures, virtual entities (Wagen and Pieters 2020); cyber-trespass, cyber-deceptions, cyber-pornography, and cyber-violence (Wall 2001).

Due to the common prevalence of cybercrime, the increasing threats of cybercrime victimization are obviously serious. Cybercrime victimization has become a crucial research subfield in recent years (Wagen and Pieters 2020). It is difficult to differ "forms of online victimization" and "acts that actually constitute a crime", then it is usual for researchers to focus less on perspective of criminal law and consider any negative experiences online as cybercrime (Näsi et al. 2015, p. 2). It was likely to lead to practical gaps between theory and practice in terms of investigating the nexus of offender and victims on cyberspace. In the light of literature review, numerous specific aspects of cybercrime victimization were investigated by questionnaire surveys or interview survey such as the prevalence of cybercrime victimization (Näsi et al. 2015; Whitty and Buchanan 2012); causes and predictors of cybercrime victimization (Abdullah and Jahan 2020; Algarni et al. 2017; Ilievski 2016; Jahankhani 2013; Kirwan et al. 2018; Näsi et al. 2015; Reyns et al. 2019; Saad

---

[1] In the 'commemorating a decade in existence of the International Journal of Cyber Criminoogy', Ngo and Jaishankar (2017) called for further research with focusing on five main areas in the Cyber Criminiology, including (1) defining and classifying cybercrime, (2) assessing the prevalence, nature, and trends of cybercrime, (3) advancing the field of cyber criminology, (4) documenting best practices in combating and preventing cybercrime, and (5) cybercrime and privacy issues.

et al. 2018); and the relationship between social networking sites (SNS) and cybercrime victimization (Das and Sahoo 2011; Algarni et al. 2017; Benson et al. 2015; Seng et al. 2018). To some extent, therefore, the current study examines cybercrime victimization in the large scale, referring to any negative experiences on cyberspace or computer systems. Nevertheless, no bibliometric analysis was found to show the research trend and general landscape of this domain.

Bibliometric is a kind of statistical analysis which uses information in a database to provide the depth insight into the development of a specified area (Leung et al. 2017). The present study aims to address this research gap by providing a bibliometric review of the relevant SSCI articles in WoS database during the period of 2010–2020. The pattern of publications, the productivity of main elements (authors, journals, institutions, and countries/regions), statistic of citations, classification of key terms, research gaps, and other collaborations will be presented and discussed in section four and five after reviewing literatures and presenting our methods conducted. This article contributes an overview of research achievements pertaining to cybercrime victimization in the given period through statistical evidence and visual findings; assists researchers to perceive clearly about the key positions in research maps of this field, and obtain more suggestions to develop their own research direction.

Literature review

Cybercrime victimization

Cybercrime victimization may exist in two levels including institutional and individual level (Näsi et al. 2015). For the former, victim is governments, institutions, or corporations, whereas for the latter, victim is a specific individual (Näsi et al. 2015). A wide range of previous studies concerned about individual level of victim and applied Lifestyle Exposure Theory (LET), Routine Activity Theory (RAT) and General Theory of Crime to explain cybercrime victimization (Choi 2008; Holt and Bossler 2009; Ngo and Paternoster 2011). Basing on these theories, situational and individual factors were supposed to play an important role in understanding cybercrime victimization (Choi 2008; Van Wilsem 2013). However, there was another argument that situational and individual factors did not predict cybercrime victimization (Ngo and Paternoster 2011; Wagen and Pieters 2020). Overall, most of those studies just focused only one distinctive kind of cybercrime such as computer viruses, malware infection, phishing, cyberbullying, online harassment, online defamation, identity theft, cyberstalking, online sexual solicitation, cyber romance scams or online consumer fraud. Referring to results of the prior research, some supported for the applicability of mentioned theories but other did not share the same viewpoint (Leukfeldt and Yar 2016). It was hard to evaluate the effect of LET or RAT for explanation of cybercrime victimization because the nature of examined cybercrime were different (Leukfeldt and Holt 2020; Leukfeldt and Yar 2016).

Previous research determined that cybercrime victimization was more common in younger group compared to older group because the young is the most active online

user (Näsi et al. 2015; Oksanen and Keipi 2013) and males tended to become victims of cybercrime more than females in general (Näsi et al. 2015). However, findings might be different in research which concerned specific types of cybercrime. Women were more likely to be victims of the online romance scam (Whitty and Buchanan 2012) and sexual harassment (Näsi et al. 2015), while men recorded higher rate of victimization of cyber-violence and defamation. Other demographic factors were also examined such as living areas (Näsi et al. 2015), education (Oksanen and Keipi 2013; Saad et al. 2018) and economic status (Oksanen and Keipi 2013; Saad et al. 2018). Furthermore, several prior studies focus on the association of psychological factors and cybercrime victimization, including awareness and perception (Ariola et al. 2018; Saridakis et al. 2016), personality (Kirwan et al. 2018; Orchard et al. 2014; Parrish et al. 2009), self-control (Ilievski 2016; Ngo and Paternoster 2011; Reyns et al. 2019), fear of cybercrime (Lee et al. 2019), online behaviors (Al-Nemrat and Benzaïd 2015; Saridakis et al. 2016). Psychological factors were assumed to have effects on cybercrime victimization at distinctive levels.

Another perspective which was much concerned by researchers was the relationship between cybercrime victimization and SNS. SNS has been a fertile land for cybercriminals due to the plenty of personal information shared, lack of guard, the availability of communication channels (Seng et al. 2018), and the networked nature of social media (Vishwanath 2015). When users disclosed their personal information, they turned themselves into prey for predators in cyberspace. Seng et al. (2018) did research to understand impact factors on user's decision to react and click on suspicious posts or links on Facebook. The findings indicated that participants' interactions with shared contents on SNS were affected by their relationship with author of those contents; they often ignored the location of shared posts; several warning signals of suspicious posts were not concerned. Additionally, Vishwanath (2015) indicated factors that led users to fall victims on the SNS; Algarni et al. (2017) investigated users' susceptibility to social engineering victimization on Facebook; and Kirwan et al. (2018) determined risk factors resulting in falling victims of SNS scam.

Bibliometric of cybercrime victimization

"Bibliometric" is a term which was coined by Pritchard in 1969 and a useful method which structures, quantifies bibliometric information to indicate the factors constituting the scientific research within a specific field (Serafin et al. 2019). Bibliometric method relies on some basic types of analysis, namely co-authorship, co-occurrence, citation, co-citation, and bibliographic coupling. This method was employed to various research domains such as criminology (Alalehto and Persson 2013), criminal law (Jamshed et al. 2020), marketing communication (Kim et al. 2019), social media (Chen et al. 2019; Gan and Wang 2014; Leung et al. 2017; Li et al. 2017; You et al. 2014; Zyoud et al. 2018), communication (Feeley 2008), advertising (Pasadeos 1985), education (Martí-Parreño et al. 2016).

Also, there are more and more scholars preferring to use bibliometric analysis on cyberspace-related subject such as: cyber behaviors (Serafin et al. 2019), cybersecurity

(Cojocaru and Cojocaru 2019), cyber parental control (Altarturi et al. 2020). Serafin et al. (2019) accessed the Scopus database to perform a bibliometric analysis of cyber behavior. All documents were published by four journals: *Cyberpsychology, Behavior and Social Networking* (ISSN: 21522723), *Cyberpsychology and Behavior* (ISSN: 10949313), *Computers in Human Behavior* (ISSN: 07475632) and *Human–Computer Interaction* (ISSN: 07370024), in duration of 2000–2018. Findings indicated the use of Facebook and other social media was the most common in research during this period, while psychological matters were less concerned (Serafin et al. 2019). Cojocaru and Cojocaru (2019) examined the research status of cybersecurity in the Republic of Moldavo, then made a comparison with the Eastern Europe countries' status. This study employed bibliometric analysis of publications from three data sources: National Bibliometric Instrument (database from Republic of Moldavo), Scopus Elsevier and WoS. The Republic of Moldavo had the moderate number of scientific publications on cybersecurity; Russian Federation, Poland, Romania, Czech Republic, and Ukraine were the leading countries in Eastern Europe area (Cojocaru and Cojocaru 2019). Altarturi et al. (2020) was interested in bibliometric analysis of cyber parental control, basing on publications between 2000 and 2019 in Scopus and WoS. This research identified some most used keywords including 'cyberbullying', 'bullying', 'adolescents' and 'adolescence', showing their crucial position in the domain of cyber parental control (Altarturi et al. 2020). 'Cyber victimization' and 'victimization' were also mentioned as the common keywords by Altarturi et al. (2020). Prior research much focus on how to protect children from cyberbullying. Besides, four online threats for children were determined: content, contact, conduct and commercial threats (Altarturi et al. 2020).

Generally, it has been recorded several published bibliometric analyses of cyber-related issues but remained a lack of bibliometric research targeting cybercrime victimization. Thus, the present study attempts to fill this gap, reviewing the achievements of existed publications as well as updating the research trend in this field.

In detail, our current study aims to address four research questions (RQs):

RQ1 What is overall distribution of publication based on year, institutions and countries, sources, and authors in cybercrime victimization?

RQ2 Which are the topmost cited publications in terms of cybercrime victimization?

RQ3 Who are the top co-authorships among authors, institutions, and countries in research cybercrime victimization?

RQ4 What are top keywords, co-occurrences and research gaps in the field of cybercrime victimization?

Table 1 Criteria for automatic filter

Criteria	
Timespan	2010–2020
Document types	Article (Exclude early access)
Language	English
Research areas	Psychology; Criminology penology
WoS index	Social Sciences Citation Index (SSCI)

Methods

Data collection procedure

Currently, among specific approaches in cybercrime's fileds, WoS is "one of the largest and comprehensive bibliographic data covering multidisciplinary areas" (Zyoud et al. 2018, p. 2). This paper retrieved data from the SSCI by searching publications of cybercrime victimization on WoS database to examine the growth of publication; top keywords; popular topics; research gaps; and top influential authors, institutions, countries, and journals in the academic community.

This paper employed Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) for data collection procedure. For timeline, we preferred to search between 2010 and 2020 on the WoS system with two main reasons. First, when the official update of the 2009 PRISMA Statement had ready upgraded with the specific guidelines and stable techniques, we consider beginning since 2010 that is timely to test. Secondly, although there are several publications from the early of 2021 to collect by the WoS, its updated articles will be continued until the end of the year. Therefore, we only searched until the end of 2020 to ensure the full updates.

To identify publications on cybercrime victimization, the study accessed WoS and used two keywords for searching: 'cybercrime victimization' or 'cyber victimization' after testing and looking for some terminology-related topics. Accordingly, the paper applied a combination of many other searching terms besides two selected words such as "online victimization", "victim of cybercrime", "phishing victimization", "online romance victimization", "cyberstalking victim", "interpersonal cybercrime victimization", or "sexting victimization", the results, however, were not really appropriate. A lot of papers did not contain search keywords in their titles, abstracts, keywords and were not relevant to study topic. After searching with many different terms and comparing the results, the current study selected the two search terms for the most appropriate articles. The query result consisted of 962 documents. Basing on the result from preliminary searching, retrieved publications were refined automatically on WoS by criteria of timespan, document types, language, research areas, and WoS Index as presented in Table 1. Accordingly, the criteria for automatic filter process were basic information of an articles and classified clearly in WoS system so the results reached high accuracy. The refined results are 473 articles.

After automatic filters, file of data was converted to Microsoft Excel 2016 for screening. The present study examined titles and abstracts of 473 articles to assess

the eligibility of each publication according to the relevance with given topic. There are 387 articles are eligible,while 86 irrelevant publications were excluded.

Data analysis

Prior to data analysis, the raw data were cleaned in Microsoft Excel 2016. Different forms of the same author's name were corrected for consistency, for example "Zhou, Zong-Kui" and "Zhou Zongkui", "Van Cleemput, Katrien" and "Van Cleemput, K.", "Williams, Matthew L." and "Williams, Matthew". Similarly, different keywords (single/plural or synonyms) used for the same concept were identified and standardized such as "victimization" and "victimisation"; "adolescent" and "adolescents"; "cyber bullying", "cyber-bullying" and "cyberbullying"; "routine activity theory" and "routine activities theory".

The data were processed by Microsoft Excel 2016 and VOS Viewer version 1.6.16; then it was analyzed according to three main aspects. First, descriptive statistic provided evidence for yearly distribution and growth trend of publications, frequency counts of citations, the influential authors, the predominant journals, the top institutions and countries/territories, most-cited publications. Second, co-authorship and co-occurrence analysis were constructed and visualized by VOS Viewer version 1.6.16 to explore the network collaborations. Finally, the current study also investigated research topics through content analysis of keywords. The authors' keywords were classified into 15 themes, including: #1 cybercrime; #2 sample and demographic factors; #3 location; #4 theory; #5 methodology; #6 technology, platforms and related others; #7 psychology and mental health; #8 physical health; #9 family; #10 school; #11 society; #12 crimes and deviant behaviors; #13 victim; #14 prevention and intervention; and #15 others. Besides, the study also added other keywords from titles and abstracts basing on these themes, then indicated aspects examined in previous research.

Results

In this section, all findings corresponding with four research questions identified at the ouset of this study would be illustrated (Fig. 1).

Distribution of publication

Distribution by year, institutions and countries

Basing on retrieved data, it was witnessed an increasing trend of articles relevant to cybercrime victimization in SSCI list during the time of 2010–2020 but it had slight fluctuations in each year as shown in Fig. 2. The total number of articles over this time was 387 items, which were broken into two sub-periods: 2010–2014 and 2015–2020. It is evident that the latter period demonstrated the superiority of the rate of articles (79.33%) compared to the previous period (20.67%). The yearly
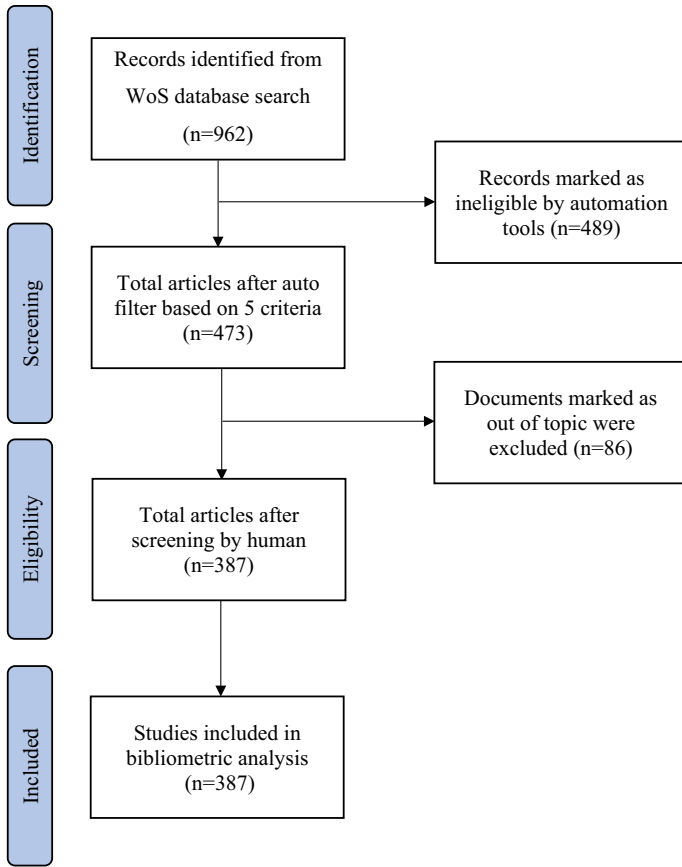
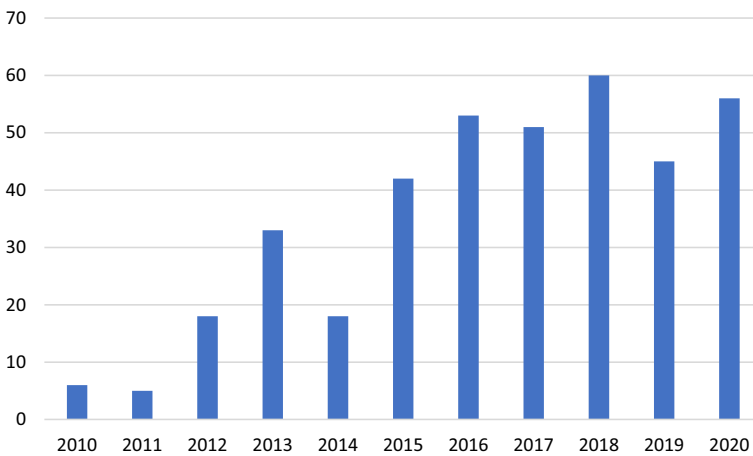**Fig. 1** PRISMA diagram depicts data collection from WoS database

Fig. 2 Annual distribution of publications

Table 2 Top contributing institutions based on total publications

Institutions	Countries	TP	TC	AC
Masaryk University	Czech Republic	17	191	11.24
Michigan State University	USA	16	290	18.13
University of Antwerp	Belgium	13	285	21.92
Weber State University	USA	10	265	26.50
Pennsylvania State University	USA	9	83	9.22
Democritus University of Thrace	Greece	8	214	26.75
University of Cordoba	Spain	8	484	60.50
University of Vienna	Austria	8	109	13.63
Edith Cowan University	Australia	7	256	36.57
University of Cincinnati	USA	7	254	36.29
University of Seville	Spain	7	495	70.71
University of Victoria	Australia	7	188	26.86

TP total publications, *TC* total citations for the publications reviewed, *AC* average citations per document

quantity of publications in this research subject was fewer than forty before 2015. Research of cybercrime victimization reached a noticeable development in 2016 with over fifty publications, remained the large number of publications in the following years and peaked at 60 items in 2018.

Distribution by institutions and countries

Table 2 shows the top contributing institutions according to the quantity of publications related to cybercrime victimization. Of the top institutions, four universities were from the USA, two ones were from Spain, two institutions were from Australia and the rest ones were from Czech Republic, Belgium, Greece, and Austria. Specifically, Masaryk University (17 documents) became the most productive publishing institution, closely followed by Michigan State University (16 documents). The third and fourth places were University of Antwerp (13 documents) and Weber State University (10 documents). Accordingly, the institutions from The USA and Europe occupied the vast majority.

In Table 2, University of Seville (total citations: 495, average citations: 70.71) ranked first and University of Cordoba (total citations: 484, average citations: 60.50) stayed at the second place in both total citations and average citations.

Referring to distribution of publications by countries, there were 45 countries in database contributing to the literature of cybercrime victimization. The USA recorded the highest quantity of papers, creating an overwhelming difference from other countries (159 documents) as illustrated in Fig. 3. Of the top productive countries, eight European countries which achieved total of 173 publications were England (39 documents), Spain (34 documents), Germany (22 documents), Netherlands (18 documents), Italy (17 documents) and Czech Republic (17 documents), Belgium (14 documents), Greece (12 documents). Australia ranked the fourth point (32
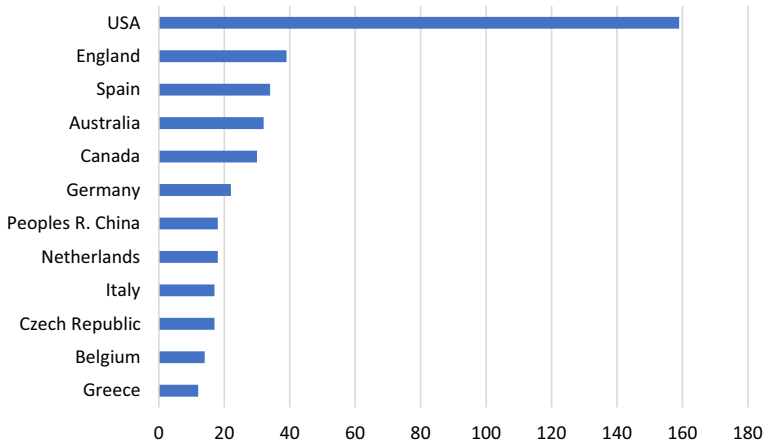
Fig. 3 Top productive countries based on the number of publications

Table 3 Top leading journals based on the quantity of publications

Journal Titles	TP	TC	AC	SPY
Computers in Human Behavior	56	2055	36.70	1985
Cyberpsychology, Behavior and Social Networking	24	554	23.08	1999
Journal of Youth and Adolescence	19	1285	67.63	1972
Aggressive Behavior	15	661	44.07	1974
Journal of Interpersonal Violence	14	370	26.43	1986
Cyberpsychology: Journal of Psychosocial Research on Cyberspace	13	73	5.62	2007
Journal of Adolescence	12	538	44.83	1978
Journal of School Violence	12	302	25.17	2002
Frontiers in Psychology	11	85	7.73	2010
School Psychology International	9	531	59.00	1979

SPY Started Publication Year

documents), followed by Canada (30 documents). One Asian country which came out seventh place, at the same position with Netherlands was China (18 documents).

Distribution by sources

Table 3 enumerates the top leading journals in the number of publications relevant to cybercrime victimization. The total publications of the first ranking journal—*Computers in Human Behavior* were 56, over twice as higher as the second raking journal—*Cyberpsychology, Behavior and Social Networking* (24 articles). Most of these journals have had long publishing history, starting their publications before 2000. Only three journals launched after 2000, consisting of *Journal of School Violence* (2002), *Cyberpsychology: Journal of Psychosocial*

Table 4 Top productive authors based on article count

Authors	TP	TC	AC
Wright, Michelle F	20	315	15.75
Holt, Thomas J	10	250	25.00
Reyns, Bradford W	10	265	26.50
Holfeld, Brett	8	110	13.75
Kokkinos, Constantinos M	8	214	26.75
Ortega-Ruiz, Rosario	8	483	60.38
Vandebosch, Heidi	8	185	23.13
Yanagida, Takuya	8	78	9.75
Leukfeldt, Rutger	7	165	23.57
Spiel, Christiane	7	107	15.29

Research on Cyberspace (2007) and *Frontiers in Psychology* (2010). Besides, it is remarked that one third of the top journals focuses on youth related issues: *Journal of Youth and Adolescence*, *Journal of Adolescence, School Psychology International* and *Journal of School Violence*.

In Table 3, relating to total citations, *Computers in Human Behavior* remained the first position with 2055 citations. *Journal of Youth and Adolescence* had total 1285 citations, ranked second and followed by *Aggressive Behavior* with 661 citations. In terms of average citations per documents, an article of *Journal of Youth and Adolescence* was cited 67.63 times in average, much higher than average citations of one in *Computers in Human Behavior* (36.70 times). The other journals which achieved the high number of average citations per document were *School Psychology International* (59.00 times), *Journal of Adolescence* (44.83 times) and *Aggressive Behavior* (44.07 times).

Distribution by authors

Table 4 displays ten productive authors based on article count; total citations of each author and their average citations per document are also included. Michelle F. Wright from Pennsylvania State University ranked first with twenty publications, twice as higher as the second positions, Thomas J. Holt (10 articles) from Michigan State University and Bradford W. Reyns (10 articles) from Weber State University. Rosario Ortega-Ruiz from University of Cordoba stayed at the third place in terms of total publications but the first place in aspect of total citations (483 citations) and the average citations (60.38 times).

Of the most productive authors based on total publications, there were three authors from universities in the USA; one from the university in Canada (Brett Holfeld); the others were from institutions in Euro, including Spain (Rosario Ortega-Ruiz), Greece (Constantinos M. Kokkinos) and Belgium (Heidi Vandebosch), Netherlands (Rutger Leukfeldt) and Austria (Takuya Yanagida and Christiane Spiel).

Most-cited publications

The most-cited literature items are displayed in Table 5. The article which recorded the highest number of citations was 'Psychological, Physical, and Academic Correlates of Cyberbullying and Traditional Bullying' (442 citations) by Robin M. Kowalski et al. published in *Journal of Adolescent Health*, 2013. Seven of ten most-cited articles were about cyberbullying; focused on youth population; made comparisons between cyberbullying and traditional bullying; analyzed the impact of several factors such as psychological, physical, academic factors or use of Internet; discussed on preventing strategies. The other publications studied victimization of cyberstalking and cyber dating abuse. All most-cited articles were from 2015 and earlier.

Of the top productive authors, only Bradford W. Reyns had an article appeared in the group of most-cited publications. His article 'Being Pursued Online: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization' (2011) was cited 172 times.

Co-authorship analysis

"Scientific collaboration is a complex social phenomenon in research" (Glänzel and Schubert 2006, p. 257) and becomes the increasing trend in individual, institutional and national levels. In bibliometric analysis, it is common to assess the productivity and international collaboration of research; identify key leading researchers, institutions, or countries (E Fonseca et al. 2016) as well as potential collaborators in a specific scientific area (Romero and Portillo-Salido 2019) by co-authorship analysis which constructs networks of authors and countries (Eck and Waltman 2020).

This section analyses international collaboration relevant to research of cybercrime victimization among authors, institutions, and countries during 2010–2020 through visualization of VOS Viewer software.

Collaboration between authors

Referring to the threshold of choose in this analysis, minimum number of documents of author is three and there were 80 authors for final results. Figure 4 illustrates the relationships between 80 scientists who study in subject of cybercrime victimization during 2010–2020. It shows several big groups of researchers (Wright's group, Vandebosch's group, or Holt's group), while numerous authors had limited or no connections to others (Sheri Bauman, Michelle K. Demaray or Jennifer D. Shapka).

Figure 5 displayed a significant network containing 23 authors who were active in collaboration in detail. The displayed items in Fig. 5 are divided into five clusters coded with distinctive colors, including red, green, blue, yellow, and purple.

Table 5 The most-cited publications in subject of cybercrime victimization during 2010–2020

| Title	Author	Source title	Year	TC
Psychological, Physical, and Academic Correlates of Cyberbullying and Traditional Bullying	Kowalski et al.	Journal of Adolescent Health	2013	442
The Nature of Cyberbullying, and Strategies for Prevention	Slonje et al.	Computers in Human Behavior	2013	323
Associations among Bullying, Cyberbullying, and Suicide in High School Students	Bauman et al.	Journal of Adolescence	2013	289
Longitudinal and Reciprocal Relations of Cyberbullying With Depression, Substance Use, and Problematic Internet Use Among Adolescents	Gamez-Guadix	Journal of Adolescent Health	2013	253
Peer and Cyber Aggression in Secondary School Students: The Role of Moral Disengagement, Hostile Attribution Bias, and Outcome Expectancies	Pornari et al.	Aggressive Behavior	2010	234
Cyber Bullying and Internalizing Difficulties: Above and Beyond the Impact of Traditional Forms of Bullying	Bonanno et al.	Journal of Youth and Adolescence	2013	205
The Rate of Cyber Dating Abuse Among Teens and How It Relates to Other Forms of Teen Dating Violence	Zweig et al.	Journal of Youth and Adolescence	2013	180
The Overlap Between Cyberbullying and Traditional Bullying	Waasdorp et al.	Journal of Adolescent Health	2015	178
A Longitudinal Study of Cyberbullying: Examining Risk and Protective Factors	Fanti et al.	European Journal of Developmental Psychology	2012	177
Being Pursued Online: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization	Reyns et al.	Criminal Justice and Behavior	2011	172
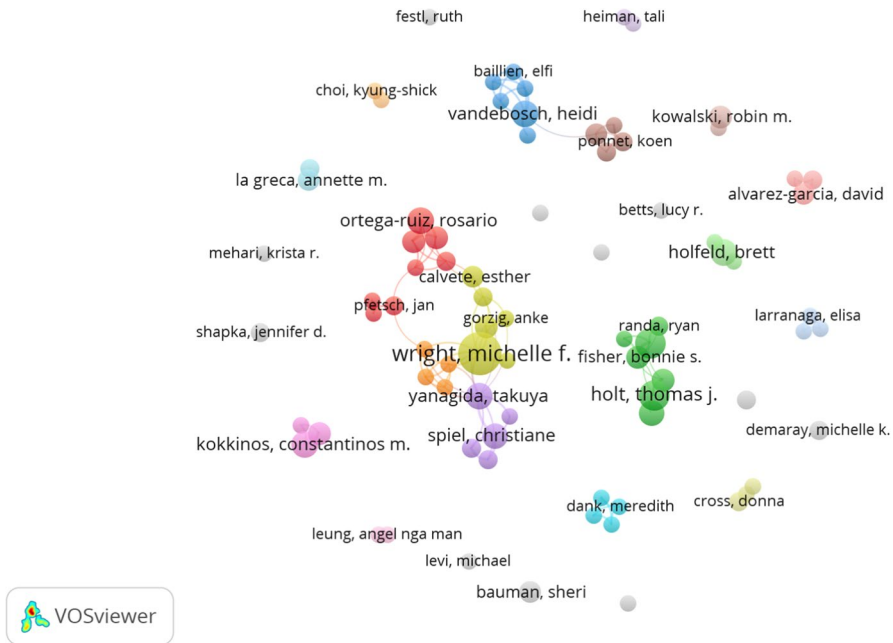
Fig. 4 Collaboration among authors via network visualization (threshold three articles for an author, displayed 80 authors)
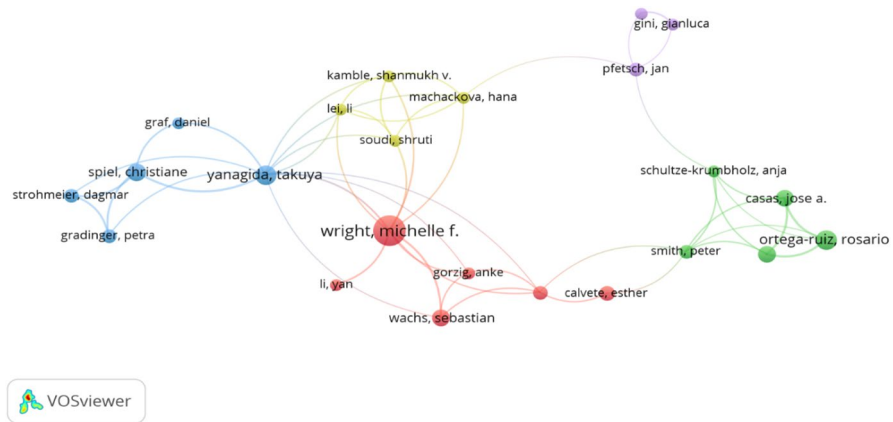

Fig. 5 Collaboration among authors via network visualization (threshold three articles for an author, displayed 23 authors)

Each author item was represented by their label and a circle; the size of label and circle are depended on the weight of the item, measured by the total publications (Eck and Waltman 2020). The thickness of lines depends on the strength of collaboration (Eck and Waltman 2020).
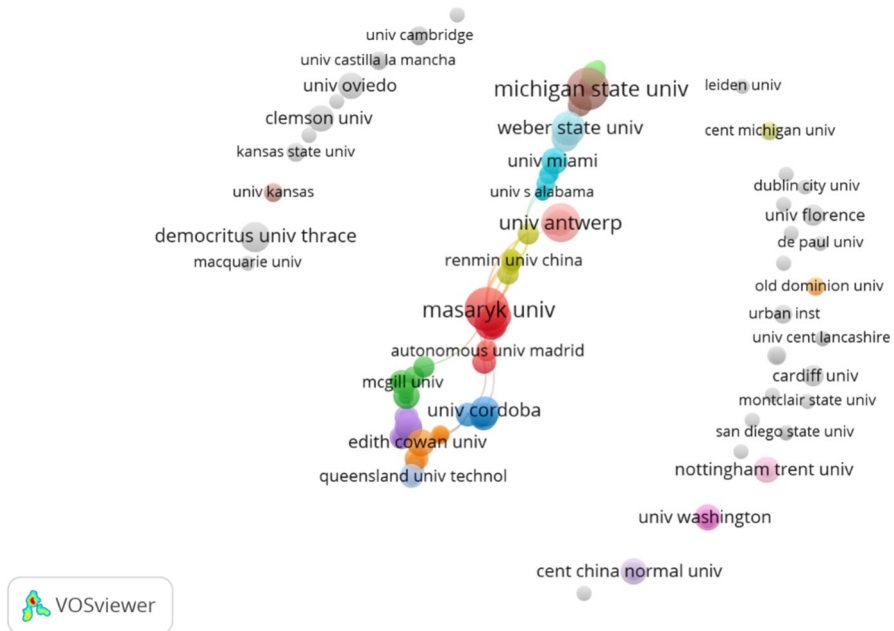
Fig. 6 Collaboration among institutions via network visualization (threshold two articles for an institution, 156 institutions were displayed)

The most significant cluster was red one which is comprised of six researchers: Michelle F. Wright, Sebastian Wachs, Yan Li, Anke Gorzig, Manuel Gamez-Guadix and Esther Calvete. The remarked author for the red cluster was Michelle F. Wright whose value of total link strength is 24. She had the strongest links with Sebastian Wachs; closely link with Yan Li, Anke Gorzig, Manuel Gamez-Guadix and collaborated with authors of yellow cluster, including Shanmukh V. Kamble, Li Lei, Hana Machackova, Shruti Soudi as well as Takuya Yanagida of blue cluster. Michelle F. Wright who obtained the largest number of published articles based on criteria of this study made various connections with other scholars who were from many different institutions in the world. This is also an effective way to achieve more publications.

Takuya Yanagida was the biggest node for the blue cluster including Petra Gradinger, Daniel Graf, Christiane Spiel, Dagmar Strohmeier. Total link strength for Takuya Yanagida was 28; twelve connections. It is observed that Takuya Yanagida's research collaboration is definitely active. Besides, other research groups showed limited collaborations comparing with the red and blue ones.

Collaboration between institutions

The connections among 156 institutions which published at least two documents per one are shown in Fig. 6. Interestingly, there is obvious connections among several distinctive clusters which were coded in color of light steel blue, orange, purple,
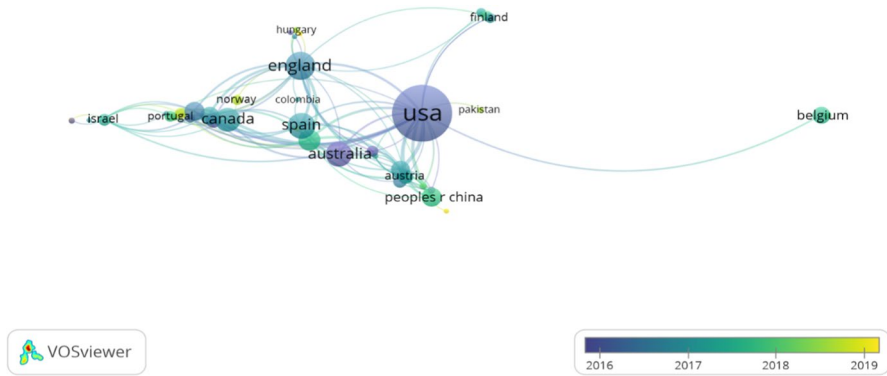
Fig. 7 Collaboration among countries via overlay visualization

steel blue, green, red, yellow, light red, dark turquoise, light blue, brown and light green. These clusters created a big chain of connected institutions and were in the center of the figure, while other smaller clusters or unlinked bubbles (gray color) were distributed in two sides. The biggest chain consisted of most of productive institutions such as Masaryk University, Michigan State University, University of Antwerp, Weber State University, University of Cordoba, Edith Cowan University, University of Cincinnati, University of Victoria, University of Vienna, and University of Seville.

Light steel blue and orange clusters presented connections among organizations from Australia. Light green included institutions from Netherland, while turquoise and light blue consisted of institutions from the USA. Yellow cluster was remarked by the various collaborations among institutions from China and Hong Kong Special Administrative Region (Renmin University of China and South China Normal University, University of Hong Kong, the Hong Kong Polytechnic University and the Chinese University of Hong Kong), the USA (University of Virginia), Cyprus (Eastern Mediterranean University), Japan (Shizuoka University), India (Karnataka University) and Austria (University Applied Sciences Upper Austria). Central China Normal University is another Chinese institution which appeared in Fig. 5, linking with Ministry of Education of the People's Republic of China, Suny Stony Brook and University of Memphis from the USA.

Masaryk University and Michigan State University demonstrated their productivity in both the quantity of publications and the collaboration network. They were active in research collaboration, reaching twelve and eleven links, respectively, with different institutions, but focused much on networking with institutions in the USA and Europe.

Collaboration between countries

The collaboration among 45 countries which published at least one SSCI documents of cybercrime victimization during the given period was examined in VOS Viewer but just 42 items were displayed via overlay visualization. Figure 7 depicts

the international collaborations among significant countries. The USA is the biggest bubble due to its biggest number of documents and shows connections with 26 countries/regions in Euro, Asia, Australia, Middle East. Excepting European countries, England collaborate with the USA, Australia, South Korea, Japan, Thailand, Singapore, Sri Lanka, and Colombia. Spain and Germany almost focus on research network within Euro. China has the strongest tie with the USA, link with Australia, Germany, Czech Republic, Austria, Cyprus and Turkey, Japan, Indian, Vietnam.

Color bar in Fig. 7 is determined by the average publication year of each country and the color of circles based on it. It is unsurprised that the USA, Australia, England, or Spain shows much research experience in this field and maintain the large number of publications steadily. Interestingly, although the average publication year of South Korea or Cyprus was earlier than other countries (purple color), their quantities of documents were moderate. The new nodes (yellow circles) in the map included Vietnam, Norway, Pakistan, Ireland, Scotland, Switzerland.

Keywords and co-occurrence

The present paper examined the related themes and contents in research of cybercrime victimization during 2010–2020 through collecting author keywords, adding several keywords from tiles and abstracts. Besides, this study also conducted co-occurrence analysis of author keywords to show the relationships among these keywords.

The keywords were collected and categorized into 15 themes in Table 6, including cybercrime; sample and demographic factors; location; theory; methodology; technology, platform, and related others; psychology and mental health; physical health; family; school; society; crimes and other deviant behaviors; victim; prevention and intervention; and others.

In the theme of cybercrime, there were numerous types of cybercrimes such as cyberbullying, cyber aggression, cyberstalking, cyber harassment, sextortion and other cyber dating crimes, cyber fraud, identity theft, phishing, hacking, malware, or ransomware. Generally, the frequency of interpersonal cybercrimes or cyber-enable crimes was much higher than cyber-dependent crimes. Cyberbullying was the most common cybercrime in research.

Relating to sample and demographic factors, there were sample of children, adolescent, adults, and the elder who were divided into more detail levels in each research; however, adolescent was the most significant sample. Besides, demographic factor of gender received a remarked concern from scholars.

It is usual that most of the research were carried out in one country, in popular it was the USA, Spain, Germany, England, Australia, Canada or Netherland but sometimes the new ones were published such as Chile, Vietnam, Thailand or Singapore. It was witnessed that some studies showed data collected from a group of countries such as two countries (Canada and the United State), three countries (Israel, Litva, Luxembourg), four countries (the USA, the UK, Germany, and Finland), or six Europe countries (Spain, Germany, Italy, Poland, the United Kingdom and Greece).

Table 6 Statistic of keywords in themes

No.	Themes	Keywords
1	Cybercrime	Cyber-interpersonal violence, cyber/online bullying, workplace cyberbullying, technologically facilitated violence, cyber/online/digital/internet aggression, proactive cyber aggression, reactive cyber aggression, cyber discrimination, cyber-ostracism, cyber hate, cyber trolling, cyberstalking, cyber grooming, cyber/online harassment, cyber/online sexual harassment, cyber dating abuse/violence, non-consensual pornography, image-based sexual abuse, revenge porn, sexting, virtual theft, cyber/online identity theft, online/internet fraud, pet scams, phishing, cyber/digital abuse, computer focused crimes, cyber-dependent crime, ransomware, hacking, malicious software, malware, computer exploits, port scans, and denial of service (dos) attacks
2	Sample and demographic factors	Young children, primary school children, elementary school children, post-primary, children and youth, secondary school students, secondary education, post secondary, school students, university students, college students, undergraduate, latino students, student leaders, higher education, juveniles, adolescent, pre-adolescent, early adolescent, late adolescent, youth, young adults, youth adults, adults, emerging adult, emerging adulthood, elder, gender, age, gender stereotype trait, gender typicality, gender junior-high, demographic differences
3	Location	Australia, Canada, Colombia, India, Northern Ireland, Republic of Ireland, Pakistan, Vietnam, Thailand, Spain, Italia, China, Hong Kong, the USA, Litva, Japan, Belgium, Romania, Turkey, Norway, South Korea, Netherland, Singapore, Portugal, Chile, Cyprus, England, Germany, Sweden, Hungary, Israel, Greece, Austria, Malaysia, Great Britain, United Kingdom, six countries (Germany, India, South Korea, Spain, Thailand and the USA), three countries (Israel, Litva, Luxembourg), four countries (the USA, the UK, Germany and Finland), four countries (Netherland, Germany, Thailand, The USA), two countries (Canada And Tazania), six countries (China, Cyprus, the Czech Republic, India, Japan and The USA), eight countries (Australia, Canada, Germany, Hong Kong, Netherlands, Sweden, The UK, and The USA), six Europe countries (Spain, Germany, Italy, Poland, the UK, and Greece), two countries (Canada and the USA)

Table 6 (continued)

No.	Themes	Keywords
4	Theory	Criminological theory, routine activities theory, lifestyle-routine activities theory, lifestyle exposure theory, cyber-routine activities theory, criminal opportunity theory, general strain theory (strain theory), actor-network theory, theory of reasoned action (TRA), attribution theory, behavior change theories, buffering effect, bystander intervention model, evolutionary theory, health belief model, multi-theoretical, parent-child communication, perception modeling, protection motivation theory, rational choice theory, risk interpretation model, spillover effect, socio-ecological approach, social identity theory, self-determination theory, self-control theory, person-oriented approach, big five, compensatory social interaction model, the general aggression model, a multi-dimensional measurement model, dark triad personality traits, the cyclic process model

Table 6 (continued)

No.	Themes	Keywords
5	Methodology	Qualitative interviews, mix method design, survey method, questionnaire, question order, natural experiment, systematic review, meta-analysis, social network analysis, thematic analysis, factor analysis, contextual analyses, state-level analysis, multi-level analyses, latent class analysis, confirmatory factor analysis, multi-level analysis, latent profile analysis, latent transition analysis, macro-level crime analysis, panel survey/study, cross-lagged panel design, ex post facto study, longitudinal study, longitudinal cohort, longitudinal data, longitudinal patterns, cross-lagged panel model, daily methods, scale development, validity, bayesian profile regression, bootstrap mediation, class-level variables, classification, co-occurrence, construct validity, construct, convergent, correlates, country comparison, cross-national comparison, cross-sectional survey, cross-national data, cross-national research, multi-nation study, factor structure, frequency, functional magnetic resonance imaging, multiple mediators, individual variables, measurement invariance, methodological challenges, methods of counting crime, national crime victimization survey, self-reports, Quebec longitudinal study of child development. dass-21, European cyberbullying intervention project questionnaire (ECIPQ), SDQ (the strengths and difficulties questionnaire), affective styles, attribution style, CDAQ (cyber dating abuse questionnaire), SN-PEQ (the social networking-peer experiences questionnaire), the submissive behavior scale, the cyber bullying scale, the cyber victimization scale, the moral disengagement scale, the cyber-peer experiences questionnaire, school refusal assessment scale revised, the screening of harassment among peers, the moods and feeling questionnaire, the cambridge friendship questionnaire, online aggression scale, the cyberbullying triangulation questionnaire, the Warwick-Edinburgh mental well-being scale, the cyber dating violence inventory, the cyber aggression questionnaire for adolescents, violence tendency scale, revised cyber bullying inventory, the partner cyber abuse questionnaire, the patient health questionnaire-9, e-victimization scale, e-bullying scale

Table 6 (continued)

No.	Themes	Keywords
6	Technology, platforms and related others	Social media, internet, social networking sites, facebook, kakaotalk, instagram, technology, new technologies, adoption of technology, anonymity, smartphone, protocol, botnet, clickbait, computer-mediated communication, digital devices, electronic communication technology, information and communication technologies (icts), technological infrastructure, technology use, problematic internet use, media, media use, internet attachment, internet and abuse, internet communication, online, online intimidation, online lifestyle, online research, online risk behavior, online risks, online routine activity, overt narcissism, online activity, online behavior, online communication, online/electronic/mobile games, online disclosure, online disinhibition, personal information privacy, virtual, texting, text messaging, technical mediation, information/techical/cyber security, screen time, security notices, security seals, technical mediation, internet frequency, self-disclosure, media violence exposure

Table 6 (continued)

No.	Themes	Keywords
7	Psychology and mental health	Self-esteem, self-compassion, self-control, self-concept, self-efficacy, ict self-efficacy, self-harming, anxiety, symptoms of anxiety, depressive symptoms, childhood stress, hopelessness, moral, moral identity, moral disengagement, mental health, loneliness, externalizing problems, internalizing problems, internalizing symptoms, psychometrics, fear of crime, fear of victimization, fear of cybercrime, nomophobia, trust, attribution, hostile attribution bias, autism, personality profile, empathic accuracy, affective empathy, empathy, cognitive empathy, developmental trajectories, impulsivity, intellectual disability, internet addiction, motivation, cyber-relationship motives, narcissism, personality, psychopathic traits, psychopathy, psychosocial adjustment, school psychology, sensation seeking, psychological well-being, subjective well-being, well-being, active–passive patterns, asperger's syndrome, attention deficit hyperactivity disorder (ADHD), attitudes, attitudes toward Facebook, attitudes toward school, cyberbullying attitudes, autism spectrum disorder, avoidance of rest, awareness, overweight preoccupation, body dissatisfaction, body esteem, callous-unemotional traits, chronic pain, cognitive reappraisal, compulsive internet use, control beliefs, coping self-efficacy, covert narcissism, cyber incivility, cyberpsychology, decision-making, digital data security awareness, distress, eating disorders psychopathology, emotion regulation, emotional problems, emotion dysregulation, emotion perception accuracy, emotion perception bias, emotional adjustment, emotional competence, emotional distress, emotional impact, emotional intelligence, socio-emotional factors, social and emotional competencies, epidemiology, expressive suppression, general self-efficacy, harmful intention, intentionality, incivility, life satisfaction, mental health difficulties, metacognitive awareness, mimicry, internet use motives, motivational valence, normative beliefs about aggression, need for stimulation, belief in a just world, normative belief, normative belief about helping, normative beliefs, optimism, social cognition, social competence, perceptions, perceived acceptance, perceived burdensomeness, perceived emotional intelligence, perceived popularity, perceived risk, perceived social support, perceptions of blame, perceptions of peers, anger rumination, anger, state anger, trait anger, perpetration trait anger, persistence, physical and psychological problems, post-traumatic stress symptoms, psychological and behavioral health problems, psychological disease, psychological distress, psychological symptoms, psychopathology symptoms, psychometric properties, romantic jealousy, rumination, vulnerabilities, violence tendency, externalizing behaviors, antisocial behavior, antisocial behavior, behavior activation, behavior problems, behavior measures, bystanders behavior, cyberbullying behavior, high-risk internet behaviors, school refusal behavior, submissive behavior, helping behavior, controlling behavior, cyber behavior, promiscuity

Table 6 (continued)

No.	Themes	Keywords
8	Physical health	Sex, sex difference, sexual double standard, sexual orientation, sexual pressure, suicide ideation, suicide attempt, suicidality, adolescent health, physical disabilities, physical health, diet, disability, health risks, paedosexual, adolescent development
9	Family	Parental mediation, parents, family climate, household activity, in-law conflict, parent-adolescent communication, parent-adolescent information sharing, parent–child communication, parental awareness, parental control, parental mediation of media, parental monitoring, parental monitoring of cyber behavior, parental style
10	School	school bonding, school context, school record, value of learning, university, teacher bonding, teacher justice, teachers, peer education, peer influence, peer rejection, peer relations, peer nominations, peers, prosocial peer affiliation, friendship networks, classmate justice, friendship quality, high school, middle school, peer nomination, peer attachment, peers/peer relations, school climate, academic performance, academic problems, school adjustment, schools
11	Society	Social standing, social relationships, norms, social norms, injunctive norms, subjective norm, descriptive norms, moral norms, interpersonal relationships, collectivism, individualism, contextual factors, controllers, cross-cultural, social information processing, social exclusion, social engagement, social desirability, social coping, social bonds, social belongingness, socialization, machiavellianism, femininity, masculinity, fun-seeking tendencies, help-seeking, helpfulness, cryptomarkets, cultural values, ethno-cultural groups, social learning, social skills, culture, bystander, cyber bystander, social support
12	Crimes and deviant behaviors	Violence, offline violence, gendered violence, dating violence, sexual violence, teen dating violence, intimate partner violence, domestic violence, youth violence, bullying, school bullying, offline bullying, covert bullying, workplace bullying, face-to-face bullying, non-physical bullying, traditional face-to-face bullying, traditional bullying perpetration, sibling bullying, perpetrators of bullying, substance use, adolescent substance use, smoking, alcohol use, fraud, scam, white-collar crime, property crime, abuse, addiction, verbal aggression, aggressive behavior, aggressor, physical aggression, face-to-face aggression, anti-muslim hate crime, hate speech, disability hate crime, crime, crime drop, delinquency, elder abuse, juvenile delinquency, perpetration, offender, online deviance, troubled offline behavior, sexual solicitation, partner abuse, sexual harassment, sexual orientation-based harassment, peer harassment, race-based harassment

Table 6 (continued)

No.	Themes	Keywords
13	Victim	Victim blaming, recurring victimization, relational victimization, victims of bullying, bullying victimization, traditional bully victimization, face-to-face victimization, family victimization, traditional victimization, school victimization, peer victimization, threat victimization, cybercrime victimization, cyberstalking victimization, cyber-theft victimization, cyber victims, aggressive victim
14	Prevention and intervention	Uniform crime reporting program, solutions, social problem-solving, safety, intervention, intervention strategies, intervention success, prevention, coping strategies, predictors, protective factors, police, policing, anti-bullying program, Canadian 24-h movement guidelines, capable guardianship, control, control balance, coping efficacy, national incident-based reporting system, crime reporting, reporting, cyber witnessing, cyberbullying intervention, bullying prevention, cyberbullying reduction, eurobarometer, evidence-based intervention, safety, prediction, preventive behavior, super controllers, counseling, guardianship, whole-school program trial, psychological service providers, risk and protective factors, intrusion prevention system, risk management, risk factors, mediation, restrictive mediation, instructive mediation, moderation,
15	Others	Routine activities, validation, opportunity, popularity, prevalence, agency, associations, assessment, attachment, causes, certs, victim-offender overlap, coronavirus, covid-19, definition, definitional issues, judgments, multiple risk exposure, multiple informants, outcome expectancies, participant roles, physical activity, publicity, reliability, resistance, response decision, response evaluation, role continuity, sustainability, sleep, similarities, severity

These keywords were most of author keyword, adding a few selected keywords from the titles and abstracts by the author of this current study
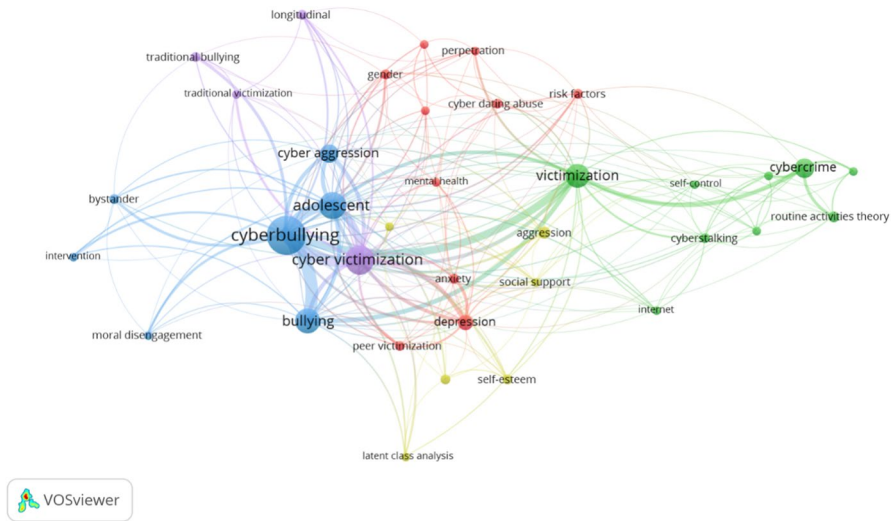
Fig. 8 Co-occurrence between author keywords via network visualization (the minimum number of occurrences per word is seven, 36 keywords were displayed)

A wide range of theories were applied in this research focusing on criminological and psychological theories such as Routine Activities Theory, Lifestyle—Routine Activities Theory, General Strain Theory, the Theory of Reasoned Action or Self-control Theory.

Table 6 indicated a lot of different research methods covering various perspective of cybercrime victimization: systematic review, questionnaire survey, interview, experiment, mix method, longitudinal study, or cross-national research; many kinds of analysis such as meta-analysis, social network analysis, latent class analysis, confirmatory factor analysis; and a wide range of measurement scales which were appropriate for each variable.

Topic of cybercrime victimization had connections with some main aspects of technology (information and communication technologies, internet, social media or technology related activities), psychology (self-esteem, fear, attitude, personality, psychological problems, empathy, perceptions or emotion), physical health, family (parents), school (peers, school climate), society (norms, culture, social bonds), victim, other crimes (violence, substance use), prevention and intervention.

Co-occurrence analysis was performed with keywords suggested by authors and the minimum number of occurrences per word is seven. The result showed 36 frequent keywords which clustered into five clusters as illustrated in Fig. 8.

Figure 8 illustrates some main issues which were concerned in subject of cybercrime victimization, as well as the relationship among them. Fifteen most frequent keywords were presented by big bubbles, including: 'cyberbullying' (174 times), 'cyber victimization' (90 times), 'adolescent' (79 times), 'bullying' (66 times), 'victimization' (56 times), 'cybercrime' (40 times), 'cyber aggression' (37 times), 'depression' (23 times), 'aggression' (14 times), 'routine activities theory' (13

times), 'cyberstalking' (11 times), 'gender' (11 times), 'longitudinal' (10 times), 'peer victimization' (10 times) and 'self-esteem' (10 times).

'Cyberbullying' linked with many other keywords, demonstrating the various perspectives in research of this topic. The thick lines which linked 'cyberbullying' and 'bullying', 'adolescent', 'cyber victimization', 'victimization' showed the strong connections between them; there were close relationship between 'cyber aggression', 'bystander'', 'self-esteem' or 'moral disengagement' and 'cyberbullying'.

'Cybercrime' had strong links with 'victimization', 'routine activities theory'. In Fig. 8, the types of cybercrime which occurred at least seven times were: cyberbullying, cyber aggression, hacking, cyberstalking, and cyber dating abuse.

Discussion

The increasing trend over the years reveals the increasing concern of scholarly community on this field, especially in the boom of information technology and other communication devices and the upward trend in research of cyberspace-related issues (Altarturi et al. 2020; Leung et al. 2017; Serafin et al. 2019). It predicts the growth of cybercrime victimization research in future.

Psychology was the more popular research areas in database, defeating criminology penology. As part of the 'human factors of cybercrime', human decision-making based on their psychological perspectives plays as a hot topic in cyber criminology (Leukfeldt and Holt 2020). Then, it is observed that journals in psychology field was more prevalent in top of productive sources. Besides, journal *Computers in Human Behavior* ranked first in total publications, but *Journal of Youth and Adolescence* ranked higher place in the average citations per document. Generally, top ten journals having highest number of publications on cybercrime victimization are highly qualified ones and at least 10 years in publishing industry.

The USA demonstrated its leading position in the studied domain in terms of total publications as well as the various collaborations with other countries. The publications of the USA occupied much higher than the second and third countries: England and Spain. It is not difficult to explain for this fact due to the impressive productivity of institutions and authors from the USA. A third of top twelve productive institutions were from the USA. Three leading positions of top ten productive authors based on document count were from institutions of the USA, number one was Michelle F. Wright; others were Thomas J. Holt and Bradford W. Reyns.

Furthermore, these authors also participated in significant research groups and become the important nodes in those clusters. The most noticeable authors in co-authors network were Michelle F. Wright. The US institutions also had strong links in research network. The USA was likely to be open in collaboration with numerous countries from different continents in the world. It was assessed to be a crucial partner for others in the international co-publication network (Glänzel and Schubert 2006).

As opposed to the USA, most of European countries prefer developing research network within Europe and had a limited collaboration with other areas. Australia, the USA, or Japan was in a small group of countries which had connections with

European ones. Nevertheless, European countries still showed great contributions for research of cybercrime victimization and remained stable links in international collaboration. The prominent authors from Euro are Rosario Ortega-Ruiz, Constantinos M. Kokkinos or Rutger Leukfeldt.

It is obvious that the limited number of publications from Asia, Middle East, Africa, or other areas resulted in the uncomprehensive picture of studied subject. For example, in the Southeast Asia, Malaysia and Vietnam lacked the leading authors with their empirical studies to review and examine the nature of cybercrimes, though they are facing to practical challenges and potential threats in the cyberspace (Lusthaus 2020a, b). The present study indicated that Vietnam, Ireland, or Norway was the new nodes and links in research network.

Several nations which had a small number of publications such as Vietnam, Thailand, Sri Lanka, or Chile started their journey of international publications. It is undeniable that globalization and the context of global village (McLuhan 1992) requires more understanding about the whole nations and areas. Conversely, each country or area also desires to engage in international publications. Therefore, new nodes and clusters are expected to increase and expand.

The findings indicated that cyberbullying was the most popular topic on research of cybercrime victimization over the given period. Over a half of most-cited publications was focus on cyberbullying. Additionally, 'cyberbullying' was the most frequent author keyword which co-occurred widely with distinctive keywords such as 'victimization', 'adolescents', 'bullying', 'social media', 'internet', 'peer victimization' or 'anxiety'.

By reviewing keywords, several research gaps were indicated. Research samples were lack of population of the children and elders, while adolescent and youth were frequent samples of numerous studies. Although young people are most active in cyberspace, it is still necessary to understand other populations. Meanwhile, the elderly was assumed to use information and communication technologies to improve their quality of life (Tsai et al. 2015), their vulnerability to the risk of cybercrime victimization did not reduce. Those older women were most vulnerable to phishing attacks (Lin et al. 2019; Oliveira et al. 2017). Similarly, the population of children with distinctive attributes has become a suitable target for cybercriminals, particularly given the context of increasing online learning due to Covid-19 pandemic impacts. These practical gaps should be prioritized to focus on research for looking the suitable solutions in the future. Besides, a vast majority of research were conducted in the scope of one country; some studies collected cross-national data, but the number of these studies were moderate and focused much on developed countries. There are rooms for studies to cover several countries in Southeast Asia or South Africa.

Furthermore, although victims may be both individuals and organizations, most of research concentrated much more on individuals rather than organizations or companies. Wagen and Pieters (2020) indicated that victims include both human and non-human. They conducted research covering cases of ransomware victimization, Bonet victimization and high-tech virtual theft victimization and applying Actor-Network Theory to provide new aspect which did not aim to individual victims. The number of this kind of research, however, was very limited. Additionally, excepting

cyberbullying and cyber aggression were occupied the outstanding quantity of research, other types of cybercrime, especially, e-whoring, or social media-related cybercrime should still be studied more in the future.

Another interesting topic is the impact of family on cybercrime victimization. By reviewing keyword, it is clear that the previous studies aimed to sample of adolescent, hence, there are many keywords linking with parents such as 'parent-adolescent communication', 'parent-adolescent information sharing', 'parental mediation', 'parental monitoring of cyber behavior', 'parental style'. As mentioned above, it is necessary to research more on sample of the elder, then, it is also essential to find out how family members affect the elder's cybercrime victimization.

Conclusion

It is a big challenge to deal with problems of cybercrime victimization because cybercrime forms become different daily (Näsi et al. 2015). Numerous researchers engage in understanding this phenomenon from various angles. The current bibliometric study assessed the scholarly status on cybercrime victimization during 2010–2020 by retrieving SSCI articles from WoS database. There is no study that applied bibliometric method to research on the examined subject. Hence, this paper firstly contributed statistical evidence and visualized findings to literature of cybercrime victimization.

Statistical description was applied to measure the productive authors, institutions, countries/regions, sources, and most-cited documents, mainly based on publication and citation count. The international collaborations among authors, institutions, and countries were assessed by co-authors, while the network of author keywords was created by co-occurrence analysis. The overall scholarly status of cybercrime victimization research was drawn clearly and objectively. The research trend, popular issues and current gaps were reviewed, providing numerous suggestions for policymakers, scholars, and practitioners about cyber-related victimization (Pickering and Byrne 2014). Accordingly, the paper indicated the most prevalent authors, most-cited papers but also made summary of contributions of previous research as well as identified research gaps. First, this article supports for PhD candidates or early-career researchers concerning about cybercrime victimization. Identifying the leading authors, remarked journals, or influencing articles, gaps related to a specific research topic is important and useful task for new researchers to start their academic journey. Although this information is relatively simple, it takes time and is not easy for newcomers to find out, especially for ones in poor or developing areas which have limited conditions and opportunities to access international academic sources. Thus, the findings in the current paper provided for them basic but necessary answers to conduct the first step in research. Secondly, by indicating research gaps in relevance to sample, narrow topics or scope of country, the paper suggests future study fulfilling them to complete the field of cybercrime victimization, especial calling for publications from countries which has had a modest position in global research map. Science requires the balance and diversity, not just focusing on a few developed countries or areas. Finally, the present study assists researchers and

institutions to determined strategy and potential partners for their development of research collaborations. It not only improve productivity of publication but also create an open and dynamic environment for the development of academic field.

Despite mentioned contributions, this study still has unavoidable limitations. The present paper just focused on SSCI articles from WoS database during 2010–2020. It did not cover other sources of databases that are known such as Scopus, ScienceDirect, or Springer; other types of documents; the whole time; or articles in other languages excepting English. Hence it may not cover all data of examined subject in fact. Moreover, this bibliometric study just performed co-authorship and co-occurrence analysis. The rest of analysis such as citation, co-citation and bibliographic coupling have not been conducted. Research in the future is recommended to perform these kinds of assessment to fill this gap. To visualize the collaboration among authors, institutions, countries, or network of keywords, this study used VOS Viewer software and saved the screenshots as illustrations. Therefore, not all items were displayed in the screenshot figures.

Declarations

References

Abdullah ATM, Jahan I (2020) Causes of cybercrime victimization: a systematic literature review. Int J Res Rev 7(5):89–98

Al-Nemrat A, Benzaïd C (2015) Cybercrime profiling: Decision-tree induction, examining perceptions of internet risk and cybercrime victimisation. In: Proceedings—14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015, vol 1, pp 1380–1385. https://doi.org/10.1109/Trustcom.2015.534

Alalehto TI, Persson O (2013) The Sutherland tradition in criminology: a bibliometric story. Crim Justice Stud 26(1):1–18

Algarni A, Xu Y, Chan T (2017) An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. Eur J Inf Syst 26(6):661–687

Altarturi HHM, Saadoon M, Anuar NB (2020) Cyber parental control: a bibliometric study. Child Youth Serv Rev. https://doi.org/10.1016/j.childyouth.2020.105134

Ariola B, Laure ERF, Perol ML, Talines PJ (2018) Cybercrime awareness and perception among Students of Saint Michael College of Caraga. SMCC Higher Educ Res J 1(1):1. https://doi.org/10.18868/cje.01.060119.03

Benson V, Saridakis G, Tennakoon H (2015) Purpose of social networking use and victimisation: are there any differences between university students and those not in HE? Comput Hum Behav 51:867–872

Brenner SW (2001) Is there such a thing as "rough"? Calif Crim Law Rev 4(1):348–349. https://doi.org/10.3109/09637487909143344

Chen X, Wang S, Tang Y, Hao T (2019) A bibliometric analysis of event detection in social media. Online Inf Rev 43(1):29–52. https://doi.org/10.1108/OIR-03-2018-0068

Choi K (2008) Computer Crime Victimization and Integrated Theory: an empirical assessment. Int J Cyber Criminol 2(1):308–333

Cojocaru I, Cojocaru I (2019) A bibliomentric analysis of cybersecurity research papers in Eastern Europe: case study from the Republic of Moldova. In: Central and Eastern European E|Dem and E|Gov Days, pp 151–161

Das B, Sahoo JS (2011) Social networking sites—a critical analysis of its impact on personal and social life. Int J Bus Soc Sci 2(14):222–228

Drew JM (2020) A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. J Criminol Res Policy Pract 6(1):17–33. https://doi.org/10.1108/JCRPP-12-2019-0070

E Fonseca B, Sampaio, de Araújo Fonseca MV, Zicker F (2016). Co-authorship network analysis in health research: method and potential use. Health Res Policy Syst 14(1):1–10. https://doi.org/10.1186/s12961-016-0104-5

Feeley TH (2008) A bibliometric analysis of communication journals from 2002 to 2005. Hum Commun Res 34:505–520

Gan C, Wang W (2014) A bibliometric analysis of social media research from the perspective of library and information science. IFIP Adv Inf Commun Technol 445:23–32. https://doi.org/10.1007/978-3-662-45526-5_3

Glänzel W, Schubert A (2006) Analysing scientific networks through co-authorship. Handb Quant Sci Technol Res. https://doi.org/10.1007/1-4020-2755-9_12

Gogolin G (2010) The digital crime tsunami. Digit Investig 7(1–2):3–8. https://doi.org/10.1016/j.diin.2010.07.001

Holt TJ, Bossler AM (2009) Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behav 30(1):1–25. https://doi.org/10.1080/01639620701876577

Holt TJ, Bossler AM (2014) An assessment of the current state of cybercrime scholarship. Deviant Behav 35(1):20–40. https://doi.org/10.1080/01639625.2013.822209

Ilievski A (2016) An explanation of the cybercrime victimisation: self-control and lifestile/routine activity theory. Innov Issues Approaches Soc Sci 9(1):30–47. https://doi.org/10.12959/issn.1855-0541.iiass-2016-no1-art02

Insa F (2007) The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against high-tech crime—results of a European study. J Digital Forensic Pract 1(4):285–289. https://doi.org/10.1080/15567280701418049

Jahankhani H (2013) Developing a model to reduce and/or prevent cybercrime victimization among the user individuals. Strategic Intell Manag. https://doi.org/10.1016/b978-0-12-407191-9.00021-1

Jamshed J, Naeem S, Ahmad K (2020) Analysis of Criminal Law Literature: a bibliometric study from 2010–2019. Library Philos Pract

Kim J, Kang S, Lee KH (2019) Evolution of digital marketing communication: Bibliometric analysis and networs visualization from key articles. J Bus Res

Kirwan GH, Fullwood C, Rooney B (2018) Risk factors for social networking site scam victimization among Malaysian students. Cyberpsychol Behav Soc Netw 21(2):123–128. https://doi.org/10.1089/cyber.2016.0714

Lee S-S, Choi KS, Choi S, Englander E (2019) A test of structural model for fear of crime in social networking sites A test of structural model for fear of crime in social networking sites. Int J Cybersecur Intell Cybercrime 2(2):5–22

Leukfeldt R, Holt T (eds) (2020) The human factor of cybercrime. Routledge, New York

Leukfeldt ER, Yar M (2016) Applying routine activity theory to cybercrime: a theoretical and empirical analysis. Deviant Behav 37(3):263–280. https://doi.org/10.1080/01639625.2015.1012409

Leung XY, Sun J, Bai B (2017) Bibliometrics of social media research: a co-citation and co-word analysis. Int J Hosp Manag 66:35–45. https://doi.org/10.1016/j.ijhm.2017.06.012

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. https://doi.org/10.3390/su9030384

Lin T, Capecci DE, Ellis DM, Rocha HA, Dommaraju S, Oliveira DS, Ebner NC (2019) Susceptibility to spear-phishing emails: effects of internet user demographics and email content. ACM Trans Comput-Hum Interact 26(5):1–28. https://doi.org/10.1145/3336141

Luong TH (2021) Prevent and combat sexual assault and exploitation of children on cyberspace in Vietnam: situations, challenges, and responses. In: Elshenraki H (ed) Combating the exploitation of children in cyberspace: emerging research and opportunities. IGI Global, Hershey, pp 68–94

Luong HT, Phan HD, Van Chu D, Nguyen VQ, Le KT, Hoang LT (2019) Understanding cybercrimes in Vietnam: from leading-point provisions to legislative system and law enforcement. Int J Cyber Criminol 13(2):290–308. https://doi.org/10.5281/zenodo.3700724

Lusthaus J (2020a) Cybercrime in Southeast Asia: Combating a Global Threat Locally. Retrieved from Canberra, Australia: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/202005/Cybercrime%20in% 20Southeast%20Asia.pdf?naTsKQp2jtSPYsWpSo4YmE1sVBNv_exJ

Lusthaus J (2020b) Modelling cybercrime development: the case of Vietnam. In: Leukfeldt R, Holt T (eds) The human factor of cybercrime. Routledge, New York, pp 240–257

Marsh I, Melville G (2008) Crime justice and the media. Crime Justice Med. https://doi.org/10.4324/9780203894781

Martí-Parreño J, Méndez-Ibáñezt E, Alonso-Arroyo A (2016) The use of gamification in education: a bibliometric and text mining analysis. J Comput Assist Learn

McLuhan M (1992) The Global Village: Transformations in World Life and Media in the 21st Century (Communication and Society). Oxford University Press, Oxford

Näsi M, Oksanen A, Keipi T, Räsänen P (2015) Cybercrime victimization among young people: a multi-nation study. J Scand Stud Criminol Crime Prev. https://doi.org/10.1080/14043858.2015.1046640

Ngo F, 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. Int J Cyber Criminol 11(1):1–9

Ngo F, Paternoster R (2011) Cybercrime victimization: an examination of individual and situational level factors. Int J Cyber Criminol 5(1):773

Nguyen VT, Luong TH (2020) The structure of cybercrime networks: transnational computer fraud in Vietnam. J Crime Justice. https://doi.org/10.1080/0735648X.2020.1818605

Oksanen A, Keipi T (2013) Young people as victims of crime on the internet: a population-based study in Finland. Vulnerable Child Youth Stud 8(4):298–309

Oliveira D, Rocha H, Yang H, Ellis D, Dommaraju S, Muradoglu M, Weir D, Soliman A, Lin T, Ebner N (2017) Dissecting spear phishing emails for older vs young adults: on the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In: Conference on Human Factors in Computing Systems—Proceedings, 2017-May, 6412–6424. https://doi.org/10.1145/3025453.3025831

Orchard LJ, Fullwood C, Galbraith N, Morris N (2014) Individual differences as predictors of social networking. J Comput-Mediat Commun 19(3):388–402. https://doi.org/10.1111/jcc4.12068

Parrish JL Jr, Bailey JL, Courtney JF (2009) A personality based model for determining susceptibility to phishing attacks. University of Arkansas, Little Rock, pp 285–296

Pasadeos Y (1985) A bibliometric study of advertising citations. J Advert 14(4):52–59

Pickering C, Byrne J (2014) The benefits of publishing systematic quantitative literature reviews for PhD candidates and other early-career researchers. Higher Educ Res Devel ISSN 33(3):534–548

Reyns BW, Fisher BS, Bossler AM, Holt TJ (2019) Opportunity and Self-control: do they predict multiple forms of online victimization? Am J Crim Justice 44(1):63–82. https://doi.org/10.1007/s12103-018-9447-5

Romero L, Portillo-Salido E (2019) Trends in sigma-1 receptor research: a 25-year bibliometric analysis. Front Pharmacol. https://doi.org/10.3389/fphar.2019.00564

Saad ME, Huda Sheikh Abdullah SN, Murah MZ (2018) Cyber romance scam victimization analysis using Routine Activity Theory versus apriori algorithm. Int J Adv Comput Sci Appl 9(12):479–485. https://doi.org/10.14569/IJACSA.2018.091267

Saridakis G, Benson V, Ezingeard JN, Tennakoon H (2016) Individual information security, user behaviour and cyber victimisation: an empirical study of social networking users. Technol Forecast Soc Change 102:320–330. https://doi.org/10.1016/j.techfore.2015.08.012

Seng S, Wright M, Al-Ameen MN (2018) Understanding users' decision of clicking on posts in facebook with implications for phishing. Workshop on Technology and Consumer Protection (ConPro 18), May, 1–6

Serafin MJ, Garcia-Vargas GR, García-Chivita MDP, Caicedo MI, Correra JC (2019) Cyberbehavior: a bibliometric analysis. Annu Rev Cyber Ther Telemed 17:17–24. https://doi.org/10.31234/osf.io/prfcw

Skinner WF, Fream AM (1997) A social learning theory analysis of computer crime among college students. J Res Crime Delinq 34(4):495–518. https://doi.org/10.1177/0022427897034004005

Tsai H, Yi S, Shillair R, Cotten SR, Winstead V, Yost E (2015) Getting grandma online: are tablets the answer for increasing digital inclusion for older adults in the US? Educ Gerontol 41(10):695–709. https://doi.org/10.1080/03601277.2015.1048165

van Eck NJ, Waltman L (2020) Manual for VOSviewer version 1.6.16

Van Wilsem J (2013) "Bought it, but never got it" assessing risk factors for online consumer fraud victimization. Eur Sociol Rev 29(2):168–178. https://doi.org/10.1093/esr/jcr053

van der Wagen W, Pieters W (2020) The hybrid victim: re-conceptualizing high-tech cyber victimization through actor-network theory. Eur J Criminol 17(4):480–497. https://doi.org/10.1177/1477370818 812016

Vishwanath A (2015) Habitual Facebook use and its impact on getting deceived on social media. J Comput-Mediat Commun 20(1):83–98. https://doi.org/10.1111/jcc4.12100

Wall D (2001) Crime and the Internet: Cybercrime and cyberfears, 1st edn. Routledge, London

Wall D (2004) What are cybercrimes? Crim Justice Matters 58(1):20–21

Whitty MT, Buchanan T (2012) The online romance scam: a serious cybercrime. Cyberpsychol Behav Soc Netw 15(3):181–183. https://doi.org/10.1089/cyber.2011.0352

You GR, Sun X, Sun M, Wang JM, Chen YW (2014) Bibliometric and social network analysis of the SoS field. In: Proceedings of the 9th International Conference on System of Systems Engineering: The Socio-Technical Perspective, SoSE 2014, 13–18. https://doi.org/10.1109/SYSOSE.2014.6892456

Zyoud SH, Sweileh WM, Awang R, Al-Jabi SW (2018) Global trends in research related to social media in psychology: Mapping and bibliometric analysis. Int J Ment Health Syst 12(1):1–8. https://doi.org/10.1186/s13033-018-0182-6