social sciences

MDPI

Article

Bibliometric Mapping of Scientific Production and Conceptual Structure of Cyber Sextortion in Cybersecurity

Fani Moses Radebe * and Kennedy Njenga

Department of Applied Information Systems, University of Johannesburg, Johannesburg P.O. Box 524, South Africa; knjenga@uj.ac.za
* Correspondence: fmradebe@uj.ac.za

Abstract: This study examines cyber sextortion research using a comprehensive bibliometric analysis. In the field of cybersecurity, cyber sextortion is a form of cybercrime that leverages privacy violations to exploit a victim. This study reviewed research developments on cyber sextortion progressively over time by looking at scientific productions, thematic developments, scholars' contributions, and the future thematic trajectory. A bibliometric approach to analyzing the data was applied, which covered 548 peer-reviewed articles, conference papers, and book chapters retrieved from the Scopus database. Results showed a growth trajectory on various thematic concerns in the cyber sextortion field, which has continued to gain traction since the year 2023. Notably, online child sexual abuse is a growing theme in cyber sextortion research. In addition, among other themes, adolescents, mental health, and dating violence are receiving interest among scholars in this field. Additionally, institutions and prolific scholars from countries such as the United States of America, Australia, and the United Kingdom have established research collaborations to improve understanding in this field. The results also showed that research is observed to be emerging from South Africa and Ghana in the African region. Overall, there is potential for more scientific publications and researchers from Africa to contribute to this growing field. The value this study holds is moving beyond deficit-based approaches to how adolescent youth can be resilient and protected from cyber sextortion. A call for a multidisciplinary approach that moves beyond deficit-based approaches toward resilient and autonomy-based approaches is encouraged so that adolescent youth are protected from exploitation. This approach should focus on investigating proactive and resilience-based interventions informed by individuals' traits and contexts to aid in building digital resilience in adolescents.

Keywords: cyber sextortion; coercive sexting; romance scam; bibliometric analysis; bibliometrix R package; science mapping; research trends; biblioshiny

Academic Editors: Pamela Wisniewski and Jinkyung Katie Park

Received: 14 October 2024
Revised: 21 December 2024
Accepted: 24 December 2024
Published: 31 December 2024

Citation: Radebe, Fani Moses, and Kennedy Njenga. 2025. Bibliometric Mapping of Scientific Production and Conceptual Structure of Cyber Sextortion in Cybersecurity. *Social Sciences* 14: 12. https://doi.org/10.3390/socsci14010012

1. Introduction

The advancement of communication technologies has, on the one hand, greatly enhanced online social interaction, but on the other hand, increased unanticipated and unexpected challenges. One notable challenge is that people, especially minors, are exploited because of how easily technology has become accessible and easy to use (Humphreys et al. 2019; Zeyzus Johns et al. 2024). Criminals and technology users with nefarious intent can now exploit technology and engage in activities such as cyber sextortion to threaten and scam other people.

Sextortion is described as a threat targeting a victim by the perpetrator to disseminate sexually explicit images or videos of the victim, and, in so doing, forces the victim to

comply with the perpetrators' demands (O'Malley and Holt 2022; Patchin and Hinduja 2020). The name for this form of attack is derived from a portmanteau of two words, "sex" and "extortion." Sextortion is seen as a form of perpetration of sexual coercion, in which sexual cooperation is obtained by pressuring the victim through threats. The online occurrence of this attack is termed cyber sextortion (Carlton 2019). Cyber sextortion can be facilitated through fake profiles on social media sites such as Facebook and dating apps (Carlton 2019; Mondal et al. 2022). Fake social media profiles are known as catfishing (Kibe et al. 2022). Catfishing fools victims into thinking that they are interacting with peers (Humphreys et al. 2019).

In the field of cybersecurity, cyber sextortion is a form of cybercrime that leverages privacy violations to exploit a victim by breaching private data and violating personal autonomy, since victims lose security and control over personal information (Wittes et al. 2016). Cyber sextortion continues to grow and has become a lucrative business for scammers and criminals (Carlton 2019; Humphreys et al. 2019). This is because, through cyber sextortion, it is possible to manipulate compromised individuals who may be in possession of sexually explicit images or videos, for example, pornography (Humphreys et al. 2019).

Advancements in communication technologies are now one of the primary reasons why there has been an increase in cyber sextortion among adults and adolescents (Mondal et al. 2022). Technology makes victims highly susceptible to cyber sextortion (O'Malley and Holt 2022). What is missing in the literature are studies that point to the extent to which youth, specifically adolescent youths in Africa, are or are becoming susceptible to sextortion. This may only be understood if prior research on sextortion conducted by other countries is examined and contextualized.

As pointed out by studies, cyber sextortion is now a global phenomenon (O'Malley and Holt 2022; Patchin and Hinduja 2020). Cyber sextortion may not have been given the societal attention this phenomenon warrants (Pethers and Bello 2023).

Studies show that cyber sextortion may exacerbate or become an antecedent to existing societal ills, such as rape (Mondal et al. 2022). As an example, studies point out that South Africa, where this study is domiciled, has a high victimization rate of rape at 70.5 out of 100,000 people in 2017–2018, compared to the United States of America with an estimated rate of 41.7 out of 100,000 individuals in 2017 (Fakunmoju et al. 2021). Therefore, there is a need to learn, from other studies carried out outside of South Africa, as well as from the advent of South African rape statistics, how susceptible South African adolescent youth are to sextortion (Pethers and Bello 2023; Wolak et al. 2018).

Humphreys et al. (2019) have pointed to the link between cyber sextortion and webcam pornography, arguing that coercion or duress in these online activities remains largely unregulated. Additionally, cyber sextortion may emerge because of romance fraud, where perpetrators create online relationships with the intent of exploiting victims for financial gain (Cross et al. 2023). However, despite the growing awareness of romance fraud, there is still limited research on how this form of fraud intersects with and leads to sextortion (Cross et al. 2023). This gap in understanding necessitates more comprehensive studies in this area.

2. Background

The literature suggests that adolescents engage in sexting both inside and outside of romantic relationships and online romance (dating), which is related to cyber sextortion (Ray and Henry 2024; Tasbiha 2024). Therefore, coercive sexting, online romance scams, and their multifaceted manifestations (characteristic of cyber sextortion) are also presented by literature, in relation to cyber sextortion (Almeida and Barreiros 2024).

2.1. Sextortion

Sextortion is seen as the use of threats to reveal intimate images to force victims into giving more photos, having sex, or performing other favors (Wolak et al. 2018). In addition, sextortion is described as a threat to expose sexually explicit or suggestive images without consent, typically in order to obtain more images, sexual acts, money, or other items (Patchin and Hinduja 2020, p. 31).

The term "sextortion" has different meanings in different contexts. Usually, sextortion involves the use of power, such as in workplaces or public sectors, against women. A study in South Africa investigated sextortion in public sector workplaces, where corrupt officials solicited sexual favors from vulnerable junior employees and public sector clients (Hlongwane 2017). Another study explored a gendered form of corruption through sexual favors, referred to as a "sextortion" phenomenon, that is perpetrated against female African migrants to South Africa (Caarten et al. 2022).

Additionally, sextortion cases can be categorized into two groups: (1) attempts to force reconciliation or humiliate a partner in a sexual relationship, and (2) occurring as the result of a perpetrator meeting the victim online (Pethers and Bello 2023). Sextortion includes threats to distribute victims' sexual content online to victims' acquaintances or families, adding the victim's identity in the distributed images, creating trouble for victims at school or with the law, stalking or physically harming victims or their next of kin, and more (Pethers and Bello 2023). Clearly, sextortion involves both physical and online forms of attacks, and therefore its research growth needs to be reviewed to enable clear definitions according to its occurrence facets.

2.2. Cyber Sextortion

The literature lacks coherence with the definition of cyber sextortion (Hagglund and Khan 2023). The term has been interpreted differently by different observers due to its multifaceted manifestations. However, there are two popular definitions of cyber sextortion: (1) an attempt to extort something from victims by threatening to distribute their personal sexual images; and (2) an act of coercing a victim into providing sexual material to the perpetrator through threats to either share intimate images or other forms of harm (Carlton 2019). In addition, manifestations of sextortion can be categorized into: (1) perpetrators that attack victims that they met through online platforms such as dating websites or social networking sites, in which victims believe they are in genuine romantic or trusting relationships; and (2) elaborate online scams, in which perpetrators hack into hundreds of victims' computers, or use fake profiles to obtain sexual material from victims before threatening them (Cross et al. 2023; Wolak et al. 2018).

Cyber sextortion in cybersecurity studies, is quid pro quo social engineering that is under-researched (Hagglund and Khan 2023). Cyber sextortion scams can be defined as forcing victims, using online communication media such as emails and social media, to meet the demands of a perpetrator, who threatens to distribute victims' sexual material (Pethers and Bello 2023). Meeting the demands usually includes the victims paying money to the perpetrators. If victims cannot pay money, they are forced to perform sexual acts in front of a webcam while being recorded, which the perpetrator uses for further coercion (Wang 2024). Pethers and Bello (2023) note that because sextortion is a scam, threats are often not carried out regardless of whether the coercion was successful or not. However, Carlton (2019) discourages victims' compliance because extorters could still publish content despite their promises to delete content once the ransom is received. Similarly, Hong et al. (2020) note that despite payments, victims are still subsequently blackmailed by having their sexual content publicly released. In addition, cyber sextortion scammers deceive their victims into believing that they already possess their sexual images (Pethers and

Bello 2023), which makes it increasingly difficult for any person to avoid falling victim to cyber sextortion. Additionally, perpetrators may not stop their victimization even after their demands are met; therefore, immediately reporting the incident to law enforcement is important (Mondal et al. 2022).

Sextortion victims fear reputational harm and embarrassment, and therefore comply with the perpetrator's demands and remain silent, which essentially empowers the perpetrator (Carlton 2019). In addition, cyber sextortion has the potential of worsening sex trafficking and gang rape challenges, as perpetrators tend to demand sexual acts from their victims (Mondal et al. 2022). Additionally, addressing sextortion can be difficult because victims choose to remain anonymous (Patchin and Hinduja 2020). On the other hand, the anonymous nature of the Internet enables perpetrators to remain unidentified with a sense of impunity (Wang 2024). Perpetrators may or may not have the sexual images that they claim to possess in attempts to extort money from victims (Cross et al. 2023). That is, victims cannot verify if threats are backed up with existing content, or if they ensue from "deepfake" images or videos. Sextortion also includes privacy and security threats sent via technology to victims and the distribution of sexual material in an attempt to coerce the victim into cooperation (Pethers and Bello 2023). According to the provided descriptions, cyber sextortion relates to coercive sexting and romance scams (Carlton 2019; Wolak et al. 2018), which are presented in the following sections.

2.3. Coercive Sexting

Sexting is the practice of creating and sharing sexual images online within the context of either dating or a sexual relationship, which is also known as consensual sexting (Gassó et al. 2019; Kernsmith et al. 2018). However, consensual sexting is seen as a potential threshold for dangerous types of online victimization, such as sextortion, child grooming, and cyberbullying (Almeida and Barreiros 2024; Gámez-Guadix et al. 2017; Gassó et al. 2019). Sextortion may occur between acquaintances of an ended romantic relationship as an attempt to force its continuation (Pethers and Bello 2023). Initially, sexual images are voluntarily shared in an intimate context, a practice that is known as consensual sexting, and later distributed by the perpetrator for various motives, such as forcing a sexual relationship (Gámez-Guadix et al. 2022). On the other hand, risk factors contributing to adolescents' susceptibility to online grooming and child sexual abuse include pornographic sexting and coercive strategies (Almeida and Barreiros 2024; Schoeps et al. 2020). Pornographic sexting involves the sharing of complete and partial nudity images, while coercive strategies pertain to forcing another person into sexual relations. Therefore, coercive sexting is a strategy of using tactics to compel another person into sending their intimate pictures or videos (Kernsmith et al. 2018). These practices fit the description of cyber sextortion, which includes the use of social media to exchange sexual text messages, intimate images, and videos (Mondal et al. 2022), and where the exchanges can be mutual or under compulsion.

Additionally, sexting is one of the requirements for online child grooming, as it is usually initiated by the sharing of personal messages and sexual content before the perpetrators reveal their abusive intentions (Almeida and Barreiros 2024). Therefore, sexting is related to cyber sextortion and is used for sexual initiation and as a coercive strategy, manipulation, and blackmail tool to force victims to comply with the perpetrators' demands (Klettke et al. 2019; Ray and Henry 2024; Schoeps et al. 2020).

2.4. Online Romance Scams

Sextortion may also result from romance fraud or scams, which involve an online constructed relationship for financial gains from unsuspecting victims (Cross et al. 2023). In this case, sextortion attacks may be perpetrated by victims' acquaintances (Pethers and Bello

2023). The authors (Patchin and Hinduja 2020), in their study involving adolescents, found that sextortion occurred more between acquaintances, whether romantic or otherwise, as opposed to attacks from an unknown person. Sextortion is also a technique used by perpetrators to enforce continued compliance for financial gains from victims (Cross et al. 2023). In the form of a romance scam, sextortion is facilitated using fake profiles on social media sites such as Facebook and dating apps, which is also known as catfishing (Carlton 2019; Kibe et al. 2022; Mondal et al. 2022). Furthermore, sextortion may be linked to webcam pornography, as there is no guarantee that such acts are free from duress (Humphreys et al. 2019). However, little is known about sextortion emanating from romance fraud (Cross et al. 2023).

Sextortion may occur as an attempt to force a romantic partner to stay in the relationship; in this case, sexual images that were obtained consensually are later used to threaten victims or exposed to stop a partner from leaving the relationship (Gámez-Guadix et al. 2022; Pethers and Bello 2023; Wolak et al. 2018). Cyber sextortion may occur as a result of online interactions where perpetrators obtain explicit images under the pretense of romantic interest (romance scams). The perpetrators then coerce additional images, sexual acts, or money from victims (Cross et al. 2023). For instance, in Indonesia, an extorter obtained a victim's nude images by pretending to be a national military member who intended to marry the victim upon his return from another province where he was deployed. After getting acquainted, the perpetrator asked the victim to send nude photos and then threatened to spread the received images if the victim did not send money to the perpetrator (Muslimin et al. 2024).

2.5. Cyber Sextortion Characteristics in Cybersecurity

In their study, O'Malley and Holt (2022) identified four different themes of sextortion perpetrators based on crime characteristics: (1) perpetrators of cyber sextortion on minors, (2) perpetrators of cyber sextortion using cybercrime, (3) abusive cyber sextortion perpetrators who are in romantic relationships with the victims, and (4) perpetrators of cyber sextortion who are transnational criminals. Sextortion of minors involves online grooming techniques to establish a trusting relationship with children and the gradual use of affectionate language and suggestive comments to solicit sexual content. Eventually, the offender demands more sexual content and physical contact (Almeida and Barreiros 2024; Notté 2024; O'Malley and Holt 2022). Therefore, authors (Thompson et al. 2024) note that sextortion is defined as the coercion of a minor into creating and sharing sexually explicit content with the offender. In cybercrime, perpetrators use trickery to make their victims believe that they possess explicit images or videos obtained through hacking victims' computers or webcams in order to coerce compliance (Cross et al. 2023; O'Malley and Holt 2022). Cyber sextortion perpetrators also often use email phishing schemes and malware as a method to hack a victim's webcam, computer files, or social media accounts (Carlton 2019; Pethers and Bello 2023).

Phishing in cybersecurity is defined as a scalable deception technique that uses impersonation to collect information from a target (Lastdrager 2014, p. 8). In the case of cyber sextortion, phishing involves perpetrators sending emails to victims with claims that they possess victims' intimate images or proof of pornographic website visits, along with payment demands (O'Malley and Holt 2022). On the other hand, malware known as remote access Trojans has been used by sextortion perpetrators to control unsuspecting victims' computers, a practice known as slaving (Carlton 2019). Cybercriminals deceive victims into downloading malware in order to gain access to their private photos via their webcams or personal files (O'Malley and Holt 2022; Wittes et al. 2016). Sextortion may occur in an intimate relationship where an abusive partner threatens to release intimate images or

videos to keep the victim from leaving the relationship or as a means of coercive strategy and power (Henry et al. 2023; Vitis 2020). This form of cyber sextortion relates to both online and offline gender-based and domestic violence as a common strategy used by men (Muslimin et al. 2024; Ray and Henry 2024). Therefore, technology promotes alternative or simultaneous means for perpetrators to transmit gender-based violence (Kavishe 2024). Transactional criminals (organized crime groups) intentionally lure male victims into online sexual activities, secretly recording the acts and eventually threatening to expose them unless they pay money (Edwards and Hollely 2023; O'Malley and Holt 2022). In addition, sextortion is a type of organized crime in which perpetrators pose as someone else online in order to trick their victims into sharing intimate images before blackmailing them for money (Cross et al. 2023; Foster 2023).

2.6. Research Objectives

The sextortion phenomenon was recently established and still lacks empirical studies (Notté 2024; O'Malley and Holt 2022; Patchin and Hinduja 2020). Additionally, the observations that are presented in the background of this study make it imperative to measure and present a comprehensive review of the cyber sextortion field's maturity, as evidenced by its recency and a lack of consistent definitions and empirical research (Carlton 2019; Hagglund and Khan 2023; Notté 2024; O'Malley and Holt 2022; Patchin and Hinduja 2020; Power and Bello 2022). Furthermore, a comprehensive review is necessary considering the multifaceted manifestations of cyber sextortion, including social engineering, privacy and cybersecurity threats, deception, Internet-afforded anonymity, and especially romance scams or fraud and coercive sexting (Cross et al. 2023; Gassó et al. 2019; Pethers and Bello 2023; Power and Bello 2022; Wolak et al. 2018). Therefore, this study focuses on a bibliometric review (Waheed et al. 2018) of cyber sextortion, along with its prevalent manifestation facets, romance scams or fraud and coercive sexting.

To the best of our knowledge, no comprehensive bibliometric study of the scholarly literature on cyber sextortion exists. Using a bibliometric analysis of the field, this study is the first to examine the trend of cyber sextortion, including its publications, thematic developments, and outstanding scholars and their contributions, and explore publication networks and collaborations between institutions, countries, and regions over time.

The outcomes of this study will provide invaluable knowledge for emerging scholars in the field of cyber sextortion. This knowledge includes the ability to easily identify the most cited research articles, outstanding authors, trending themes, and the thematic future direction of cyber sextortion research. The main research question addressed in this study is: how has cyber sextortion research progressed over time regarding scientific productions, thematic developments, scholars' contributions, and the future thematic trajectory?

3. Materials and Methods

This study employed bibliometric mapping analysis, which has recently gained popularity in science mapping (Aria and Cuccurullo 2017; Song et al. 2019). A comprehensive bibliometric analysis was conducted on published scholarly works on cyber sextortion in the Scopus indexed database. The following sub-sections present the procedure that was used to conduct the bibliometric mapping analysis in this study, including data collection, extraction, and cleaning, data analysis and synthesis, and results and discussion, as depicted in Figure 1.

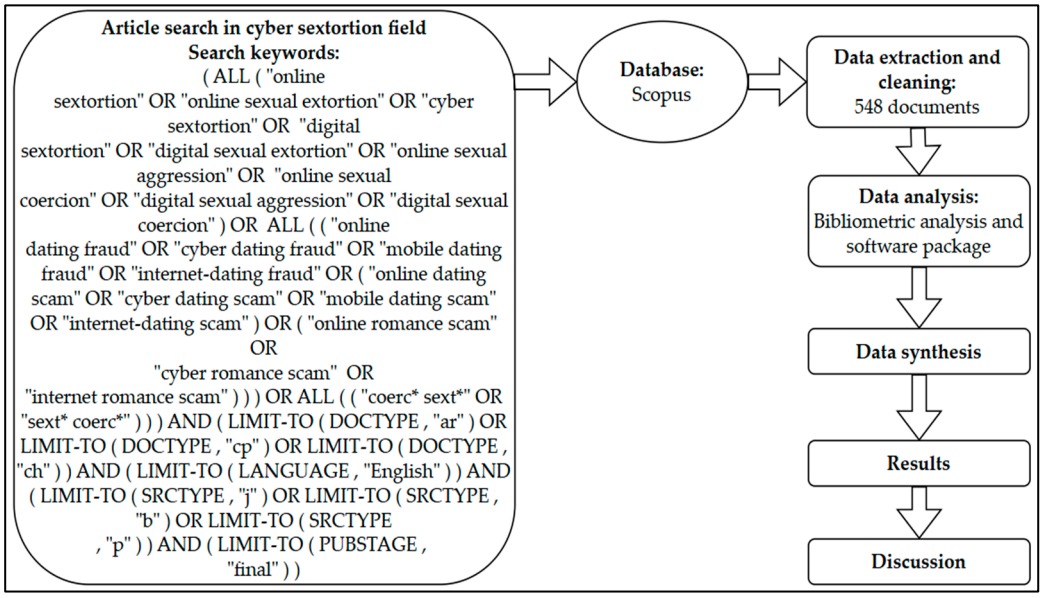

Figure 1. Bibliometric procedure used to conduct this study.

3.1. Data Extraction and Cleaning

Figure 1 presents the search string combination, operators, and filtering in the left-side block. A compound search and concatenation were carried out using the OR Boolean operator. The search string contained the keywords searched, including an asterisk (*) wildcard so that all possible keywords falling within the search would be included in the results. For instance, using the search string "coerce* sext*" returned results that included "coercive sexting", "coercion sexting", or "coerced sexting", etc. Table 1 presents the search strings and rationale for included keywords.

Table 1. Search string rationale.

Search String	Rationale
("online sexual aggression" OR "online sexual coercion" OR "online sextortion" OR "online sexual extortion" OR "cyber sextortion" OR "digital sexual aggression" OR "digital sexual coercion" OR "digital sextortion" OR "digital sexual extortion")	Technology-facilitated sextortion is termed "cyber" or "online" sextortion, sexual aggression, sexual coercion, or sexual extortion (Champion et al. 2022; Liggett 2019; O'Malley and Holt 2022).
("cyber dating fraud" OR "mobile dating fraud" OR "online dating fraud" OR "internet-dating fraud") OR ("online dating scam" OR "cyber dating scam" OR "mobile dating scam" OR "internet-dating scam") OR ("online romance scam" OR "cyber romance scam" OR "internet romance scam")	Initially shared intimate images are often used to threaten victims (Mainwaring et al. 2024), and online dating facilitates sextortion acts (Carlton 2019; Mondal et al. 2022). In addition, online dating facilitates sextortion acts such as scams (Carlton 2019; Cross et al. 2023; Mondal et al. 2022; Pethers and Bello 2023).
("coerc* sext*" OR "sext* coerc*")	Cyber sextortion also involves coerced sexting (Wolak et al. 2018), and sexting relates to sextortion as an enabler or tactic (Cross et al. 2023; Gámez-Guadix et al. 2022; Ray and Henry 2024).

Asterisk symbol (*) = Wildcard.

The document type for all searches was limited to journal articles (ar), conference papers (cp), and book chapters (ch) published in English. At the center of Figure 1, the oval

shape symbolizes the Scopus database, which was the primary source for the document search. Although there were other databases that could have been used, such as Web of Science, PubMed, and ERIC, the Scopus database was chosen because it is a curated, excellent source of bibliometric data for scholarly research in quantitative science studies, providing an extensive collection of journal publications (Baas et al. 2020, p. 377; Singh et al. 2021).

The search results returned 548 documents based on the search string presented in Table 1. These documents were downloaded in CSV file format, including all documents that contained search string keywords in the title, abstract, or author keywords. No data cleaning was conducted, as no duplicates or discrepancies were identified in the document list.

3.2. Data Analysis

The dataset was analyzed using the bibliometric R-package software, version 4.4.0, an open-source software developed in the R language (Aria and Cuccurullo 2017). For the purposes of this study, the software did not support the merging of data generated from independent databases (Agbo et al. 2021). This software provides a set of tools for conducting quantitative research in bibliometrics using algorithms for conducting statistical and science mapping analysis. Furthermore, it features a web interface application called Biblioshiny, which allows importing data in CSV, BibTex, or plain text formats from Scopus or Web of Science databases. For this study, Biblioshiny was used to analyze the CSV file dataset from Scopus.

3.3. Data Synthesis

Table 2 presents a summary of information on the dataset, document contents, authors, and author collaborations. The dataset's timespan was between 2008 and the third quarter of 2024, with a total number of 548 documents. A total of 1403 author's keywords (DE) were used to scope the focus of published documents. Of 1392 authors, 76 were individually authored documents, while single-authored documents numbered 110. Document types include 410 articles, 69 conference papers, and 69 book chapters.

Table 2. Data synthesis indicates primary information and a summary of the dataset.

Description	Results
MAIN INFORMATION ABOUT DATA	
Timespan	2008–2024
Sources (Journals, Books, etc.)	336
Documents	548
Annual Growth Rate %	31.19
Document Average Age	3.14
Average citations per doc	14.59
References	29,307
DOCUMENT CONTENTS	
Keywords Plus (ID)	1816
Author's Keywords (DE)	1403
AUTHORS	
Authors	1392
Authors of single-authored docs	76
AUTHORS COLLABORATION	
Single-authored docs	110
Co-Authors per Doc	3.32
International co-authorships %	18.98
DOCUMENT TYPES	
Article	410
book chapter	69
conference paper	69

4. Results

This section presents the results of the work, organized as follows: (1) the growth of cyber sextortion research based on publication output, distribution, source, and citations; (2) scholarship, affiliations, and social networks; and (3) the thematic focus in in the cyber sextortion field.

4.1. The Growth of Cyber Sextortion Research

Table 3 was derived using the bibliometrix R package and shows the average annual growth of cyber sextortion research, covering 31.19% of scientific production from 2008 to the third quarter of 2024.

Table 3. Annual Article production.

Year	Articles
2008	1
2009	1
2010	0
2011	0
2012	3
2013	6
2014	6
2015	10
2016	18
2017	24
2018	28
2019	43
2020	58
2021	76
2022	86
2023	111
2024	77

The term 'cyber sextortion' was not familiar before 2012. Before 2008, the terminology was not used in any known research. As shown by Table 3, one article (Tettey 2008) presented research on "globalization and Internet fraud in Ghana", pointing to the start of research in Africa regarding the understanding of nefarious activities that technology was starting to present. In 2009, another article with the theme of "online friendships" was published, showing how technology was shaping behavior and human interaction (Fair et al. 2009). These early authors did not directly or indirectly address any specific themes related to cyber sextortion in their titles and abstracts. However, a clear pattern was beginning to emerge, namely the focus on behavior and nefarious activities.

There were no publications in the field of cyber sextortion in 2010 and 2011. Research in cyber sextortion seems to have possibly commenced from 2012 onwards, with Whitty and Buchanan (2012), Couch et al. (2012), and Mazanderani (2012) being the first three articles published that year, mainly focusing on "online romance scams", "risks and dangers of online dating", and "online dating ethics of intimacy", respectively. In 2013, the number of articles that touched on nefarious online behavior increased to six, but there was no recorded growth in 2014. The number of published documents increased steadily from 2015 to 2018, with six, ten, eighteen, twenty-four, and twenty-eight recorded articles for the respective years, which indicated a steady growth of research and understanding of cyber sextortion. There was gradual growth from 2019 to 2021, with 43, 58, and 76 articles recorded in those years, respectively. In 2022, the number of published documents in the field of cyber sextortion slowed down, with only 86 articles recorded. However, there was a sharp increase in the number of published documents in 2023. In September 2024,

the number of recorded documents was 77. So far, the highest number of publications recorded was in 2023, with 111 articles, indicating an impressive growth trend in the cyber sextortion field. Since the cyber sextortion field is still emerging, the number of scientific publications is expected to continue growing year-on-year, as shown in the outcomes of this analysis. Figure 2 visualizes the geometric progression of scientific production over a period of 17 years.

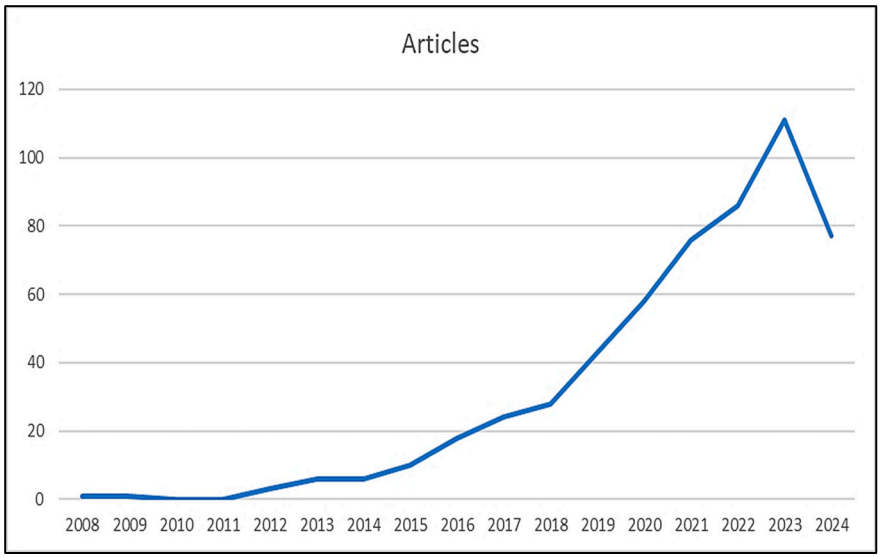

Figure 2. Annual scientific growth of cyber sextortion: a geometric progression ratio with a constant scientific production rate over a period.

Table 4 provides the annual average citation counts for publications on cyber sextortion, illustrating their impact on the field's growth and the quality of research contributions (Bornmann and Mutz 2015; Larsen and von Ins 2009). Studies indicate that the number of citations for a publication forms indices for ascertaining its significance and scholarly impact (Grant et al. 2000).

Table 4. Average citations per year.

Year	Average Citation
2008	0.06
2009	1.25
2012	4.79
2013	2.62
2014	3.02
2015	5.65
2016	3.11
2017	4.74
2018	5.37
2019	4.19
2020	4.01
2021	3.70
2022	2.34
2023	1.57
2024	0.61

Prior work before 2012, by Tettey (2008) and Fair et al. (2009), was not included in the theme of sextortion and yielded average citations of 0.06 and 1.25, respectively. Three seminal articles were published in 2012 by Whitty and Buchanan (2012), Couch et al. (2012), and Mazanderani (2012) on cyber sextortion, which yielded an average of 4.79 citations per

year. This pointed to the significant impact of these works in shaping the early foundations and seminal understanding of cyber sextortion. However, in 2013, there was a noticeable decline in the average number of citations, dropping to 2.62. This trend reversed in the subsequent years, with the average rising to 3.02 in 2014 and peaking at 5.65 in 2015, the highest annual average in the dataset. This peak reflects a period of notable growth and high-quality contributions to the field of cyber sextortion.

4.2. Scholarship, Affiliations, and Social Networks

After 2015, the average number of citations decreased to 3.11 in 2016 but gradually rose again in 2017 and 2018, reaching 4.74 and 5.37, respectively. Despite a minimal increase in the number of publications in 2018, the quality and influence of these publications remained substantial, as indicated by the high average citation count of 5.37. This consistency in citation performance could be attributed to the limited yet focused definition of cyber sextortion during this period (Hagglund and Khan 2023).

From 2019 onward, the average number of citations experienced a gradual decline, with figures dropping to 4.19 in 2019, 4.01 in 2020, 3.70 in 2021, 2.34 in 2022, and 1.57 in 2023. Interestingly, this decline coincided with a sharp increase in the number of scientific publications in the field, as shown in Table 3. By the third quarter of 2024, the average citation count had further decreased to 0.61. This downward trend in average citations since 2019 may be a consequence of the growing volume of publications in the cyber sextortion field. As pointed out in Table 4, the rising number of publications indicates sustained interest and engagement in cyber sextortion and online sexual behavior despite the decline in publication citations.

The top 20 most relevant sources of published work on cyber sextortion are presented in Figure 3, based on data retrieved from Scopus in September 2024. The journal *Computers in Human Behaviour* remained the most relevant and most cited (753 documents) source at the time of this study. Other relevant sources included the *Journal of Interpersonal Violence* (300 documents), the *International Journal of Environmental Research & Public Health* (219 documents), and the *Archives of Sexual Behaviour* (177 documents). Apart from these sources, other multidisciplinary sources included *Victims and Offenders* (133 documents), *the Conference on Human Factors in Computing Systems* (107 documents), *the International Journal of Cyber Criminology* (69 documents), *the Journal of Financial Crime* (161 documents), *the Palgrave Handbook of International Cybercrime* (61 documents), and *ECrime Researchers Summit (ECRIME)* (85 documents), to name but a few.

Citation counts were used to understand the publication's influence in cyber sextortion, with local citations indicating relevance. As Hasumi and Chiu (2024) noted, Biblioshiny for Bibliometrix was the tool used to elicit local citation metrics to identify core publications. Further analysis compared local documents and the same documents cited globally. This analysis is presented in Table 5.

Among the documents analyzed, Henry and Powell's (2018) article on technology-facilitated sexual violence (TFSV), published in *Trauma, Violence, and Abuse*, was the most globally cited paper, with 301 citations. Their detailed work addressed various dimensions of TFSV, such as coercion into unwanted sexual acts. The work addressed the scarcity of both qualitative and quantitative research in this domain, particularly concerning adults. Their findings revealed significant gaps in understanding the nature, scope, and impacts of TFSV, which predominantly affected women. Klettke et al.'s (2019) study on sexting and psychological distress stood out with the highest local citation count of 71 and a global citation count of 98. Similarly, Whitty and Buchanan's (2012) article on online romance scams had 70 local citations and 114 global citations, while Drouin et al.'s (2015) work on sexting as a form of intimate partner aggression also recorded 70 local citations but

a significantly higher global citation count of 209. Interestingly, papers with high global citation counts, such as McGlynn et al.'s (2017) article on image-based sexual abuse (277 global citations, 39 local citations) and Van Ouytsel et al.'s (2017) study on adolescent sexting behaviors (164 global citations, 32 local citations), tended to have relatively lower local citation numbers. This trend was found to be consistent across the dataset, as seen with Klettke et al. (2019) and Whitty and Buchanan (2012), whose work had a broader global impact. These works pointed to widespread recognition of the contribution in areas of cyber sextortion and online romance fraud.

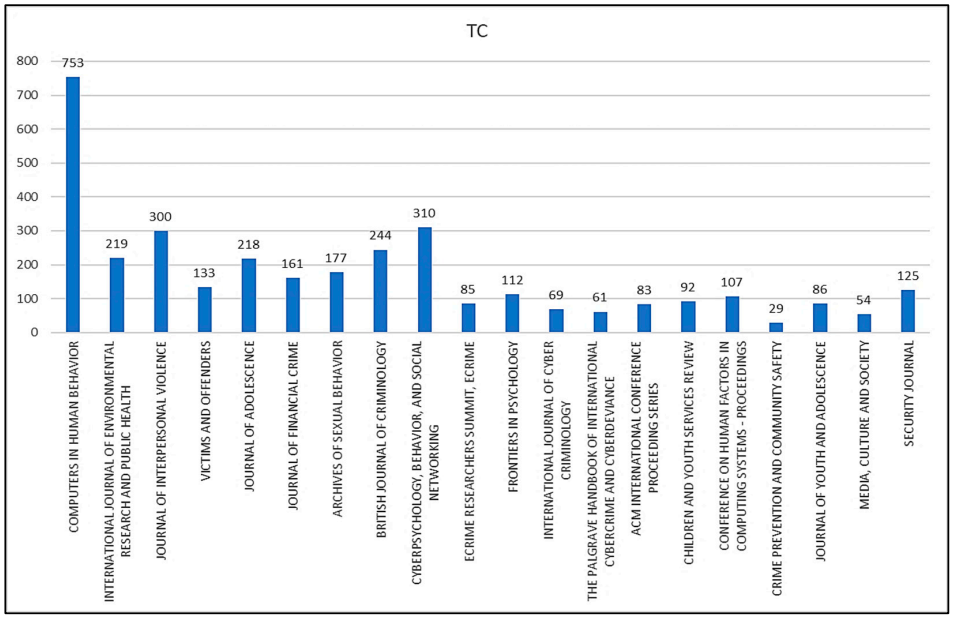

Figure 3. Relevant publishing outlets with the most local citations.

This study analyzed the global scientific production and contribution to the field of cyber sextortion, focusing on countries and regions. The results, presented in Figure 4, show that the United States (USA) has the leading publication count, followed by Australia, the United Kingdom (UK), and Spain. Other contributing countries include Indonesia, the Philippines, Malaysia, India, Pakistan, Israel, and China in Asia; Belgium, Germany, Portugal, and the Netherlands in Europe; and South Africa, Nigeria, and Ghana in Africa. African contributions remain limited, with South Africa, Ghana, and Nigeria as emerging contributors.

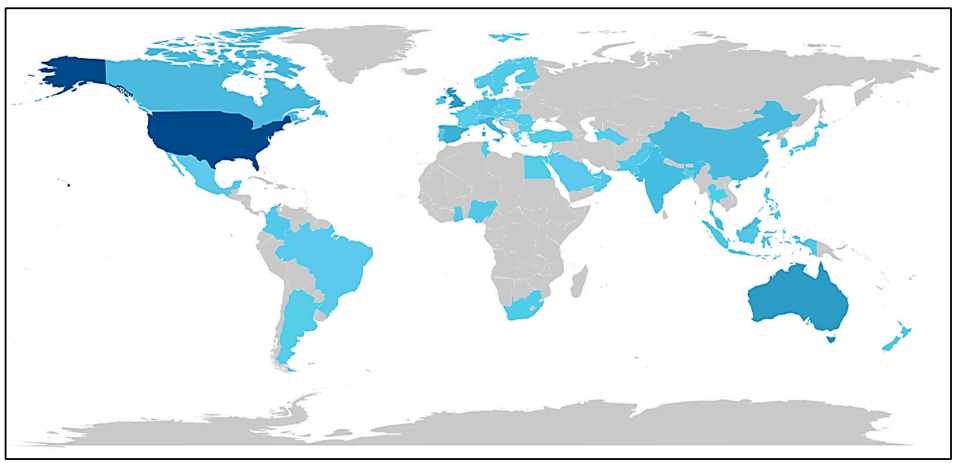

Figure 4. Scientific production and contribution of the top 20 countries/regions.

Table 5. Top twenty most cited references based on the number of local citations from the collection dataset.

Document Title	Reference	Publication Source	LTC	GTC
Sexting and Psychological Distress: The Role of Unwanted and Coerced Sexts	Klettke et al.'s (2019)	*Cyberpsychology, Behaviour, and Social Networking*	71	98
The Online Romance Scam: A Serious Cybercrime	Whitty and Buchanan (2012)	*Cyberpsychology, Behaviour, and Social Networking*	70	114
Sexting: A New, Digital Vehicle for Intimate Partner Aggression?	Drouin et al. (2015)	*Computers in Human Behaviour*	70	209
The Online Dating Romance Scam: Causes and Consequences of Victimhood	Buchanan and Whitty (2014)	*Psychology, Crime and Law*	59	126
Online, Offline, and Over the Line: Coercive Sexting Among Adolescent Dating Partners	Kernsmith et al. (2018)	*Youth and Society*	51	76
The Prevalence of Sexting Behaviours Among Emerging Adults: A Meta-Analysis	Mori et al. (2020)	*Archives of Sexual Behaviour*	42	134
The Scammers Persuasive Techniques Model	Whitty (2013)	*British Journal of Criminology*	40	107
Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse	McGlynn et al. (2017)	*Feminist Legal Studies*	39	277
The Online Dating Romance Scam: The Psychological Impact on Victims—Both Financial and Non-Financial	Whitty and Buchanan (2016)	*Criminology and Criminal Justice*	38	102
Anatomy of the Online Dating Romance Scam	Whitty (2015)	*Security Journal*	38	86
Sexting Coercion as A Component of Intimate Partner Polyvictimisation	Ross et al. (2019)	*Journal of Interpersonal Violence*	35	63
Sexting: Adolescents' Perceptions of the Applications Used for, Motives for, and Consequences of Sexting	Van Ouytsel et al. (2017)	*Journal of Youth Studies*	32	164
Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research	Henry and Powell (2018)	*Trauma, Violence, and Abuse*	30	301
No Laughing Matter: Blaming the Victim of Online Fraud	Cross (2015)	*International Review of Victimology*	28	111
Do You Love Me? Psychological Characteristics of Romance Scam Victims	Whitty (2018)	*Cyberpsychology, Behaviour, and Social Networking*	27	85
Understanding Romance Fraud: Insights from Domestic Violence Research	Cross et al. (2018)	*British Journal of Criminology*	25	53
Association Between Sexting and Sexual Coercion among Female Adolescents	Choi et al. (2016)	*Journal of Adolescence*	23	78
Online Romance Scams and Victimhood	Sorell and Whitty (2019)	*Security Journal*	22	34
Not-Allowed Sharing of Sexts and Dating Violence from the Perpetrator's Perspective: The Moderation Role of Sexism	Morelli et al. (2016)	*Computers in Human Behaviour*	20	85
Improving the Police Response to Online Fraud	Cross and Blackshaw (2015)	*Policing (Oxford)*	19	46

LTC = Local Total Citation; GTC = Global Total Citation.

Further analysis of the top 20 countries by total and average citations, presented in Table 6, reveals that the USA holds the highest total citations (1685, average 15.30), followed by the UK (1422, average 30.90) and Australia (1369, average 21.40). Notably, Belgium, with 403 total citations and the highest average (50.40), as well as countries such as Norway, Sweden, and Hong Kong, despite lower publication counts, exhibit significant impact through high citation averages. South Africa ranks 21st globally, with 21 citations (average 5.20), while Ghana and Nigeria rank 24th and 28th, respectively. This indicates that while African countries are underrepresented, their contributions to cyber sextortion research are beginning to grow, particularly in the southern and western African regions.

Table 6. Top twenty most cited countries in the field of cyber sextortion.

Country	Total Citations (TC)	Av. Article Citations
USA	1685	15.30
United Kingdom	1422	30.90
Australia	1369	21.40
Belgium	403	50.40
Spain	358	13.30
Canada	329	18.30
Italy	284	17.80
Netherlands	116	16.60
India	102	10.20
China	78	5.60
Ireland	57	14.20
Germany	55	11.00
Norway	55	18.30
New Zealand	54	54.00
Czech Republic	46	23.00
Israel	46	5.10
Croatia	40	5.70
Sweden	31	7.80
Hong Kong	28	7.00
Georgia	21	7.00

4.3. Thematic Focus in the Cyber Sextortion Field

This study also examined the directional change in topics discussed among scholars in the field of cyber sextortion by analyzing the first author's keywords and their frequency. Key trends, co-occurrence networks, and thematic areas were investigated to understand the evolving focus of research. According to Song et al. (2019), analyzing publication keywords is crucial to identify trending topics and scholarly focus within a field. Keywords offer a quick snapshot of a publication's primary topic and emphasis. The keyword dynamics are illustrated in Figure 5.

Each line corresponds to a keyword, with the frequency in the third quarter of 2024 indicated in parentheses. The figure reveals that terms such as cybercrime and fraud began appearing in 2013, while keywords such as sexting, victimization, online dating, scams, social media, intimate partner violence, and mental health emerged in 2015. In subsequent years, adolescents and dating violence appeared in 2016, followed by sextortion, romance fraud, and image-based sexual abuse in 2017. The term sexual harassment was introduced in 2018. The frequency of these keywords has steadily grown since their first appearance. By the third quarter of 2024, sexting reached 104 mentions, cybercrime 64 mentions, and adolescents 35 mentions. Similarly, the terms sextortion and online fraud each increased to 22 mentions, while romance fraud rose to 16 mentions. Notably, keywords such as sextortion, romance fraud, and image-based sexual abuse have gained prominence since 2017. These trends indicate that cyber sextortion research will likely continue to focus on core topics, including sexting, cybercrime, adolescents, online dating, romance fraud,

image-based sexual abuse, and sexual harassment. This ongoing evolution reflects the dynamic nature of the field and its responsiveness to emerging societal challenges.

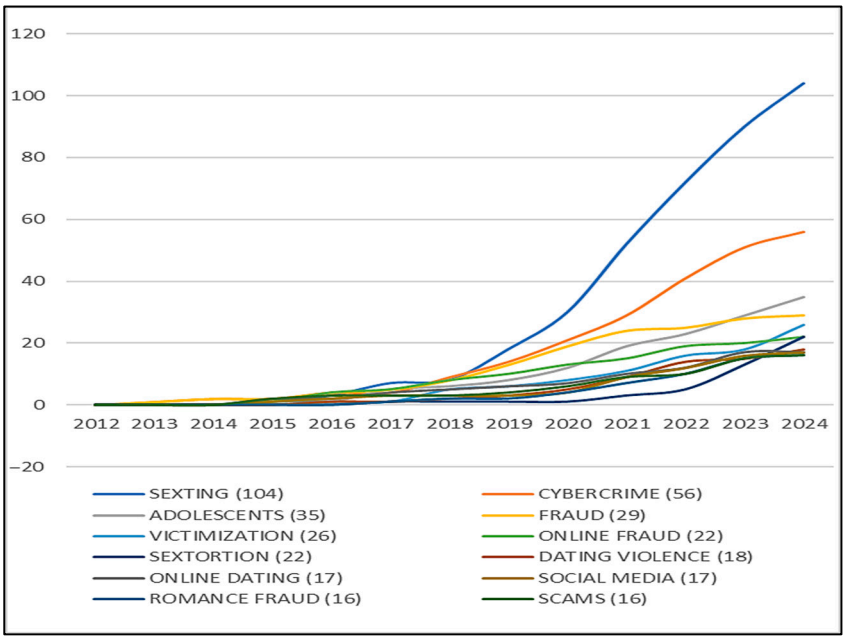

Figure 5. Dynamic view of authors' keywords over time.

This study also analyzed the keywords co-occurrence network (KCN) to uncover the interconnections and trends within the field of cyber sextortion. The KCN provides insight into the field's knowledge structure by mapping the relationships between keywords found in the literature (Prell et al. 2009). As shown in Figure 6, the network reveals the significant links between various keywords, highlighting how certain terms play a central role in the research landscape. The size and width of the keywords in the visualization indicate their importance and level of interconnectedness with other terms. Sexting is a pivotal keyword, closely connected to related terms such as adolescents, youth, young adults, and online victimization.

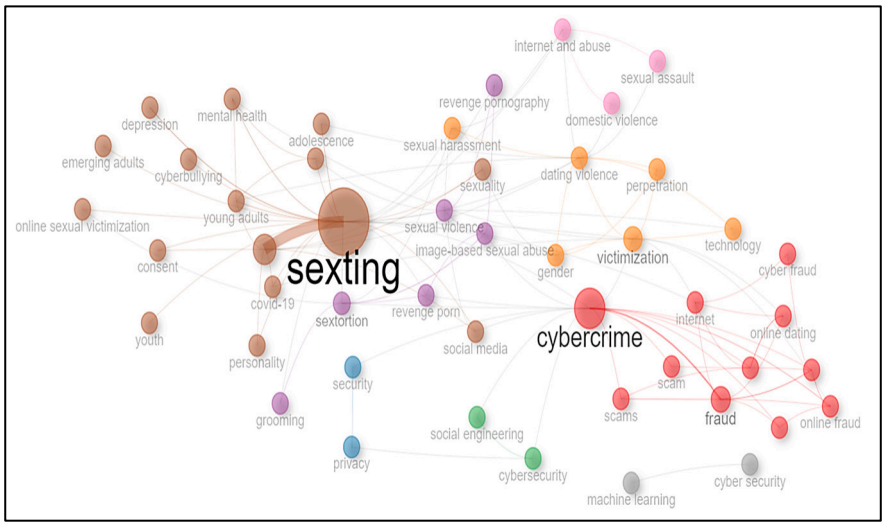

Figure 6. Co-occurrence network of keywords.

The term sextortion is strongly linked to concepts such as grooming, image-based sexual abuse, and revenge porn, while revenge porn also has ties to social media. The

keyword cybercrime emerges as another significant hub, interlinking with terms such as sextortion, sexting, fraud, social engineering, victimization, and cybersecurity. These findings demonstrate the cohesive structure of the field, where specific keywords act as central nodes, bridging various research topics. This network analysis highlights the interconnected and multidisciplinary nature of cyber sextortion research, indicating that future studies may continue to build on these foundational themes.

Figure 7 presents an overview of the annual rankings and trends of topics in the cyber sextortion field between 2016 and 2024, highlighting their relevance to key themes within the domain. In 2021, cybercrime emerged as the most prominent topic, reflecting its centrality to discussions on online threats and criminal activities.

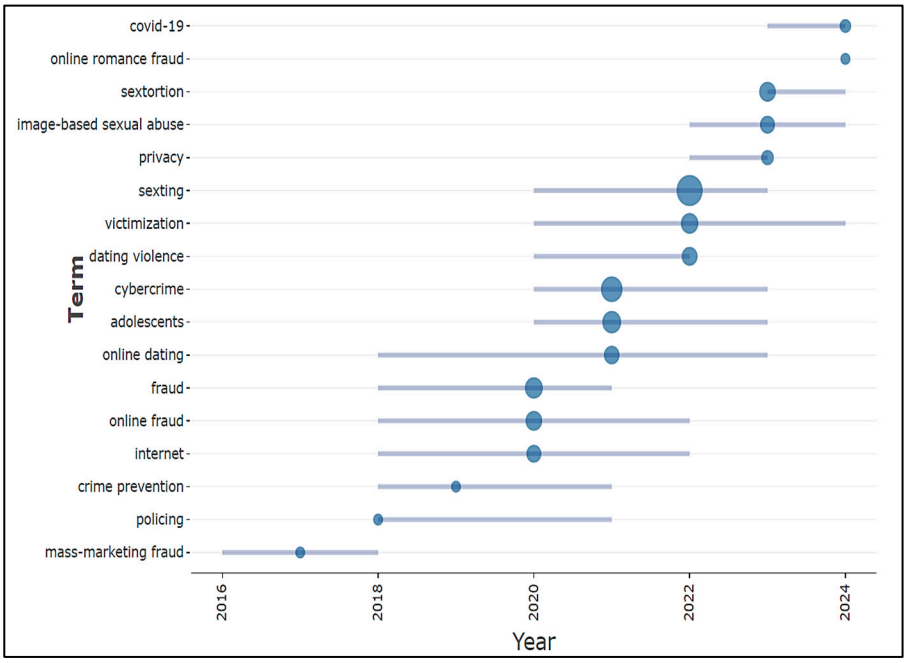

Figure 7. Trending topics between 2016 to 2024.

By 2022, sexting became the most frequently discussed topic, demonstrating increased scholarly focus on its role in cyber exploitation and victimization. The year 2023 witnessed a shift in focus toward sextortion, which became the leading topic of discourse, accompanied by related themes such as image-based sexual abuse and privacy. In the third quarter of 2024, online romance fraud and COVID-19 were the latest trending topics, indicating the evolving nature of the field in response to emerging societal and technological developments. The analysis also highlights the interconnectedness of trending topics within the field. For example, sexting was frequently discussed alongside victimization and dating violence, while cybercrime was examined in relation to adolescence and online dating. Sextortion was often studied in conjunction with image-based sexual abuse and privacy, showcasing the interconnected and multi-dimensional nature of these research themes. Thematic mapping was conducted further to understand the field's current status and future trajectory. This method utilized clusters of interconnected keywords to derive properties of centrality, which reflects the importance of topics, and density, which represents the cohesiveness of research themes (Esfahani et al. 2019). Centrality was used to identify the degree of correlation among different topics, with higher centrality indicating greater importance and positioning within the network. Conversely, density reflected the cohesiveness of topics, signaling their development potential and sustainability.

Topics with high centrality, such as sextortion, cybercrime, and sexting, were positioned as critical themes, indicating their significance and extensive connections to other

areas of study. Topics with high density demonstrated strong cohesiveness, reflecting their maturity as research themes. Emerging topics, such as online romance fraud, have gained attention in recent years, signaling the field's dynamic evolution. This mapping provides a comprehensive understanding of the development and sustainability of research themes within the cyber sextortion domain.

Figure 8 depicts the thematic map of the cyber sextortion research field, categorizing themes into four quadrants (Q1 to Q4) based on their centrality and density. The upper-right quadrant (Q1) represents driving themes (motor themes), which are well-developed and highly important to the field.

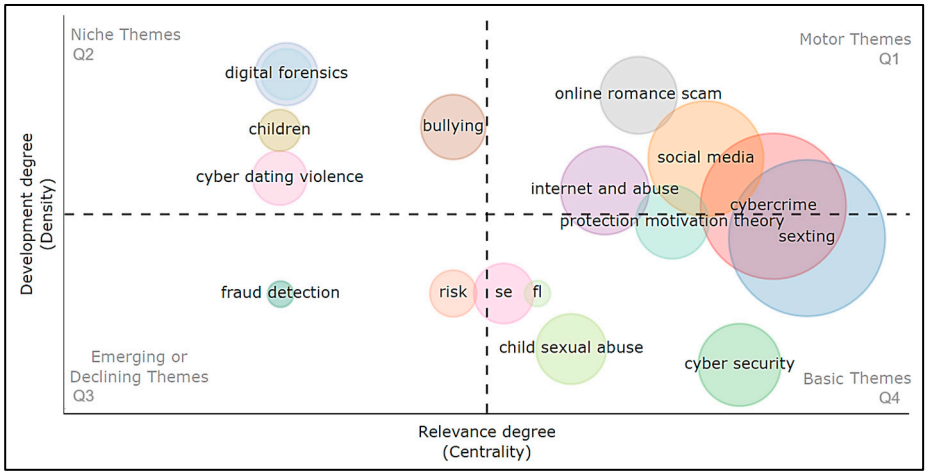

Figure 8. Thematic map.

The lower-right quadrant (Q4) contains underlying themes (basic themes), which are equally significant but less developed. Specialized themes (niche themes) appear in the upper-left quadrant (Q2), characterized by lower relevance to the core research field but connected to other less central topics. Finally, the lower-left quadrant (Q3) includes emerging or declining themes, reflecting marginal importance or themes undergoing transitions. Some node texts overlap due to their proximity. For instance, in Q2, nodes such as "digital forensics" and "all crime" completely overlap, as do "content analysis" and "children". Similarly, in Q3, the "fraud detection" and "fraud prediction" nodes overlap, as well as the "risk" and "self-esteem" nodes. In Q4, the "self-esteem" (se) and "federated learning" (fl) nodes also exhibit overlap. The results highlight key findings within the thematic map. In Q1, highly important themes include the "online romance scam" node, encompassing topics such as financial exploitation and persuasion, and the "social media" node, which includes privacy, intimacy, and deception. Additional critical themes include the "Internet and abuse" and "cybercrime" nodes. In Q4, themes such as the "sexting" node, encompassing topics such as sextortion, sexual violence, dating violence, and intimate partner violence, along with the "protection motivation theory" node, are shown to be well-developed and foundational to the research field. Other key nodes in Q4, such as "child sexual abuse", include topics such as child sexual exploitation, child pornography, and online sexual solicitation. Similarly, the "cybersecurity" node, which includes themes such as machine learning, deep learning, and dating fraud, indicates areas that are still in development but critical to the field. The "self-esteem" node in Q4 includes topics such as deaf adolescents and moderation models, partially traversing into Q3, indicating that these themes are emergent and developing.

Niche themes in Q2 include the "bullying" node, which incorporates topics related to child abuse, educational policy, and educational leadership, as well as other nodes such as "digital forensics", "all crimes", "children", and "cyber dating violence". These themes

connect to less central topics. For example, the "cyber dating violence" node in Q2, which includes coercive sexting, relates to sextortion in Q4. In contrast, the child abuse topic within the "bullying" node connects to themes in the "child sexual abuse" node in Q4. Emerging or declining themes in Q3 include nodes such as "fraud detection" and "fraud prediction". These findings suggest that topics in Q2, such as cyber dating violence, digital forensics, children, and bullying, could be integrated with topics in Q1 and Q4 to develop the cyber sextortion research field further. This integration may enable a more cohesive and comprehensive understanding of the field's evolving dynamics.

4.4. Prolific Scholars, Institutions, and Collaboration Networks

Figure 9 presents the top 20 most prolific scholars contributing to the field of cyber sextortion from 2012 to 2024 based on the dataset. These scholars have demonstrated consistent and impactful contributions to the research in this area. Among them, Cassandra Cross from Australia stands out with a total of 25 documents and 524 citations. Cross holds the highest h-index (14), indicating her significant impact in the field. Her first publication on cyber sextortion appeared in 2015, with an average of 15.7 citations per year. Cross consistently published one to three articles annually from 2015 to 2023, with notable peaks of six articles in 2018 and five in 2020.

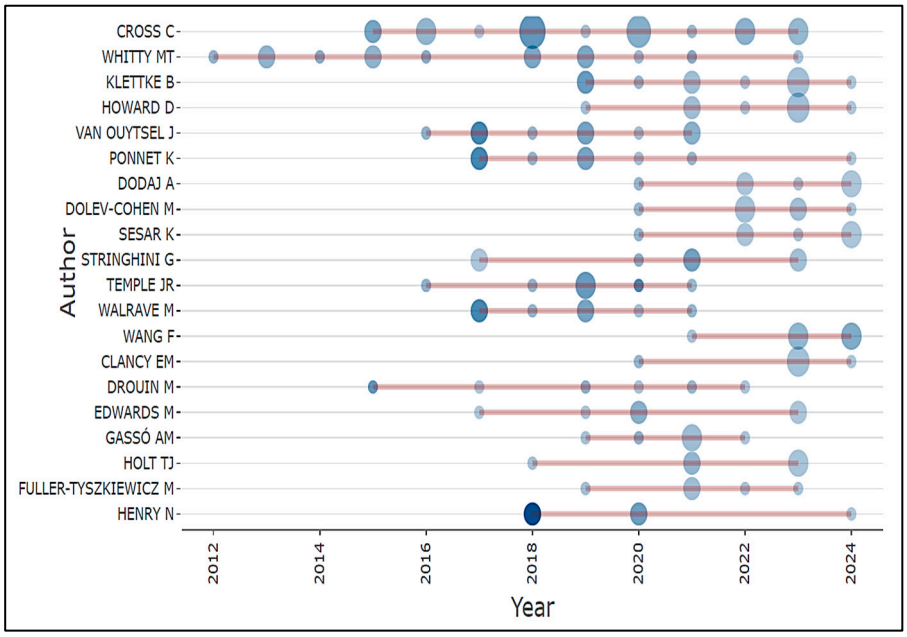

Figure 9. Top 20 authors' productivity over the years.

Monica Whitty from the United Kingdom is another leading scholar, with 14 documents and the highest citation total of 805. Whitty has an h-index of 11, the second highest in the field, highlighting her influence. Her first article in this domain was published in 2012, with an average of 8.77 citations per year. Whitty consistently published one to two articles annually from 2013 to 2023, except for 2017, when no publications were recorded. Bianca Klettke from Australia ranks as another prominent contributor, with 11 documents and 182 total citations. Klettke published her first article in 2019, achieving an average citation count of 19.5 per year. She has consistently published one to two articles annually through to 2024. Dominika Howard, also from Australia, has authored nine articles with a total of 52 citations. Howard's first publication appeared in 2019, with an average citation rate of 3.17 per year. While there were no publications in 2020, Howard has consistently contributed since 2021, peaking with four articles in 2023. Based on productivity over the years, Klettke ranks second and Howard ranks third, with h-indices of 5 and 4, respectively.

Joris Van Ouytsel from Belgium is another significant figure in the field, producing nine articles with an impressive total of 510 citations. Van Ouytsel holds an h-index of 9, signifying his substantial scholarly impact. His first publication appeared in 2016, and he consistently contributed to the field until 2021. Other impactful contributors include Koen Ponnet (Belgium), Jeff R. Temple (USA), and Michel Walrave (Belgium), each with an h-index of 7. Additionally, scholars such as Michelle Drouin, Yu Lu, and Gianluca Stringhini from the USA, alongside Klettke from Australia, have an h-index of 5, affirming their relevance in the research field. These scholars and their contributions, as depicted in Figure 10, highlight the intellectual growth and collaborative efforts within the cyber sextortion research domain. Their publications and citation metrics underscore the evolving landscape and expanding interest in this critical area of study.

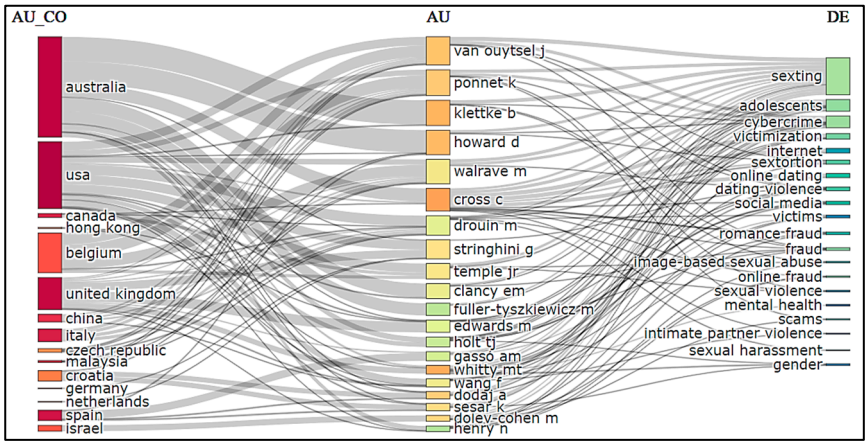

Figure 10. A three-field plot of countries, authors, and themes of cyber sextortion.

Figure 10 provides a visual representation of prolific scholars, their countries, and specific areas of interest (themes) within the field of cyber sextortion. This three-field plot consists of three columns: the left-most column represents countries, the middle column lists authors, and the right-most column highlights themes (authors' keywords).

The frequency of keyword occurrences defines the themes in this study. The significance of each element is reflected in the height of the boxes and the thickness of the connecting lines. Specifically, box height signifies the relative importance of a country, author, or theme, while the thickness of the lines correlates with the volume of scholarly contributions. As indicated by the height of the country boxes, Australia holds the highest number of author affiliations, with 222 contributors affiliated with institutions in the country. Although the United States leads in total scientific productions and citation counts, it ranks second with 148 author affiliations. Belgium follows in third place, with other countries such as the United Kingdom, Italy, Spain, Croatia, China, and Israel contributing notable affiliations.

The thickness of the lines connecting countries to authors illustrates the significant contributions made by specific individuals. In Australia, the leading contributors include Bianca Klettke, Dominika Howard, Cassandra Cross, Elizabeth Clancy, and Matthew Fuller-Tyszkiewicz. In the United States, prolific contributors to the field are Joris Van Ouytsel, Koen Ponnet, Michelle Drouin, Gianluca Stringhini, Jeff Temple, and Fuzhou Wang. Belgium's notable contributors include Joris Van Ouytsel, Koen Ponnet, and Michel Walrave. In the United Kingdom, the primary contributors are Gianluca Stringhini, Matthew Edwards, and Monica Whitty. In Italy, the significant contributors are Joris Van Ouytsel, Koen Ponnet, and Michel Walrave, while in Spain, Aina Gasso is a notable scholar. Croatia's key contributors include Arta Dodaj and Kristina Sesar. In China, major contributors are

Joris Van Ouytsel, Koen Ponnet, Michel Walrave, and Michelle Drouin. From Israel, Michal Dolev-Cohen emerges as a leading contributor to the field.

In terms of themes, "sexting" has garnered the most interest, with 74 associated articles, followed by the "adolescents" theme, with 34 articles authored by scholars such as Joris Van Ouytsel, Koen Ponnet, Bianca Klettke, Michel Walrave, Cassandra Cross, and Jeff Temple. Other themes, including "cybercrime", "online fraud", "romance fraud", and "online dating", are also attracting scholarly attention, with respective article counts of twelve, eleven, nine, and eight. Additionally, emerging themes such as "mental health", "sextortion", "sexual violence", "dating violence", and "intimate partner violence" have attracted some interest, with article counts of three, three, three, two, and two, respectively.

This visual mapping demonstrates the collaborative and thematic focus in the field of cyber sextortion, highlighting the interdisciplinary nature of the research and the key areas that continue to shape its trajectory.

Figure 11 illustrates a three-field plot highlighting the relationship between countries (left-most column), themes of interest (middle column), and authors (right-most column) in the cyber sextortion research field. This visualization offers an overview of global contributions to specific themes and the authors driving research in these areas.

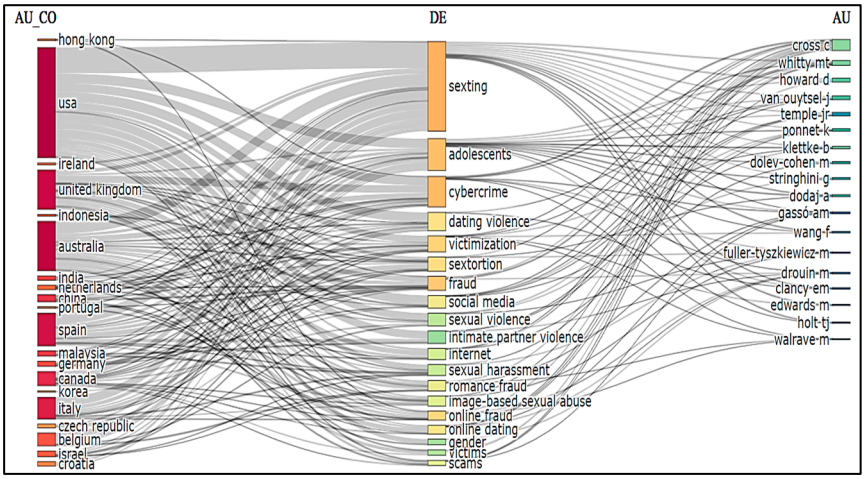

Figure 11. A three-field plot of countries, themes of cyber sextortion, authors.

The results indicate that the "sexting" theme has attracted significant interest from 18 countries, with the United States leading in contributions from the North American region, followed by Australia in the Oceania region. Other notable contributors to this theme include Spain and Italy from southern Europe, Canada from North America, and Belgium from western Europe. Similarly, the "adolescents" theme has garnered attention from 11 countries, with the United States again at the forefront, followed by Australia, Spain, Italy, and Belgium. The "cybercrime" theme has seen contributions from 12 countries, with the United States, the United Kingdom, northern Europe, and Australia taking the lead. The "dating violence" theme, although less widely explored, has received interest from eight countries, led by the United States and followed by Spain, and Italy. The "victimization" theme has garnered substantial interest from 9 countries, with leading contributions from the United States, Australia, Spain, and Italy. Similarly, the "sextortion" theme has attracted research from 9 countries, with Spain emerging as the leader, followed by the United States and India from southern Asia.

The "social media" theme has drawn attention from five countries, with the United States leading, followed by the United Kingdom and Australia. The "intimate partner violence" theme has been addressed by three countries, with the United States again leading, followed by Spain and Malaysia. Notably, regions such as the United States

(North America), Australia (Oceania), Spain (southern Europe), Italy (southern Europe), Canada (northern America), Belgium (western Europe), and the United Kingdom (northern Europe) have made substantial contributions to addressing key themes, including sexting, adolescents, cybercrime, dating violence, victimization, and sextortion. However, there remain themes that require further exploration across different regions. These include topics such as the Internet, fraud, sexual harassment, sexual violence, online dating, mental health, gender, image-based sexual violence, romance fraud, online fraud, scams, and victims, as indicated by the relative heights of their boxes in Figure 11. This highlights opportunities for further research to bridge thematic and geographic gaps in the field.

Institutions, Co-Authorship, and Collaboration Networks

As shown in Table 7, Deakin University in Australia ranks first with 63 documents. It is followed by the Queensland University of Technology, also in Australia, with 25 documents. These two Australian universities are followed by George Mason University in the USA with 23 documents and the Sapienza University of Rome in Italy with a document count of 23. Michigan State University, the University of Antwerp, Zhejiang University, Barcelona International University of Catalonia, the University of Michigan, and the University of Tennessee are all among the top 20 institutions, with document numbers of 20, 19, 15, 12, 12, and 12, respectively.

Table 7. Most relevant institutions in the field of cyber sextortion.

Affiliation	Number of Articles
Deakin University	63
Queensland University of Technology	25
George Mason University	23
Sapienza University of Rome	23
Michigan State University	20
University of Antwerp	19
Zhejiang University	15
Barcelona International University of Catalonia	12
University of Michigan	12
University of Tennessee	12
Arizona State University	11
Oranim Academic College of Education	11
The University of Hong Kong	11
University of California	11
University of Siena	11
Autonomous University of Madrid	10
University of Toronto	10
Monash University	9
Tongji University	9
University of New Hampshire	9

As shown by Table 7, institutions such as Queensland University of Technology, Deakin University in Australia, and Michigan State University in the USA have a big network of collaborations with other universities. This collaboration network is shown in Figure 12.

As shown in Figure 12, Queensland University of Technology has networked with the University of South Florida, Michigan State University, Wayne State University, and Michigan State University. In addition, the University of Hong Kong, Zhejiang University, and Monash University have collaborated with each other. Although these institutions are actively contributing to the research field of cyber sextortion, they have not established collaborations with other institutions to expand their social network in the field.

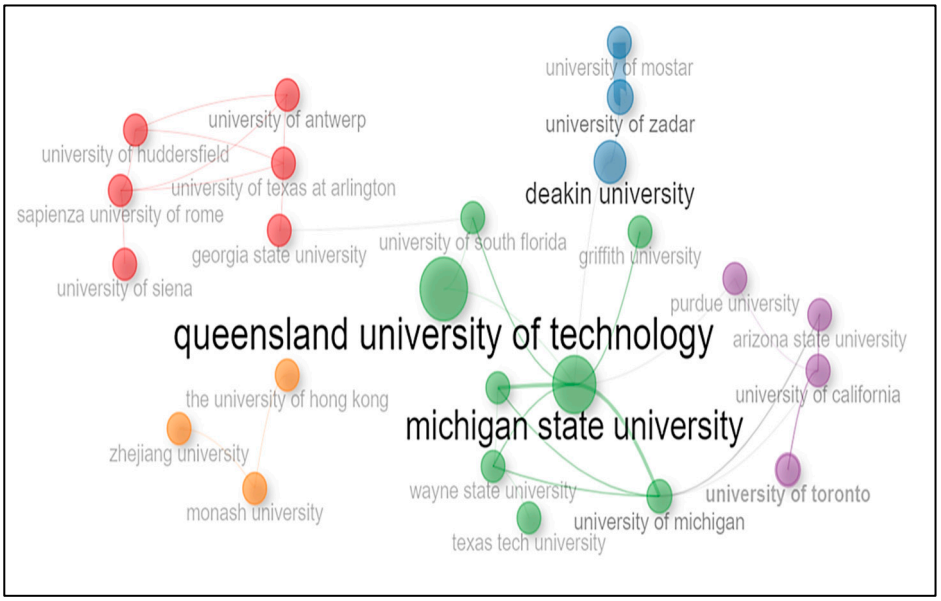

Figure 12. Mapping of institutions' collaboration and social networks.

Regarding co-authorship and social collaboration analysis, this study explored the social structure component of the bibliometrix R-package (Aria and Cuccurullo 2017) provided in the biblioshiny user interface (UI). According to scholars, the social network of actors within a field delineates the relationship between two or more individuals, institutions, or countries with regards to collaborations (Song et al. 2019; Prell et al. 2009). These relationships are presented in a network where nodes represent actors, and links connecting the nodes represent relationships. In this study, the collaboration network between authors is presented in Figure 13.

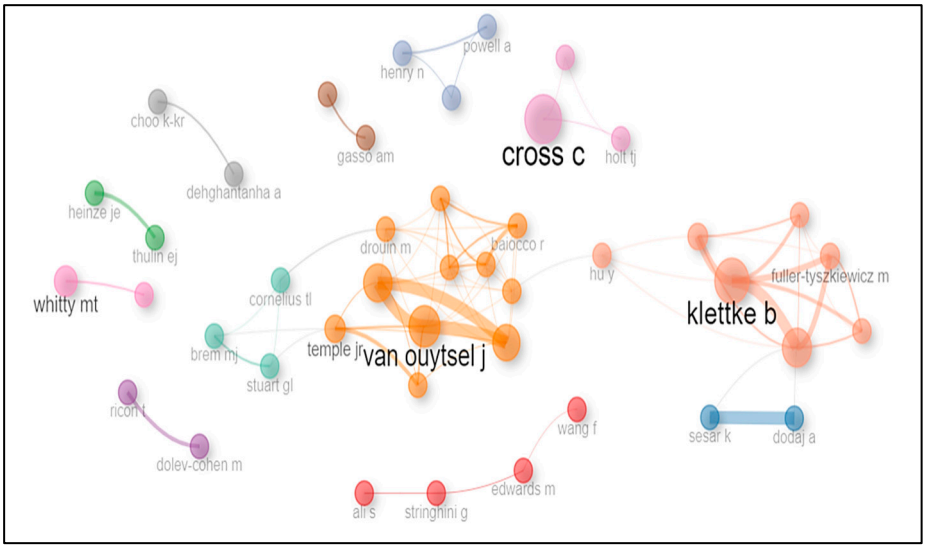

Figure 13. Mapping of authors' collaboration networks.

5. Discussion

This study aimed to address the primary research question of how cyber sextortion research has evolved over time in terms of scientific productions, thematic developments, scholars' contributions, and future thematic trajectories. To achieve this, a bibliometric mapping analysis was employed, providing both quantitative and qualitative measures of reviewing the maturity of the cyber sextortion field. As demonstrated, cyber sextortion

research commenced in 2012, with Whitty and Buchanan (2012), Couch et al. (2012), and Mazanderani (2012) being the first three published articles. There was a steady publication growth of three or more articles between 2013 and 2018, except for 2014, where no growth was recorded. Then, there was an impressive growth trend of 15+ articles between 2019 and 2021, but this growth declined in 2022. In 2023, there was a sharp increase in publication growth, and the sextortion keyword began to trend in the same year. The results also showed that the trending status of the adolescents topic in 2021 paved the way for future studies. For instance, the sexting topic trended in the subsequent year (2022), followed by sextortion in 2023.

Additionally, themes such as self-esteem, deaf adolescents, and the mediation model appear as basic emerging and developing themes with a focus on special needs issues in the cyber sextortion field. Similarly, child sexual abuse, child sexual exploitation, child pornography, and online sexual solicitation are developing in this field as basic and child-focused themes. These findings are particularly insightful because the age groups that are more inclined to report sextortion among children or adolescents aged 12–17 have not been established (Patchin and Hinduja 2020). Thorn's (2017) study found that 47% of participants aged between 13 and 25 experienced sextortion before they reached 18 years. These observations confirm the recency and impressive growth of empirical studies in the sextortion research field, as it was called for in the literature (O'Malley and Holt 2022; Patchin and Hinduja 2020). Hagglund and Khan (2023) note that cyber sextortion lacks a consistent definition. Therefore, the observed research growth in the field could also aid in the creation of adequate cyber sextortion definitions in future studies. Overall, these observations indicate a growth trajectory of the cyber sextortion research field.

The results on relevant sources and documents of cyber sextortion publications showed that *Computers in Human Behaviour* is the most relevant source, while other relevant sources include the *Journal of Interpersonal Violence*, *International Journal of Environmental Research and Public Health*, and *Archives of Sexual Behaviour*. Additionally, the most relevant documents include Henry and Powell's (2018) article published in 2018, which is the most globally cited paper with a total of 301 citations. However, Hasumi and Chiu (2024) note that the number of local citations reveals core publications in a specific field. Therefore, works such as that of Klettke et al. (2019), with 71 local citations and 98 global citations, Whitty and Buchanan (2012), with 70 local citations and 114 global citations, and Drouin et al. (2015), with 70 local citations and 209 global citations, are the most impactful in the field of cyber sextortion. Overall, all documents had low local citation counts compared to global citations. This observation revealed that these authors' work has a great influence in the field of cyber sextortion. Additionally, as suggested by Agbo et al. (2021), a high global citation count indicates that authors also publish their work outside of a research field (in this case, cyber sextortion). This study noted authors who have high global citations, including Henry and Powell's (2018) work with 301 global citations and 30 local citations, McGlynn et al.'s (2017) work with 277 global citations and 39 local citations, and Van Ouytsel et al.'s (2017) work with 164 global citations and 32 local citations. These authors' works, with higher global citation counts, indicate the possibility of multidisciplinary research in the cyber sextortion field (Agbo et al. 2021).

Results on prolific scholars, institutions, and collaboration networks showed that the most outstanding scholars in the field of cyber sextortion include Cassandra Cross from Australia, Monica Whitty from the United Kingdom, Bianca Klettke from Australia, Dominika Howard from Australia, and Joris Van Ouytsel from Belgium. In addition, the results showed a steadily rising interest in the cyber sextortion research field as distinguished authors affiliated with different institutions around the world are inclined to collaborate. These author collaboration networks include those of Cassandra Cross, Bianca Klettke,

Joris van Ouytsel, and Monica Whitty. These collaborations could bring thematic domains such as bullying, cybersecurity, digital forensics, and machine learning into the cyber sextortion field. This is particularly important as Wang and Topalli (2024) advocate for the development of social media tools and algorithms that can recognize the vulnerabilities of victims in order to proactively prevent or stop the continuation of online scams such as romance fraud. Therefore, bullying, cybersecurity, and machine learning domains have the potential to boost the research maturity of the cyber sextortion field.

The results of countries' scientific publications show that the United States of America (USA) is the country with the most contributions, followed by Australia and the United Kingdom (UK). However, countries in the African region had low contributions to the cyber sextortion field, indicating that most African countries are still lagging in the cyber sextortion field, while South Africa in the southern region and Ghana in the western region of Africa are emerging. This dearth of cyber sextortion research in the African region could be attributed to a scarcity of funding, as researchers and institutions depend on government funding as the main source. Lately, their allocations have been clustered across fewer institutions and are based on a competitive allocation system (Angori et al. 2024). This observation indicates a need to increase funding and overall productivity in the numbers and quality of research publications in the African region. The results of this study presented countries where prominent scholars produce their work in this field to highlight the potential for collaboration opportunities for emerging countries (Bhagat et al. 2022).

The investigation of prolific scholars versus their countries and specific areas of interest (themes) in the field of cyber sextortion showed that Australia had more author affiliations, which surpassed the USA even though the latter had the highest number of scientific productions and citation counts. Similarly, UK author affiliations were surpassed by those of Belgium. The sexting theme attracted more interest from authors such as Joris Van Ouytsel, Koen Ponnet, Bianca Klettke, and Michel Walrave. The adolescents topic follows the sexting theme, which has drawn the interest of Joris Van Ouytsel, Koen Ponnet, Bianca Klettke, Michel Walrave, Cassandra Cross, and Jeff Temple. Other themes that attracted interest include cybercrime, online fraud, romance fraud, and online dating. Additionally, themes such as mental health, sextortion, sexual violence, dating violence, and intimate partner violence seem to be drawing scholars' interest. This observation shows that despite the prevailing dearth of empirical knowledge about the sextortion phenomenon (Notté 2024; Wang 2024), there is an increasing scholarly interest in online dating as a path of technology-facilitated sexual violence (Filice et al. 2024). Therefore, these themes have the potential to grow and attract more author interest.

Additionally, this study identified themes such as sexting, adolescents, cybercrime, dating violence, victimization, and sextortion, which are addressed in different countries and regions over time. The results showed that the USA in North America is the leading contributor on themes. Other countries and regions that have been impactful in their contribution to addressing these themes include Australia in the Oceania region, Spain in the southwestern European region, Italy in southwestern Europe, Canada in North America, Belgium in western Europe, and the UK in northern Europe. Interdisciplinary collaboration fosters creativity and innovation and advances academic research by tackling pressing issues in the real world, while individual researchers can find peer support, creative competitiveness, and critical mass, as well as a sense of belonging in their communities provided by discipline-based collaboration (Newman 2024). Furthermore, collaborations between universities, industries, and governments are required to effectively address grand challenges (Rådberg and Löfsten 2024). Therefore, whether emerging researchers seek to establish interdisciplinary or discipline-based collaborations, the knowledge identified in this study could be invaluable in guiding researchers to potential collaborators from

the identified countries and regions to help develop research on cyber sextortion in their countries. In addition, themes that still need attention across different regions were identified, including the Internet, fraud, sexual harassment, sexual violence, online dating, mental health, gender, image-based sexual violence, romance fraud, online fraud, scams, and victims. Addressing the psychological, societal, and systemic issues related to child sexual abuse that occurs online is a complex task that requires an all-encompassing and collaborative approach (Hamdi Bacha 2024). Hence, this finding presents an opportunity to investigate cyber sextortion in relation to these identified themes by fostering collaborative approaches to address research gaps in other countries and regions. These collaborations could focus on empowering adolescents with skills for safety and protection, with digital resilience as one of the essential skills.

As pointed out by many of these studies, many are deficient in resilience and focus on adolescent vulnerabilities and weaknesses, often blaming or stigmatizing them for these situations. It is therefore necessary to move beyond these approaches towards more digitally resilient and autonomy-based research design principles. Sage et al. (2021) note that building digital resilience in adolescents, as well as practicing safe decision-making both online and offline, can help buffer online harm. Resilience is one of the essential predictors that can help to characterize the harm experienced, which can contribute to the development of interventions to facilitate protective factors in adolescents to buffer harms from online attacks such as cyber sextortion (Patchin and Hinduja 2020). Some key considerations that can help foster adolescent digital resilience include self-awareness. It is crucial for any adolescent engaging in cyber communication and usage to know and understand their own strengths, weaknesses, values, and, importantly, emotions that are prone to manipulation. The adolescent youth should foster positive cyber relationships by having a network of family, friends, and peers who can intervene and manage their emotions (Setyawati and Hamka 2022). Importantly, the adolescent should develop skills to navigate challenges, adapt to changing situations, and inculcate coping strategies and ways to deal with online adversity.

These interventions should leverage the building of mentalization abilities in adolescents, which enables one to precisely gauge the motives and intents of others when interacting online (Bucci et al. 2023). Adolescents who are distressed or have regulatory difficulties as a result of online abuse or victimization are at the highest risk of developing difficulties in mentalization and repeated victimization and its harm (Penner et al. 2019). Therefore, resilience-based interventions tailored to proactively address sextortion risk factors are extremely essential to build adolescents' mentalization (Bucci et al. 2023). Research on these interventions can provide insights into the prevalence, tactics, and characteristics of perpetrators and victims. Studying these experiences and the behavior of adolescent youth may form part of victimology studies on cyber sextortion that will inform the design of better intervention programs and better support the empowerment of victims.

There is presently a lack of studies on adolescents' digital resilience and evidence-based interventions to improve mental health and prevent them from falling victim to technology-facilitated sexual abuse and its recurrence (Qi and Yang 2024; Sage et al. 2021). Future studies should thus concentrate on examining adolescents' digital resilience from the viewpoints of sextortion, coercive sexting, dating violence, and mental health. Furthermore, future studies should also focus on the development and evaluation of digital resilience-based interventions.

Research shows that youth can flag low- and medium-risk online interactions, such as flirty comments and sexting, as unsafe, which helps them to build resilience before encountering high-risk behaviors such as increased sexting and the sale or promotion of illegal activities (Alsoubai et al. 2024; Jia et al. 2015; Wisniewski et al. 2015, 2016). Care and

proactive interventions are essential for youth, especially for higher-risk youth who are susceptible to high-risk sexual interactions, self-harm, and delinquencies online that could increase real-world physical and emotional difficulties (Alsoubai et al. 2024). Future studies should therefore concentrate more on identifying the traits of young people and contextual elements that may promote digital resilience and the ability to resist low- and medium-risk behavious while providing proactive and tailored interventions for high-risk individuals (Alsoubai et al. 2024). In this regard, collaborative studies should investigate contextual factors such as participant demographics, which could aid in fostering digital resilience to enable the identification of proactive intervention entry points in the development stages of adolescents.

As previously discussed, themes that have been researched in relation to cyber sextortion so far include sexual violence, dating violence, and intimate partner violence, among others. In addition to romance fraud and coercive sexting, other thematic domains that can be included in the cyber sextortion research include digital forensics, bullying, and cyber dating violence. In addition, Ray and Henry (2024) suggest that there is a need for studies that are focused on both adults and minors (cross-age) to enable synthesizing data on age as a risk demographic. Therefore, scholars could combine the identified topics and employ cross-age strategies to further develop the cyber sextortion research field, especially tailored for adolescent youth. These studies will inform programs for digital literacy, healthy online relationships, resilience and coping skills, counseling, and reporting mechanisms. This study presents a potential for more scientific publications, since the body of literature may not currently be large compared to other bibliometric studies (Bhagat et al. 2022). Thus, researchers in this study recommend increasing research output globally through institutional and author collaborations and a multidisciplinary approach, combining theoretical and empirical knowledge to better understand cyber sextortion nuances (Notté 2024). Encouraging interagency collaboration is crucial for the involvement of institutions such as law enforcement, higher education providers, and social services to foster digital resilience among adolescent youth, ultimately reducing their vulnerability to online exploitation.

6. Conclusions

This study undertook a comprehensive bibliometric analysis of the cyber sextortion research field over the years, applying a bibliometric approach to analyze the data for a comprehensive overview of the trend, thematic focus, and scientific production in the cyber sextortion field. The dataset was retrieved from the Scopus-indexed database only, as the bibliometrix R-package software used in this study does not support the merging of data generated from independent databases (Agbo et al. 2021). Therefore, the authors acknowledge the single-source limitations and potential language biases.

The results identified prolific scholars and research trends and showed a growth trajectory of the field, with possibilities for multidisciplinary research, including thematic domains such as bullying, cybersecurity, and machine learning to advance the cyber sextortion field research. This analysis is useful in providing knowledge to researchers and stakeholders regarding the potential of future research development of thematic areas such as special needs adolescents and child sexual exploitation within the cyber sextortion field.

This study identified themes such as sexting, adolescents, cybercrime, dating violence, victimization, and sextortion that have been addressed in different countries and regions. Other themes that still need focus in the field of cyber sextortion include the Internet, fraud, sexual harassment, sexual violence, online dating, mental health, gender, image-based sexual violence, and romance fraud. Regarding the themes that have been addressed in other countries, this study recommends (1) expanding these themes in different countries and regions to gain insight into the influence of socio-economic factors on cyber sextortion.

(2) Future studies should incorporate themes that still need focus to expand the knowledge base about their influence on cyber sextortion; (3) countries and regions with established research should collaborate with emerging countries in the field, and vice versa. This will enable peer support and creative competitiveness, as well as a sense of belonging in the communities provided by discipline-based collaboration in the field of cyber sextortion; (4) future studies should also conduct cross-age research that includes both adults and adolescents to enable a synthesis of data on age as a risk demographic; and (5) multidisciplinary studies are also encouraged to gain insights into combating cyber sextortion from other disciplines such as cyberbullying, cybersecurity, digital forensics, and machine learning.

Author Contributions: Conceptualization, F.M.R. and K.N.; methodology, F.M.R.; software, F.M.R.; validation, F.M.R. and K.N.; formal analysis, F.M.R.; investigation, F.M.R.; resources, F.M.R.; data curation, F.M.R. and K.N.; writing—original draft preparation, F.M.R.; writing—review and editing, F.M.R. and K.N.; visualization, F.M.R.; supervision, F.M.R.; project administration, F.M.R.; funding acquisition, F.M.R. and K.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

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

References

Agbo, Friday Joseph, Oyelere Sunday Solomon, Suhonen Jarkko, and Tukiainen Markku. 2021. Scientific production and thematic breakthroughs in smart learning environments: A bibliometric analysis. *Smart Learning Environments* 8: 1. [CrossRef]

Almeida, Telma C., and Inês Barreiros. 2024. Online grooming among Portuguese adolescents and the COVID-19 lockdown: Relationship with other types of victimization. *Children and Youth Services Review* 156: 107370. [CrossRef]

Alsoubai, Ashwaq, Afsaneh Razi, Zainab Agha, Shiza Ali, Gianluca Stringhini, Munmun De Choudhury, and Pamela J. Wisniewski. 2024. Profiling the offline and online risk experiences of youth to develop targeted interventions for online safety. *Proceedings of the ACM on Human-Computer Interaction* 8: 1–37. [CrossRef]

Angori, Gabriele, Marzocchi Chiara, Ramaciotti Laura, and Rizzo Ugo. 2024. A patent-based analysis of the evolution of basic, mission-oriented, and applied research in European universities. *The Journal of Technology Transfer* 49: 609–41. [CrossRef]

Aria, Massimo, and Corrado Cuccurullo. 2017. Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics* 11: 959–75. [CrossRef]

Baas, Jeroen, Schotten Michiel, Plume Andrew, Côté Grégoire, and Karimi Reza. 2020. Scopus as a curated, high-quality bibliometric data source for academic research in quantitative science studies. *Quantitative Science Studies* 1: 377–86. [CrossRef]

Bhagat, Priya R., Naz Farheen, and Magda Robert. 2022. Artificial intelligence solutions enabling sustainable agriculture: A bibliometric analysis. *PLoS ONE* 17: e0268989. [CrossRef]

Bornmann, Lutz, and Rüdiger Mutz. 2015. Growth rates of modern science: A bibliometric analysis based on the number of publications and cited references. *Journal of the Association for Information Science and Technology* 66: 2215–22. [CrossRef]

Bucci, Sandra, Filippo Varese, Ethel Quayle, Kim Cartwright, Matthew Machin, Pauline Whelan, Prathiba Chitsabesan, Cathy Richards, Victoria Green, John Norrie, and et al. 2023. A Digital Intervention to Improve Mental Health and Interpersonal Resilience in Young people who have experienced technology-assisted sexual abuse: Protocol for a Nonrandomized Feasibility Clinical Trial and Nested qualitative study. *Journal of Medical Internet Research on Research Protocols* 12: e40539. [CrossRef]

Buchanan, Tom, and Monica T. Whitty. 2014. The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime and Law* 20: 261–83. [CrossRef]

Caarten, Ashleigh Bicker, Loes van Heugten, and Merkle Ortrun. 2022. The intersection of corruption and gender-based violence: Examining the gendered experiences of sextortion during migration to South Africa. *African Journal of Reproductive Health* 6: 45–54.

Carlton, Alessandra. 2019. Sextortion: The Hybrid Cyber-Sex Crime. *North Carolina Journal of Law and Technology* 21: 177.

Champion, Amanda R., Flora Oswald, Devinder Khera, and Cory L. Pedersen. 2022. Examining the gendered impacts of technology-facilitated sexual violence: A mixed methods approach. *Archives of Sexual Behavior* 51: 1607–24. [CrossRef]

Choi, HyeJeong, Joris Van Ouytsel, and Jeff R. Temple. 2016. Association between sexting and sexual coercion among female adolescents. *Journal of Adolescence* 53: 164–68. [CrossRef]

Couch, Danielle, Pranee Liamputtong, and Marian Pitts. 2012. What are the real and perceived risks and dangers of online dating? Perspectives from online daters: Health risks in the media. *Health, Risk and Society* 14: 697–714. [CrossRef]

Cross, Cassandra. 2015. No laughing matter: Blaming the victim of online fraud. *International Review of Victimology* 21: 187–204. [CrossRef]

Cross, Cassandra, and Dom Blackshaw. 2015. Improving the police response to online fraud. *Policing: A Journal of Policy and Practice* 9: 119–28. [CrossRef]

Cross, Cassandra, Dragiewicz Molly, and Richards Kelly. 2018. Understanding romance fraud: Insights from domestic violence research. *The British Journal of Criminology* 58: 1303–22. [CrossRef]

Cross, Cassandra, Karen Holt, and Thomas J. Holt. 2023. To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud. *Criminology and Criminal Justice*. [CrossRef]

Drouin, Michelle, Jody Ross, and Elizabeth Tobin. 2015. Sexting: A new, digital vehicle for intimate partner aggression? *Computers in Human Behavior* 50: 197–204. [CrossRef]

Edwards, Matthew, and Nick M. Hollely. 2023. Online sextortion: Characteristics of offences from a decade of community reporting. *Journal of Economic Criminology* 2: 100038. [CrossRef]

Esfahani, Hossein J., Keyvan Tavasoli, and Armin Jabbarzadeh. 2019. Big data and social media: A scientometrics analysis. *International Journal of Data and Network Science* 3: 145–64. [CrossRef]

Fair, Jo E., Melissa Tully, Brian Ekdale, and Rabiu K. Asante. 2009. Crafting lifestyles in urban Africa: Young Ghanaians in the world of online friendship. *Africa Today* 55: 28–49. [CrossRef]

Fakunmoju, Sunday B., Tina Abrefa-Gyan, Ntandoyenkosi Maphosa, and Priscilla Gutura. 2021. Rape myth acceptance: Gender and cross-national comparisons across the United States, South Africa, Ghana, and Nigeria. *Sexuality & Culture* 25: 18–38. [CrossRef]

Filice, Eric, Amy Matharu, Diana C. Parry, and Corey W. Johnson. 2024. A Thousand Catcalls: Survivors' Experiences of Sexual Violence in Online Dating. *Leisure Sciences*, 1–19. [CrossRef]

Foster, Ally. 2023. Australian Teenagers Targeted by Sick Sextortion Scams. News.com.au. Available online: https://www.news.com.au/technology/online/security/australian-teenagers-targeted-by-sick-sextortion-scams/news-story/ae6975b8308917f611b03fa99bd2b0d9 (accessed on 9 October 2024).

Gassó, Aina M., Bianca Klettke, José R. Agustina, and Irene Montiel. 2019. Sexting, mental health, and victimization among adolescents: A literature review. *International Journal of Environmental Research and Public Health* 16: 2364. [CrossRef]

Gámez-Guadix, Manuel, Estibaliz Mateos-Pérez, Sebastian Wachs, Michelle Wright, Jone Martínez, and Daniel Íncera. 2022. Assessing image-based sexual abuse: Measurement, prevalence, and temporal stability of sextortion and nonconsensual sexting ("revenge porn") among adolescents. *Journal of Adolescence* 94: 789–99. [CrossRef]

Gámez-Guadix, Manuel, Patricia Santisteban, and Santiago Resett. 2017. Sexting among Spanish adolescents: Prevalence and personality profiles. *Psicothema* 29: 29–34. [CrossRef]

Grant, Jonathan, Robert Cottrell, Françoise Cluzeau, and Gail Fawcett. 2000. Evaluating "payback" on biomedical research from papers cited in clinical guidelines: Applied bibliometric study. *British Medical Journal* 320: 1107–11. [CrossRef]

Hagglund, Kirstin, and Franaaz Khan. 2023. The Gendered Impact of Corruption: Women as Victims of Sextortion in South Africa. *Journal of Anti-Corruption Law* 7: 1. [CrossRef]

Hamdi Bacha, Yasmine. 2024. Online Child Sexual Abuse: Exploring Psychological and Social Impacts, Prevention, and Intervention Strategies. *Journal of Studies in Deviation Psychology* 9: 903–15.

Hasumi, Toshiyuki, and Mei-Shiu Chiu. 2024. Technology-enhanced language learning in English language education: Performance analysis, core publications, and emerging trends. *Cogent Education* 11: 2346044. [CrossRef]

Henry, Nicola, and Anastasia Powell. 2018. Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, and Abuse* 19: 195–208. [CrossRef]

Henry, Nicola, Nicola Gavey, and Kelly Johnson. 2023. Image-based sexual abuse as a means of coercive control: Victim-survivor experiences. *Violence Against Women* 29: 1206–26. [CrossRef]

Hlongwane, Peter. 2017. Sextortion in South African public sector institutions. *Sabinet African Journals* 25: 7–25.

Hong, Suyeon, Nancy Lu, Doreen Wu, David E. Jimenez, and Ruth L. Milanaik. 2020. Digital sextortion: Internet predators and pediatric interventions. *Current Opinion in Pediatrics* 32: 192–97. [CrossRef]

Humphreys, Krystal, Brian Le Clair, and Janet Hicks. 2019. Intersections between pornography and human trafficking: Training ideas and implications. *Journal of Counselor Practice* 10: 19–39.

Jia, Haiyan, Pamela J. Wisniewski, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. Risk-taking as a learning process for shaping teen's online information privacy behaviors. Paper presented at the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, Vancouver, BC, Canada, March 14–18.

Kavishe, Angela. 2024. The contribution of digital technology in exacerbating gender-based violence against female students in higher learning institutions in Tanzania. *African Journal of Social Issues* 7: 756–69. [CrossRef]

Kernsmith, Poco D., Bryan G. Victor, and Joanne P. Smith-Darden. 2018. Online, offline, and over the line: Coercive sexting among adolescent dating partners. *Youth and Society* 50: 891–904. [CrossRef]

Kibe, Lucy, Tom Kwanya, Angella Kogos, Erick Ogolla, and Claudior Onsare. 2022. Types of Cyberbullying Experienced on Facebook by Undergraduate Students in Kenyan Universities. *Journal of Cyberspace Studies* 6: 149–82. [CrossRef]

Klettke, Bianca, David J. Hallford, Elizabeth Clancy, David J. Mellor, and John W. Toumbourou. 2019. Sexting and psychological distress: The role of unwanted and coerced sexts. Cyberpsychology. *Behavior, and Social Networking* 22: 237–42. [CrossRef] [PubMed]

Larsen, Peder, and Markus von Ins. 2009. The steady growth of scientific publication and the declining coverage provided by science citation index. Paper presented at the 12th International Conference on Scientometrics and Informetrics, Rio de Janeiro, Brazil, July 14–17.

Lastdrager, Elmer. 2014. Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science* 3: 9. [CrossRef]

Liggett, Roberta. 2019. Exploring Online Sextortion. *Family and Intimate Partner Violence Quarterly* 11: 45.

Mainwaring, Chelsea, Adrian J. Scott, and Fiona Gabbert. 2024. Facilitators and barriers of bystander intervention intent in image-based sexual abuse contexts: A focus group study with a university sample. *Journal of Interpersonal Violence* 39: 2655–86. [CrossRef]

Mazanderani, Fadhila. 2012. An ethics of intimacy: Online dating, viral-sociality and living with HIV. *BioSocieties* 7: 393–409. [CrossRef]

McGlynn, Clare, Erika Rackley, and Ruth Houghton. 2017. Beyond 'revenge porn': The continuum of image-based sexual abuse. *Feminist Legal Studies* 25: 25–46. [CrossRef]

Mondal, Himel, Manas R. Sahoo, and Shaikat Mondal. 2022. Characteristics of Cyber Sextortion in India: Content Analysis of Online Newspapers Published in 2019–2021. *Journal of Psychosexual Health* 4: 171–77. [CrossRef]

Morelli, Mara, Dora Bianchi, Roberto Baiocco, Lina Pezzuti, and Antonio Chirumbolo. 2016. Not-allowed sharing of sexts and dating violence from the perpetrator's perspective: The moderation role of sexism. *Computers in Human Behavior* 56: 163–69. [CrossRef]

Mori, Camille, Jessica E. Cooke, Jeff R. Temple, Anh Ly, Yu Lu, Nina Anderson, Christina Rash, and Sheri Madigan. 2020. The Prevalence of Sexting behaviours Among Emerging Adults: A Meta-Analysis. *Archives of Sexual Behavior* 49: 1103–19. [CrossRef]

Muslimin, J., Shubhan Shodiq, and Thamer Hamdi M. Almutairi. 2024. Sextortion, Gender, and Digital Crime: A Socio-Legal Comparison between Positive and Islamic Law. *AL-IHKAM: Journal Hukum and Pranata Sosial* 19: 53–77. [CrossRef]

Newman, Joshua. 2024. Promoting interdisciplinary research collaboration: A Systematic Review, a critical literature Review, and a pathway forward. *Social Epistemology* 38: 135–51. [CrossRef]

Notté, Raoul J. 2024. Exploring the impact of sextortion on adult males: A narrative approach. *Technology in Society* 78: 102617. [CrossRef]

O'Malley, Roberta L., and Karen M. Holt. 2022. Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. *Journal of Interpersonal Violence* 37: 258–83. [CrossRef]

Patchin, Justin W., and Sameer Hinduja. 2020. Sextortion among adolescents: Results from a national survey of US youth. *Sexual Abuse* 32: 30–54. [CrossRef] [PubMed]

Penner, Francesca, Malgorzata Gambin, and Carla Sharp. 2019. Childhood maltreatment and identity diffusion among inpatient adolescents: The role of reflective function. *Journal of Adolescence* 76: 65–74. [CrossRef] [PubMed]

Pethers, Brent, and Abubakar Bello. 2023. Role of Attention and Design Cues for Influencing Cyber-Sextortion Using Social Engineering and Phishing Attacks. *Future Internet* 15: 29. [CrossRef]

Power, Veronica, and Abubakar Bello. 2022. Individual differences in cyber security behavior using personality-based models to predict susceptibility to sextortion attacks. In *Cybersecurity and Cognitive Science*. Cambridge: Academic Press, pp. 89–113. [CrossRef]

Prell, Christina, Klaus Hubacek, and Mark Reed. 2009. Stakeholder analysis and social network analysis in natural resource management. *Society and Natural Resources* 22: 501–18. [CrossRef]

Qi, Chunlin, and Nanchang Yang. 2024. Digital resilience in Chinese adolescents: A portrayal of the current condition, influencing factors, and improvement strategies. *Frontiers in Psychiatry* 15: 1278321. [CrossRef] [PubMed]

Ray, Alana, and Nicola Henry. 2024. Sextortion: A Scoping Review. *Trauma, Violence, and Abuse* 26: 138–55. [CrossRef]

Rådberg, Kamilla K., and Hans Löfsten. 2024. The entrepreneurial university and development of large-scale research infrastructure: Exploring the emerging university function of collaboration and leadership. *The Journal of Technology Transfer* 49: 334–66. [CrossRef]

Ross, Jody M., Drouin Michelle, and Coupe Amanda. 2019. Sexting coercion as a component of intimate partner polyvictimization. *Journal of Interpersonal Violence* 34: 2269–91. [CrossRef] [PubMed]

Sage, Melanie, Karen Randolph, Dale Fitch, and Toddy Sage. 2021. Internet use and resilience in adolescents: A systematic review. *Research on Social Work Practice* 31: 171–79. [CrossRef]

Schoeps, Konstanze, Montserrat Peris-Hernández, Maite Garaigordobil, and Inmaculada Montoya-Castilla. 2020. Risk factors for being a victim of online grooming in adolescents. *Psicothema* 32: 15–23. [CrossRef]

Setyawati, Lia M., and Muhammad Hamka. 2022. Digital resilience: Opportunities and threats for adolescents in A virtual world. *Acta Informatica Malaysia (AIM)* 2: 67–71. [CrossRef]

Singh, Vivek K., Prashasti Singh, Mousumi Karmakar, Jacqueline Leta, and Philipp Mayr. 2021. The journal coverage of Web of Science, Scopus and Dimensions: A comparative analysis. *Scientometrics* 126: 5113–42. [CrossRef]

Song, Yu, Xieling Chen, Hao Tianyong, Zhinan Liu, and Lan Zixin. 2019. Exploring two decades of research on classroom dialogue by using bibliometric analysis. *Computers in Education* 137: 12–31. [CrossRef]

Sorell, Tom, and Monica T. Whitty. 2019. Online romance scams and victimhood. *Security Journal* 32: 342–61. [CrossRef]

Tasbiha, Naila S. 2024. Qualitatively Examining and Analyzing Social Learning Theory in an Online Arena with a Focus on Sexting. *European Journal of Humanities and Social Sciences* 4: 9–14. [CrossRef]

Tettey, Wisdom J. 2008. Globalization and Internet Fraud in Ghana: Interrogating the Political Economy of Survival, Subaltern Agency, and their Ramifications. In *Neoliberalism and Globalization in Africa: Contestations from the Embattled Continent*. Edited by Joseph Mensah. New York: Palgrave Macmillan, pp. 241–66. [CrossRef]

Thompson, Olasupo, Olugbenga S. Aina, Ridwan Tosho Idris, Emmanuel O. Ademola, BaseerahAbisola Akinreti-Raji, Phoebe Dooshima Awange, and Surajudeen O. Oladele. 2024. Are you gonna cooperate with me or i release your nude': Sextortion, responses and implications for national development in Nigeria? *Ochendo: An African Journal of Innovative Studies* 5: 8–26.

Thorn. 2017. Sextortion Summary Findings from a 2017 Survey of 2097 Survivors (No. 121919). Available online: https://www.thorn.org/wp-content/uploads/2019/12/Sextortion_Wave2Report_121919.pdf (accessed on 12 August 2024).

Van Ouytsel, Joris, Ellen van Gool, Michel Walrave, Koen Ponnet, and Emilie Peeters. 2017. Sexting: Adolescents' perceptions of the applications used for, motives for, and consequences of sexting. *Journal of Youth Studies* 20: 446–70. [CrossRef]

Vitis, Laura. 2020. Private, hidden and obscured: Image-based sexual abuse in Singapore. *Asian Journal of Criminology* 15: 25–43. [CrossRef]

Waheed, Hajra, Saeed-UI Hassan, Naif R. Aljohani, and Muhammad Wasif. 2018. Bibliometric perspective of learning analytics research landscape. *Behavior and Information Technology* 37: 941–57. [CrossRef]

Wang, Fangzhou. 2024. Breaking the silence: Examining process of cyber sextortion and victims' coping strategies. *International Review of Victimology* 31: 02697580241234331. [CrossRef]

Wang, Fangzhou, and Volkan Topalli. 2024. Understanding romance scammers through the lens of their victims: Qualitative modeling of risk and protective factors in the online context. *American Journal of Criminal Justice* 49: 145–81. [CrossRef]

Whitty, Monica T. 2013. The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology* 53: 665–84. [CrossRef]

Whitty, Monica T. 2015. Anatomy of the online dating romance scam. *Security Journal* 28: 443–55. [CrossRef]

Whitty, Monica T. 2018. Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior, and Social Networking* 21: 105–9. [CrossRef] [PubMed]

Whitty, Monica T., and Tom Buchanan. 2012. The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking* 15: 181–83. [CrossRef] [PubMed]

Whitty, Monica T., and Tom Buchanan. 2016. The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology and Criminal Justice* 16: 176–94. [CrossRef]

Wisniewski, Pamela, Haiyan Jia, Na Wang, Saijing Zheng, Heng Xu, Mary Beth Rosson, and John M. Carroll. 2015. Resilience mitigates the negative effects of adolescent internet addiction and online risk exposure. Paper presented at the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea, April 18–23.

Wisniewski, Pamela, Heng Xu, Mary Beth Rosson, Daniel F. Perkins, and John M. Carroll. 2016. Dear Diary: Teens Reflect on Their Weekly Online Risk Experiences. Paper presented at the CHI '16 Conference on Human Factors in Computing Systems, San Jose, CA, USA, May 7–12.

Wittes, Benjamin, Cody Poplin, Quinta Jurecic, and Clara Spera. 2016. Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault. Centre for Technology Innovation at Brookings. pp. 1–47. Available online: https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf (accessed on 12 August 2024).

Wolak, Janis, David Finkelhor, Wendy Walsh, and Leah Treitman. 2018. Sextortion of minors: Characteristics and dynamics. *Journal of Adolescent Health* 62: 72–79. [CrossRef]

Zeyzus Johns, Bree A., Allison R. Casola, Olivia Rea, Neil Skolnik, and Susan K. Fidler. 2024. Safe-Guarding Youth from Online Sexual Exploitation in the Digital Era: A Role for Primary Care. *American Journal of Lifestyle Medicine*, *online ahead of print*. [CrossRef]