forensic sciences

MDPI

Systematic Review

A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature

Melissa Martineau [1,*], Elena Spiridon [2] and Mary Aiken [1]

[1] Cyberpsychology Department, Capitol Technology University, Laurel, MD 20708, USA; mpaiken@captechu.edu
[2] Department of Psychology, Edge Hill University, Ormskirk L39 4QP, UK; spiridoe@edgehill.ac.uk
* Correspondence: mmartineau@captechu.edu

Abstract: Cybercrime presents a significant threat to global society. With the number of cybercrimes increasing year after year and the financial losses escalating, law enforcement must advance its capacity to identify cybercriminals, collect probative evidence, and bring cybercriminals before the courts. Arguably to date, the approach to combatting cybercrime has been technologically centric (e.g., anti-virus, anti-spyware). Cybercrimes, however, are the result of human activities based on human motives. It is, therefore, important that any comprehensive law enforcement strategy for combatting cybercrime includes a deeper understanding of the hackers that sit behind the keyboards. The purpose of this systematic review was to examine the state of the literature relating to the application of a human-centric investigative tool (i.e., profiling) to cybercrime by conducting a qualitative meta-synthesis. Adhering to the PRISMA 2020 guidelines, this systematic review focuses specifically on cybercrime where a computer is the target (e.g., hacking, DDoS, distribution of malware). Using a comprehensive search strategy, this review used the following search terms: "cybercrime", "computer crime", "internet crime", "cybercriminal", "hacker", "black hat", "profiling", "criminal profiling", "psychological profiling", "offender profiling", "criminal investigative analysis", "behavioral profiling", "behavioral analysis", "personality profiling", "investigative psychology", and "behavioral evidence analysis" in all combinations to identify the relevant literature in the ACM Digital Library, EBSCOhost databases, IEEE Xplore, ProQuest, Scopus, PsychInfo, and Google Scholar. After applying the inclusion/exclusion criteria, a total of 72 articles were included in the review. This article utilizes a systematic review of the current literature on cyber profiling as a foundation for the development of a comprehensive framework for applying profiling techniques to cybercrime—described as cyber behavioral analysis (CBA). Despite decades of research, our understanding of cybercriminals remains limited. A lack of dedicated researchers, the paucity of research regarding human behavior mediated by technology, and limited access to datasets have hindered progress. The aim of this article was to advance the knowledge base in cyber behavioral sciences, and in doing so, inform future empirical research relating to the traits and characteristics of cybercriminals along with the application of profiling techniques and methodologies to cybercrime.

Keywords: analytical framework; criminal investigative analysis; cyber behavioral analysis; cybercrime; hacker typologies; dark web; ethical hacker; law enforcement; profiling

Citation: Martineau, M.; Spiridon, E.; Aiken, M. A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. *Forensic Sci.* **2023**, *3*, 452–477. https://doi.org/10.3390/forensicsci3030032

Academic Editor: Bruce Royston McCord

Received: 4 July 2023
Revised: 15 July 2023
Accepted: 19 July 2023
Published: 22 July 2023

1. Introduction

The internet has become a space for the proliferation of criminal activity where protective guardianship is lacking [1]. Cyberspace, and more specifically the Dark web, has become a productive domain for malicious threat actors, from hackers to organized cybercriminals, as perpetrators who use their knowledge of computer systems for personal profit or to wreak havoc [2,3]. While the cybersecurity industry has an important role to play in preventing cybercrime through target hardening (e.g., anti-virus, anti-spyware), the legal response to cybercrime falls to law enforcement agencies [4].

It is evident that cyberspace is a frontier that poses a wide range of security and law enforcement challenges. In 2021, one in ten businesses in Canada were impacted by ransomware yet only 10% of these businesses reported the crime to law enforcement [5]. In their Cyber Threat Assessment 2023–2024, the Canadian Centre for Cyber Security (CCCS) assessed that cybercrime poses a sophisticated threat to Canada [6]. In May of 2021, the White House issued an "Executive Order on Improving the Nation's Cybersecurity" [7]. The Federal Bureau of Investigation [8] received 2.76 million complaints of cybercrime from 2017 to 2021, with the number of complaints increasing year to year. The global cost of cybercrime in 2021 was estimated at USD 6 trillion [8]. Cybersecurity researchers estimate that this amount will increase to USD 10.5 trillion by 2025 [9]. A multi-faceted law enforcement strategy is imperative in order to disrupt cybercriminals, and in doing so, curb the rate of cyber victimization. However, the development of law enforcement strategies to address cybercrime has lagged behind advancements made in the cybercriminal underground.

In general, the law enforcement approach to cybercrime to date has been technologically centric [10]. Much effort has been expended to develop effective digital forensic tools and protocols and to train law enforcement personnel in their use [11]. The National Institute of Standards and Technology defines digital forensics as "the process used to acquire, preserve, analyze and report on evidence using scientific methods that are demonstrably reliable, accurate and repeatable such that it may be used in judicial proceedings" ([12], p. 24). While establishing probative digital evidence is imperative to any cybercrime investigation, cybercrimes, like their traditional counterparts, are the result of human activities based on human motives. Notably, socially engineered attacks constitute 98% of all phishing and data breach cybercrimes. Therefore, the attack vector should arguably be considered primarily psychological as opposed to purely technological [13]. According to Turvey ([14], p. 286), "historically, no matter what objective a technology is designed to achieve, and no matter what intentions or beliefs impel its initial development, technology is still subordinate to the motives and morality of those who employ it". It is, therefore, important that any comprehensive law enforcement strategy for combatting cybercrime includes a deeper understanding of the individuals perpetrating the crimes and their motivations. Academia, industry, and private cybersecurity companies have devoted some attention to understanding these individuals by means of, for example, hacker typologies. By and large, however, the efforts of these groups have been to understand attack vectors and technical vulnerabilities in order to develop target hardening activities. Recently, however, there has been recognition among cybersecurity specialists of the importance of profiling not only the technical threat but also the threat actor [15]. Arguably, the law enforcement response to cybercrime should similarly involve a human-centric psychological component (i.e., cyber behavioral analysis) as well as a digital forensic and computer science component. The application of behavioral analysis to cybercrime, however, is still in the early-stage development.

1.1. Prior Systematic Reviews

A search of Prospero did not yield any systematic reviews related to the application of behavioral analysis to cybercrime. During database searches to scope the literature, two systematic reviews relating to the criminal profiling of traditional crime were identified and one systematic review relating to the profiling of cybercrime was located.

Dowden et al. [16] and Fox and Farrington [17] each presented a systematic review of the literature relating to criminal profiling. Dowden et al. [16] indicated that after three decades of criminal profiling application and research, little to no effort has been made to synthesize the state of the literature in this field. The aim of their study was to assess whether profiling practice is based on an adequate foundation of empirical research. Dowden et al. [16] developed a coding manual and method of classifying the articles included in their review. Based on 132 studies, the authors concluded that "the methodological sophistication of research in the area is sorely lacking" ([16], p. 50). There were few journals presenting more than three works on the topic, and very few authors appeared to specialize

in this field. Many of the works were literature reviews or discussion pieces that were not based on primary data. The authors [16] recommended that future research should focus on establishing a theoretical foundation for profiling practices and developing empirical studies to test the proposed theories. Fox and Farrington [17] extended the work of Dowden et al. [16] to include an additional decade of criminal profiling research. Fox and Farrington [17] found that there had been improvement in the scientific rigor of research in this field. Despite this improvement, there remained a dearth of evaluation research determining how profiling performs in actual investigations. Notably, in the context of this present research, the authors recommended that profiles should be developed using an empirically informed and systematic process.

The only systematic review that specifically addressed the application of criminal profiling to cybercrime was the work of Bada and Nurse [18]. The researchers [18] argued that applying the same profiling techniques used in interpersonal violent crime to cybercrime offered law enforcement another investigative tool when responding to cybercrime. In their systematic review, the authors adopted an inclusive definition of cybercrime, including articles on cybercrime where the computer was the target and where it was the instrument (e.g., cyber bullying, child exploitation, etc.). They concluded that much of the existing literature comprised case studies, with few studies based on primary data. In addition, the field suffered from a lack of common taxonomy and data. The authors indicated that a limitation of their review was the exclusive use of academic literature. They recommended that future reviews include non-academic sources [18].

1.2. Aim of the Review

The purpose of this systematic review was to examine the state of the literature relating to the application of profiling to cybercrime by conducting a qualitative meta-synthesis. Specifically, this entailed a content analysis of both published and unpublished literature exploring the fields in which research is currently being conducted, along with consideration of the approaches to profiling that are being applied to cybercrime. The focus of this systematic review was on cybercrime where a computer is the target (e.g., hacking, denial of service attacks, ransomware), also known as cyber-dependent or "crimes against the machine" ([19], p. 2), and the study of behavioral analysis as applied to the human perpetrator. The decision to focus on cybercrime where the computer is the target was made because these crimes are significantly different from the crimes for which profiling has traditionally been applied. This research differs from previous systematic reviews in that it focuses specifically on cybercrime where the computer is the target, thus recognizing the heterogeneity of cybercrime. In addition, this review incorporated research from both social and computer science as well as published and unpublished works to allow for a more comprehensive exploration of the literature relating to cyber profiling. Grounded in the theories that generally underpin profiling and the existing approaches to profiling, this review provides the foundation for the development of a new comprehensive framework for applying profiling techniques to cybercrime—cyber behavioral analysis (CBA)—presented at the end of this paper. This systematic review, therefore, provides a robust foundation for future empirical research relating to the traits and characteristics of cybercriminals and the application of profiling to cybercrime.

2. Materials and Methods

2.1. Eligibility Criteria

This work adheres to the PRISMA 2020 guidelines for reporting systematic reviews [20]. The selection of articles for the review was based on established inclusion criteria. The first criterion required articles to be published in English. This criterion was selected based on the language spoken by the authors as well as being the language of publication of the majority of journals pertaining to this field. The second criterion sought to elicit articles that pertained to the study of cybercrime where a computer was the target, i.e., hacking. For inclusion in the review, articles also had to address the application of behavioral analysis

(also known as criminal profiling) or hacker characteristics or motivations (which inform the development of a profile [21]). Articles relating to cybercrime where the computer was the instrument, described as "crimes in the machine" [19] (e.g., cyberstalking or cyberbullying), were not included in the review, nor were articles related to the analysis of the behavior of malware.

2.2. Information Sources

An inclusive approach was adopted in this review. The inclusion of law enforcement reports and grey literature was deemed particularly important given the rapidly evolving nature of cybercrime. The inclusion of grey literature also helped to avoid publication bias. Peer-reviewed journal articles, unpublished manuscripts, conference papers, books, book chapters, unpublished doctoral dissertations, magazine articles (including web magazines), and private industry reports published prior to 2023 were included. The literature was identified through an electronic search of psychological, criminological, and information systems/cybersecurity databases, including the ACM Digital Library, EBSCOhost databases, IEEE Xplore, ProQuest, Scopus, and PsychInfo. To ensure the inclusion of grey literature, queries were also conducted in Google, Google Scholar, and Research Gate. The searches were conducted in April 2023.

2.3. Search Strategy

The search queries were carried out using keywords associated with the research topic and appropriate variations: "cybercrime", "computer crime", "internet crime", "cybercriminal", "hacker", and "black hat". Also, to elicit the literature on cyber profiling, several terms were used, including: "profiling" "criminal profiling", "psychological profiling", "offender profiling", "criminal investigative analysis", "behavioral profiling", "behavioral analysis", "personality profiling", "investigative psychology", and "behavioral evidence analysis". Combining all search terms into one complex query was problematic for many databases queried for this review. Therefore, the search terms were broken down into 51 query combinations. The 51 search combinations were entered into each database and the query results amalgamated by database.

2.4. Selection Process

The selection of articles was accomplished using an iterative process of applying the inclusion criteria. Initially, the article titles were reviewed, followed by a review of the article abstracts. The full texts of all articles appearing to meet the inclusion criteria were obtained after the initial title and abstract reviews were performed. The full text of each article was reviewed, and the inclusion criteria applied. Attention was also given to the reference list of each included article in order to identify additional articles that were appropriate for inclusion. To maintain a rigorous systematic process, 25% of the articles included based on the article abstract and 25% of those included based on the full text were reviewed by an independent reviewer. The final article inclusion was based on consensus between reviewers.

2.5. Data Collection Process

Data collection was informed by previous systematic reviews relating to criminal profiling [14–16] in order to enable a comparison of the findings. The data collected were also determined by the aim of this review—to establish the foundation for a comprehensive framework for cyber behavioral analysis. A data extraction spreadsheet was used to guide the retrieval of relevant data from the selected articles. The data collection protocol included both high-level descriptive data for each included article, as well as more in-depth information regarding the study's purpose and how the study contributed to a deeper understanding of cybercriminals and informed cybercriminal profiling. Table 1 provides a list and description of the collected data.

Table 1. Description of data collected.

	Item	Description
Descriptive	Year of Publication	The year in which the item was published or submitted
	Publication Type	Book, book chapter, journal article, magazine article, dissertation, trade report, conference paper, LE bulletin
	Authors	Authors
	Discipline	Criminologist, psychologist, sociologist, law enforcement, computer science, multi-disciplinary
	Country	Country of authors
	Peer review status	Peer reviewed or non-peer reviewed
	Study Type	Qualitative or quantitative
	Emphasis	Case study, comparison study, discussion piece, evaluation, literature review, primary empirical, theoretical
	Sample size	Number of participants in research
	Sampling technique	Sampling technique employed in research
	Method	Method used for data collection
	Use of statistics	No statistics, descriptive statistics or inferential statistics
	Number of citations	Number of citations according to Google Scholar
In-Depth	Profiling Approach	Inductive, deductive, mixed, none
	Variables	List of the variables included in analysis
	Study Results	Summary of the study results
	Theoretical frameworks	List of any theoretical frameworks identified as informing the study
	Bias evaluation	Identification of any sources of bias

One reviewer collected data from 72 articles and a second reviewer corroborated the information from a sample consisting of 25% of the 72 papers. The data collected were analyzed using both quantitative and qualitative content analysis. Descriptive data were analyzed using formulas for descriptive statistics (e.g., frequencies) in Excel. A meta-synthesis was undertaken using thematic analysis [22]. The thematic analysis was conducted manually.

3. Results

3.1. Study Selection (Flow of Studies)

The database queries resulted in the identification of 8020 articles. The deduplication process reduced the selected set to 5686 unique articles. All 5686 article titles were reviewed and any article that was clearly not related to the review was excluded; this included 22 articles that failed to meet the first inclusion criterion (i.e., publication in English). Following a review of the article titles, a total of 194 articles remained. The abstracts of these 194 articles were reviewed by a single reviewer based on the second inclusion criterion (i.e., related to the understanding of cybercrime target offenders and/or cyber profiling). The number of included articles was reduced to 82. The final iteration of the selection process involved a full text review of the 82 articles. The full text review resulted in the identification of 41 articles for inclusion in the review.

A second independent reviewer scrutinized 25% of the 194 articles identified following the title review and 82 articles following the review of the abstracts, with attention placed on their titles, abstracts, and keywords, and subsequently on the full text of the article and the sources of information used in the article (i.e., list of references). An inter-rater reliability assessment was performed to reduce the research bias. A kappa analysis was conducted to determine the agreement between the reviewers [23]. The levels of agreement based on the abstract and full text reviews were 0.64 and 0.56, respectively. This was considered a moderate level of agreement [23]. Agreement between the two reviewers was discussed

at the end of the independent reviews, and consensus was reached. The references of the 41 included articles were reviewed during the data collection process. This resulted in the identification and review of an additional 31 articles. The systematic review was therefore based on 72 articles. Figure 1 presents a PRISMA flow diagram, providing details related to the search strategy and article inclusion and exclusion [20].

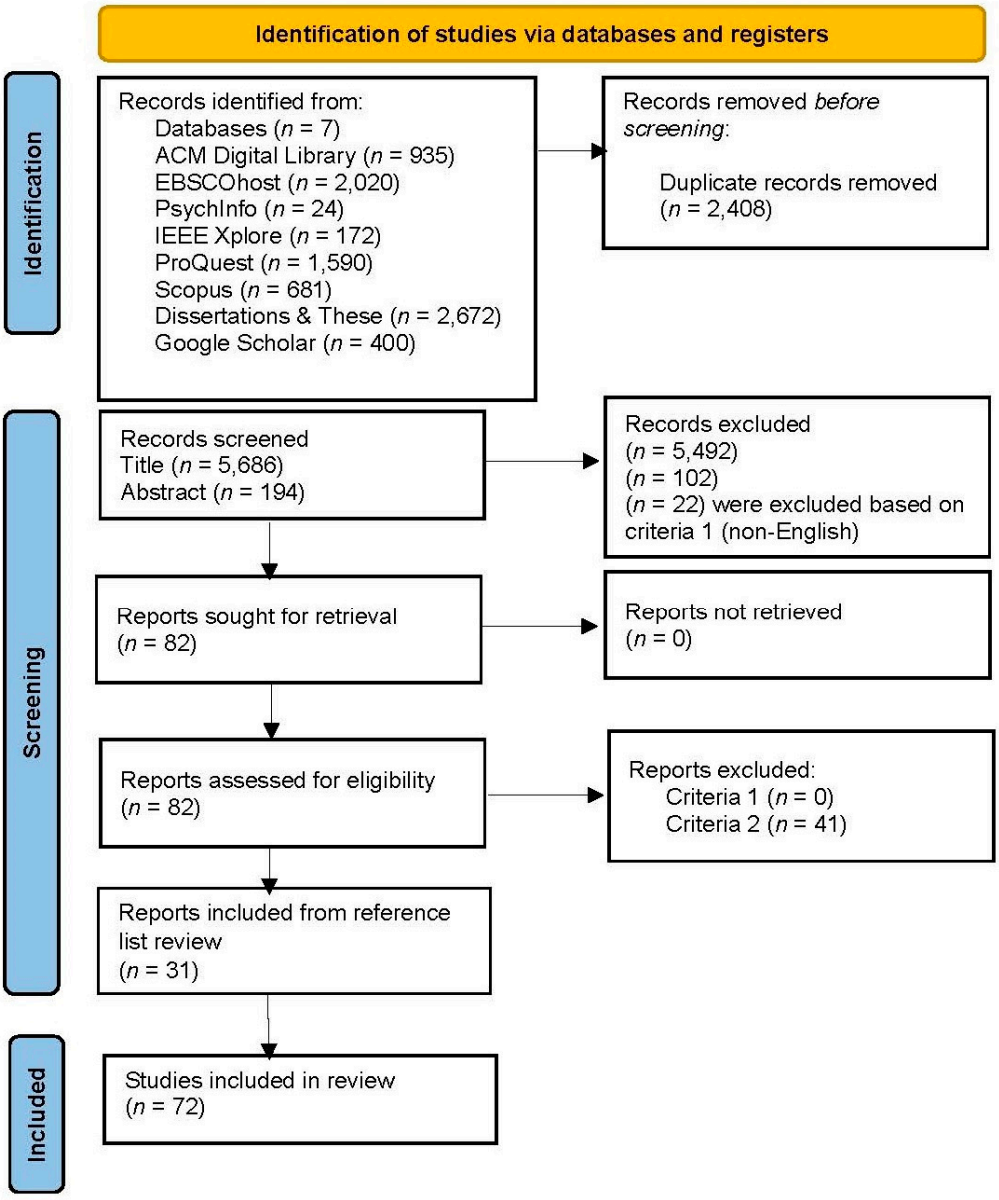

Figure 1. PRISMA flow diagram of the systematic review.

Among the 72 works were 3 books, 3 book chapters, 11 conference papers, 12 dissertations, 3 industry reports, 32 peer-reviewed journal articles, 1 law enforcement bulletin, and 7 magazine articles. The date range for all included works was from 1981 to 2022. The distribution of publication dates, as illustrated in Figure 2, indicated that the topic of understanding cybercriminals has been of steady interest since the early 1980s. The proliferation of cybercrime in the past decade coincided with renewed research interest, with 46 articles published since 2010.

The 72 works were authored by 129 authors emanating from various disciplines, including sociology, psychology, criminology, law enforcement, and computer science. Given the exclusion of works that focused exclusively on the technical elements of cybercrime, it

was somewhat surprising that computer scientists or other IT specialists wrote 32 (44%) of the 72 works. Researchers emanating from the social sciences (i.e., psychology, criminology, and sociology) authored only 16 (22.2%) of the articles included in the review. While law enforcement officers [11] and FBI agents [24,25] authored earlier works in the field of cyber profiling, their presence was noticeably absent in works from the past decade.

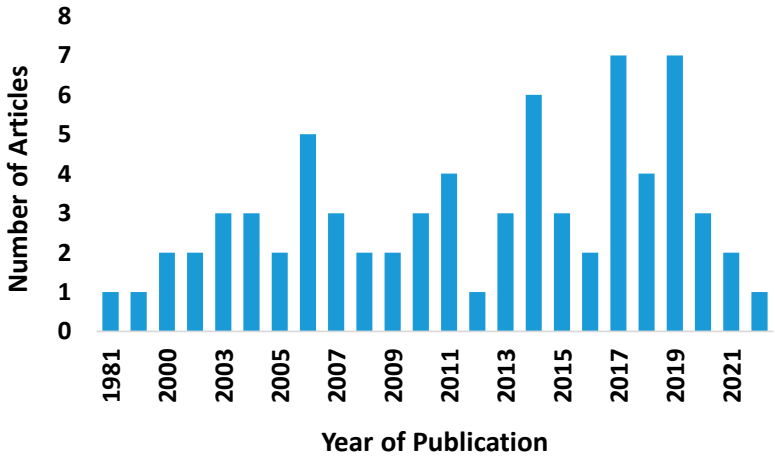

Figure 2. Year of publication of the selected articles.

In 13 of the included articles, the teams of authors were multi-disciplinary. The vast majority (n = 104) of authors contributed to only one article. Eight authors contributed to two of the articles included in the review, while there was only a single case of an author (Lucas Donato) contributing three works. The greatest contributor to the articles reviewed was Marcus Rogers, who authored/co-authored six articles. Table 2 provides descriptive statistics for all works included in this review.

The works of authors from 27 different countries were included in this review. The country with the greatest representation of authors was the United States of America with 36 authors. This was followed by the United Kingdom with 10 authors. Brazil and Canada were represented by three authors each. Estonia, Germany, Singapore, South Africa, Spain, and The Netherlands were each represented by two authors. Meanwhile, the remaining countries (Australia, Austria, Bulgaria, China, France, India, Iraq, Ireland, Italy, Latvia, Malaysia, New Zealand, Philippines, Poland, South Korea, and Switzerland) were represented by a single author each.

The 72 articles emanated from 52 different sources. The 32 journal articles were published in 26 different journals, with the majority of journals (n = 23) publishing a single article each. *The Journal of Cyber Criminology* and *Deviant Behavior* each published two articles. The journal with the greatest number of publications (n = 5) was *Digital Investigation*. Among the 26 different journals, 14 journals were related to computer technology and security, five were criminology journals, three journals were in the field of psychology, and four journals specialized in science or forensic science.

The 11 conference papers included in the review were presented at 10 different conferences. The only conference where two papers related to cyber profiling were presented was the European Conference on Cyber Warfare and Security (ECCWS). The seven magazine articles were found in five different magazines, with a single article appearing in each of *CSO*, *Cybertalk Magazine*, and *New Security Learning*. *Network World* and *Digital Forensics Magazine* each published two articles. The three industry reports emanated from three different sources—Cyber Road, Sans Institute, and Symantec Security. As illustrated in Table 2, less than half of the articles (45.8%) were peer reviewed. When the journal articles were isolated, however, all 32 journal articles were subject to peer review.

Table 2. Descriptive statistics on works/articles related to Cyber Behavioral Analysis.

Study Variables	Frequency	Percentage
Publication Decade		
1980–1989	2	2.8
1990–1999	0	0.0
2000–2009	24	33.3
2010–2019	40	55.6
2019–2023	6	8.3
No. of articles by author		
One article	104	91.2
Two articles	8	7
Three articles	1	0.9
Six articles	1	0.9
Discipline of Authors		
Computer Science/IT	32	44.4
Criminology	8	11.1
Law Enforcement	3	4.2
Psychology	7	9.7
Sociology	1	1.4
Multidisciplinary	13	18.1
Other (unspecified)	8	11.1
Publication Type		
Book	3	4.2
Book chapter	3	4.2
Conference paper	11	15.3
Dissertation	12	16.7
Industry report	3	4.2
Journal article	32	44.4
LE bulletin	1	1.4
Magazine article	7	9.7
Review Status		
Peer reviewed	33	45.8
Non-peer reviewed	39	54.2

To assess the nature of the articles relating to cyber profiling, an analysis was performed on the type of study, emphasis of the study, method, sampling procedures, and use of statistics. The vast majority (n = 50) of the articles reviewed were qualitative in nature. In terms of emphasis, the majority of the articles were discussion pieces (n = 24) or literature reviews (n = 15). Four of the articles were theoretical in nature and three were case studies. The remaining articles (n = 26) presented some primary empirical research, with comparison studies comprising half of these articles. Original data were collected in 28 of the articles; five studies gathered data from archival sources (e.g., law enforcement files), one study used the ethnographic method of observation, two studies involved interviews, and one study created a honeypot for data collection purposes. The most common method of primary data collection was the survey method (n = 18), particularly online questionnaires (n = 12).

An analysis of the sampling methods used among the studies reporting primary data found that the most common method employed was that of convenience sampling (e.g., snowball, voluntary response), with 21 studies employing such methods. Three of the studies using archival data employed an exhaustive sampling method within the specified study period. The sampling technique was unspecified in four of the studies. More than half of the articles (n = 45) included in this review involved no statistical analysis. Of the 27 articles that presented statistics, 6 studies provided descriptive statistics while 21 studies used analytical methods producing inferential statistics. Table 3 provides a summary of the statistical analyses and tests that were performed among the 27 articles that contained statistics.

Table 3. Predominant statistical analyses used in the selected articles.

Type of Statistics	Tests & Statistics
Assumptions	Normality; Homogeneity of variance; Independence; correlations for regression; Homogeneity of regression
Power and effect size	Statistical power
Descriptive	Frequency count; Percentages; Cross-tabulation; Mean; Standard deviation; Standard error; Median
Reliability	Cronbach's alpha
Correlational	Pearson's correlation; zero-order correlation; Spearman's correlation
Regression	Logistic regression (LG); Linear regression; Multiple regression correlation (MRC); Stepwise multiple regression; Backward stepwise (Wald) logistic regression; Stepwise logic regression
Model fit	Hosmer and Lemeshow
Univariate	Independent samples t-test; One-way ANOVA; Seemingly unrelated estimation
Multivariate	MANOVA
Co-variate	ANCOVA, MANCOVA
Probability distribution	Wilk's lambda
Non-parametric	Fisher's exact; Likelihood Ratio Chi Square; Mann–Whitney U; Wilcoxon W
Post-hoc	Bonferroni; Hochberg's GT2; Games–Howell; Hotelling's Trace; Hosmer and Lemeshow; Hosmer and Lemeshow's Measure (R_L^2)
Alpha levels	0.001; 0.01; 0.02; 0.05; 0.10

To assess the potential impact of the reviewed articles on the field of research, the number of citations for all articles in the dataset was analyzed. For the sake of consistency, citations were determined for all articles using Google Scholar. Using the method presented in [17] for standardizing citation counts, the number of citations for each article was divided by the number of years since publication. The number of citations across the 72 articles ranged from 0 to 349 (M = 37.91, SD = 58.84). Table 4 provides a ranking of the top 10 most cited articles relating to cyber profiling.

Table 4. Top 10 most cited articles in cyber profiling.

Rank	Reference	Authors	Year	Total Citations	Impact Score
1	[11]	Cross, M.	2008	349	23.3
2	[25]	Al-Mhiqani, M.N., Ahmad, R., Abidin, Z.Z., Yassin, W., Hassan, A., Abdulkareem, K.H. Ali, N.S., & Yunos, Z.	2020	40	13.3
3	[26]	Madarie, R	2017	67	11.2
4	[27]	Kirwan, G. & Power, A	2013	104	10.4
5	[28]	Chiesa, R., Ducci, S., & Ciappi, S.	2008	133	9.5
6	[29]	Rogers, M.K., Smoak, N.D., & Liu, J.	2006	160	9.4
7	[30]	Bachmann, M.	2010	115	8.8
8	[31]	Nykodym, N., Taylor, R., & Vilela, J.	2005	146	8.1
9	[32]	Rogers, M.K.	2001	177	8.0
10	[33]	Rogers, M.K.	2003	160	8.0

3.2. Contribution Themes

An analysis of the main focus or contribution to understanding cybercriminals among the 72 articles was undertaken. The majority of the articles (n = 61) had a singular main theme, while a minority of articles (n = 11) were identified as having a dual focus. An analysis of the articles identified the following themes: cybercriminal/hacker typologies, cybercriminal motivations, characteristics and traits, defining cybercriminals from non-

cybercriminals, predicting cybercrime, criminal profiling and cybercrime, and approaches to cyber profiling, which are discussed below.

3.3. Cybercriminal/Hacker Typologies

Becker [34] delivered a typology of cybercriminals based on his experience working at the National Centre for Computer Crime Data. This early effort at a typology focused on offender motivation. A number of authors have presented their own variations of cybercriminal or hacker typologies [31–34]. There is considerable overlap across many of the typologies, as shown in Table 5.

Table 5. Summary of hacker classifications.

Typologies	Papers
Old school hackers/old guard hackers	[35,36]
Bedroom hackers, casual hackers	[35,37]
Larval hackers & newbies/novices	[35–38]
WaRez D00dz	[39]
Internet hackers	[39]
Hacktivists/political activists	[35,36,38,40]
Script kiddies	[35,41]
Hackers	[35]
Crackers/cyber-punks/cybercriminals	[36,38,41]
Internals/disgruntled insiders	[36,42]
Petty thieves/the bank robber	[36,40,42]
Virus writers	[41]
Professional criminals, cyber syndicates	[36,38,40]
Information warriors	[41]
Cyber terrorists	[37]
Spies	[38,40]
Guru hackers	[42]
The accidental hacker	[38]
The rogue gamer	[38]
Nation state hacker	[38]

One of the more comprehensive hacker typologies was presented by Rogers et al. [29]. Rogers et al. [29] presented nine categories of cybercriminals based on their motivations and skill level, advocating for the use of a circumplex model to study and evaluate the taxonomy. While many of the authors presenting cybercriminal taxonomies have focused on classifying diverse groups of cybercriminals, some authors [36] have developed typologies for specific groups of cybercriminals. Shaw [36] conducted a literature review of research relating to insider threats, that is, individuals who commit cybercrimes against the organization for which they currently work or formerly worked.

Zhang et al. [42] presented an alternative way of developing a hacker typology, basing the classification on how hackers exchange knowledge on hacker forums. On this basis, Zhang et al. [42] identified four hacker groups, labelled as guru hackers, casual hackers, learning hackers, and novice hackers. The authors argued that the element of knowledge exchange behavior and the resultant hacker types should be used to extend existing typologies, such as in [29], as opposed to being a stand-alone classification system.

Cybersecurity industry personnel have also proposed hacker typologies based on what they have observed in the cyber threat landscape. For example, in a CSO online article, Grimes [38] argued the importance of understanding hackers and how they may attack. The author then presented 11 different types of hackers, including: the bank robber, the nation state, the corporate spy, the professional hacking group for hire, the rogue gamer, cryptojackers, hacktivists, botnet masters, adware spammers, the thrill hacker, and the accidental hacker. Many of the types of hackers presented by Grimes [38] were common among the classifications included in previous typologies.

3.4. Cybercriminal Motivations

A number of the reviewed works focused on the motivations that drive cybercriminals to commit their digital crimes (Table 6). Bissett and Shipton [40] focused specifically on the motivation of virus writers. Woo [43] considered intrinsic and extrinsic motivations and how internally and externally driven motivations relate to the types of hacking activities exhibited by hackers.

Table 6. Cybercriminal Motivations.

Motive	Papers
Non-specific malice	[40]
Revenge	[42–45]
Ideological motives/the soapbox, hacktivism /fight for freedom	[29,39,41,43,45]
Commercial sabotage, espionage	[41,43]
Warfare/the war zone	[39,41,43]
Playpen/for fun	[29,39,45,46]
Monetary/cookie jar, extortion/fraud	[29,39,41,42,44,47]
Curiosity	[27,41,46]
Vandalism	[35]
Intellectual challenge	[27,29]
Power trip	[28]
Escape from their physical life	[28]
Notoriety/fame/peer recognition	[27,29,44,45,47]
Addiction	[48]
Mental health disorder	[44]

In his dissertation research, McBrayer [48] examined which motivations were associated with different computer deviant behaviors. McBrayer [48] was able to attribute specific motivations by cybercriminal type, finding that script kiddies are often motivated by addiction, cyber-punks by financial gain and, to a lesser extent, peer recognition and revenge, and internals by financial gain and peer recognition. In contrast, instead of assessing motives by type of cybercriminal behavior, Back et al. [44] examined the motives of youth and adult hackers in South Korea. Their findings suggested that motivations may change based on the age of the offender. Youth offenders were found to be motivated by hacktivism, revenge, and exposure. Meanwhile, adult hackers were found to be motivated by blackmail or mental health disorders. Both youth and adults were most often motivated, however, by financial gain and entertainment [44].

Using Q-analysis, Cayubit et al. [46] identified three factors that could explain why hackers engage in hacking activities even though the behavior is illegal. These factors were superiority, exploitation, and opportunity. According to the authors, these factors aligned with the classification of black hat and white hat hackers, such that black hat hackers are motivated by exploitive and opportunistic factors while white hats are motivated by superiority. The authors further argued that these factors can be understood using the expectancy–value theory of motivation [46]. Madarie [26] grounded the exploration of hacker motives within a theoretical framework, based on the theory of motivational types of values. Despite the common misperception that cybercrimes are all financially motivated, Madarie [26] found money to be the least motivating factor among a sample of 65 hackers. Intellectual challenge and curiosity were found to be the strongest motivators, followed by peer recognition. Also, the values of openness to change and self-transcendence were positively related to hacking activities [26].

The final work included in this review examining the motivations that lead to cyber criminality was the dissertation research of Palmieri [47]. This research explored how different motivations, social power, and anonymity impact the decision to engage in cybercrime. Impulsivity and reward interest were both found to be positively related to the decision to engage in cybercrime. Reward reactivity and goal-driven persistence

were both negatively correlated with this decision. Palmieri's research also identified a number of personal characteristics related to the commission of cybercrime, including race, ethnicity, un- or under employment, sex, and education [47]. Males of European descent who were middle class and/or unemployed were more likely to engage in cybercrime. Palmieri [47] also found that as one's perception of anonymity increased, the odds of committing cybercrime also increased.

3.5. Characteristics and Traits

A number of other researchers have focused on identifying the traits and characteristics of various cybercriminals, particularly hackers. Some authors have grounded their research in theory, for example, Woo [43], who explored various psychological traits among a sample of 719 hackers through the lens of flow and terror management theories. Woo [43] found a relationship between narcissism and aggressiveness, such that hackers who scored high on narcissism also scored high on angry temperament. Hackers who were identified as having a high level of extrinsic motivation were also found to have an angrier temperament. Woo [43] found that the experience of flow was related to the frequency and type of hacking activities in which an individual engaged.

Arguably the most comprehensive study to date examining the traits and characteristics of hackers is the work of Chiesa et al. [28] on the Hackers' Profiling Project (HPP). It is important to note that this research included both criminal hackers and hackers who did not profess to having committed any cybercrimes. Chiesa et al. [28] found that hackers were diverse in terms of demographics. There were hackers of all age groups, socioeconomic status, professions, ethnic groups, and geographic locations. Contrary to the common misconception that all hackers are geniuses, only 17% of the hackers included in the HPP had university degrees; however, many hackers may not have engaged with conventional educational systems or awards. A number of the respondents indicated suffering from a psychological condition, the most common of which was insomnia (34%), followed by anxiety (27%), paranoia (20%), panic attacks (13%), and hallucinations (6%). In relation to the number of hours spent hacking, 31% hacked 1–3 h per day, 30% hacked 4–6 h per day, 14% hacked 7–10 h per day, and 21% hacked more than 12 h per day. Despite the amount of time spent on hacking activities, 47% indicated that they did not believe they had a so called "addiction" to hacking. Only 14% indicated that they believed they were "addicted" to hacking [28]. Among a sample of college students in Hong Kong, Chiu [49], found no individual factors related to cybercriminal behavior. However, a positive correlation between total score for computer criminal behavior, exploitive manipulative behavior, and computer "addiction" was found [49].

Research conducted by Seigfried-Spellar, Villacis-Vukadinovic and Lynam [50] sought to validate the elemental psychopathy assessment (EPA) short form and extend validity criteria to computer crime. Specifically, this research examined the relationship between cyber criminality and psychopathy as well as other antisocial traits. Based on their sample of 235 respondents emanating from Amazon's Mechanical Turks, Seigfried-Spellar, Villacis-Vukadinovic and Lynam [50] found that psychopathy, narcissism, interpersonal antagonism, disinhibition, as well as other types of antisocial behavior were all related to the commission of cybercrime. Among these traits, psychopathy was found to be most strongly related to cybercrime. In contrast, Withers [51] found no significant positive relationship between the dark triad (i.e., narcissism, psychopathy, and Machiavellianism) and the commission of cybercrime. In fact, Withers [51] found a significant negative relationship between Machiavellianism and cybercrime.

One of the common perceptions of cybercriminals is that they are technological geniuses. Research by Treadway [52] refuted this assumption. Among a sample of 319 respondents, equally split by gender and cyber deviant status, Treadway [52] found no significant differences between the intelligence measures of cyber and non-cyber deviants. Virgara and Whitten [53] defined cyber deviance as "engaging in deviant or criminal behaviors with the facilitation of technology". More recently, researchers and practitioners have con-

sidered whether there is a link between autism and the commission of cybercrime [49,50]. In their research on the relationship between autism, autistic traits, and cybercrime, Payne et al. [54] found that those with higher autistic quotient (AQ) scores were more likely to have committed cybercrime. A self-reported diagnosis of autism, however, was associated with a decreased risk of committing cyber-dependent crime. The increased likelihood of committing cybercrime may therefore be better explained by the advanced technical skills of certain individuals with autistic traits, as opposed to a diagnosis of autism [54].

3.6. Differentiating Cybercriminals from Non-Cybercriminals

Foundational to being able to apply criminal profiling approaches to cybercrime is an understanding of what makes cybercriminals different from non-cybercriminals and from individuals who commit offences in the physical world. In his dissertation [32], Rogers conducted exploratory research focused on establishing the differences between individuals who engage in cybercrime and those who do not. Grounded in social learning and moral disengagement theories, Rogers [32] found that individuals who committed cybercrime had higher levels of differential association, differential reinforcement, and moral disengagement than individuals who did not engage in such activities. Interestingly, the author [32] found no significant differences between computer criminals and general criminals in relation to demographics, with the exception of race.

Similarly, Young et al. [55] found that among their sample of 127 individuals attending DefCon, a popular conference for hackers held in the US, illegal hackers (n = 54) had significantly higher levels of moral disengagement. Young et al. [56] also found that while illegal hackers' perception of the severity of punishment for hacking was higher than that of others surveyed, illegal hackers perceived a significantly lower likelihood of getting caught for their illegal activities. This may in part be explained by the work of Bachmann [30]. In a study of 124 individuals who attended a hacker conference in the US, it was found that hackers had a significantly higher than average rationality value and a higher risk propensity than the general public. The most successful hackers, however, were the ones who preferred analytic-rational approaches to thinking but had a lower propensity for risk [30]. This preference for rational thinking may in part explain why hackers perceived a significantly lower likelihood of getting caught. Arguably, given the low rate of reporting of cybercrime, a rational cybercriminal may assess that the potential for personal gain or fulfillment outweighs any risk.

In an effort to further elucidate the differences between cybercriminals and non-cybercriminals, as well as among the different types of cybercriminals, Seigfried-Spellar and Treadway [55] studied a sample of 296 undergraduate students with diverse majors at a university in the southern United States. Among the 296 undergraduates, 60% self-reported having committed some form of cybercrime. These respondents reported engaging in hacking (57%), identity theft (13%), cyberbullying (23%), and virus writing (8%), with 47% of the hackers reporting engagement in one of the other types of cybercrime. Seigfried-Spellar and Treadway [55] found no significant differences in study majors or personality characteristics among those engaged in computer crime and those not engaged in computer crime. The authors were able to identify predictors for the different types of cybercrime, which are reported in the next section.

Kranenbarg et al. [57] applied a novel approach to differentiating cybercriminals from general criminals by examining whether different events over the courses of their lives led to one form of crime over the other. Using police and registry data in the Netherlands from 2000 to 2012, the authors found that household composition effects for cybercrime were in the same direction as those for traditional crime, only the effects were greater. Cyber criminality was much more likely when a person lived in a single parent household than when the same person lived alone. Having a job reduced the odds of an individual committing cybercrime or traditional crime by 10% and 7%, respectively. For those employed in IT, the opposite results were found. It increased the odds of committing cybercrime by 14%, whereas it decreased the odds of committing a traditional crime by 11% [57].

3.7. Predicting Cybercrime

A number of studies have attempted to identify the factors that may predict cybercrime. Gordon and Ma [58] focused on factors that impact the intention to hack. They found that moral obligation and self-efficacy were significant predictors, with moral obligation showing the strongest negative effect. Based on their research, Gordon and Ma ([59], p. 8) concluded that hackers "tend to be self-motivated and self-centered individuals; they are not likely to be easily influenced by friends or family members". In their study of 77 university students, Rogers, Seigfried and Tidke [59] found that only extraversion was predictive of cybercriminal behavior. The findings of this study were at odds with those of other studies (including by the same lead author) in which no significant relationship between extraversion and cybercriminal behaviors was reported [29]. In their study of 381 Canadian university students, Rogers, Smoak and Liu [29] found that computer-related deviant behavior was negatively correlated with internal and social moral choices and positively correlated with exploitive manipulative amoral dishonesty.

In his dissertation research, Crimmins [60] tested the predictive model presented in [59] using a more diverse sample of college students. Crimmins [60] found that internet addiction and openness to experiences were significantly related to computer criminal behavior. No significant correlation was found between the amount of time spent online and computer criminal behavior. Unlike Rogers, Seigfried and Tidke [59], Crimmins [60] found no significant relationship between cybercriminal activities and extraversion, nor did he find a relationship with manipulative/exploitative behavior or morality. Crimmins [60] concluded that so called "internet addiction" is the best predictor for computer criminal behavior in college students.

Seigfried-Spellar and Treadway [55] argued for the importance of recognizing the heterogeneity among cybercriminal groups and to discriminate among groups when conducting research. These researchers found differences in the personality factors that predict different types of cybercriminal activities. A low score on agreeableness was a moderate predictor for hacking. The best predictors for distinguishing between identify and non-identity thieves were high scores on neuroticism and low scores on internal moral values. The best predictive model for virus writers was a low score on moral values. However, cyberbullies were predicted by high scores on neuroticism and low scores on internal values [55].

3.8. Criminal Profiling and Cybercrime

Coutourie [24] appears to be the first author to propose the usefulness of criminal profiling in cybercrime investigation. Coutourie [24] recognized the need to slightly adjust the practice of criminal investigative analysis (CIA) to account for the differences between an interpersonal crime occurring in physical space and a cybercrime occurring in virtual space. Over the years, a number of authors have advocated for the use of criminal profiling in cybercrime investigations [11,24,32,38,42,45,46,61–81]. Bongradt [81], a former FBI agent, argued that modern criminal profiling requires an understanding of how an offender interacts in cyberspace. In 2004, Bednarz recognized the work of Marcus Rogers in the development of a cybercriminal classification framework but concluded that profiling cybercriminals is a "promising but immature science [82]". The main issue for advancing cyber profiling, according to Bednarz [82], is the lack of comprehensive data on cybercriminals. This is a sentiment that has been echoed by others [42,60,75].

A number of authors have taken an existing approach to profiling and attempted to apply that approach to cybercrime. For example, Nykodym, Taylor and Vilela [31] provided an overview of behavioral evidence analysis (BEA), a profiling method developed by Brent Turvey [83]. The authors concluded that it is more difficult to profile cybercrimes than traditional crimes [31]. Despite the perceived difficulty, many authors see value in integrating criminal profiling into cybercrime investigations [24,62,64,67,82]. Casey and Turvey [65], in their book chapter Investigative reconstruction with digital evidence, provided the reader with an overview of BEA and how this approach to profiling can be applied to cyber inves-

tigations. Particular attention was paid to the reconstruction of cybercrime based on an equivocal forensic analysis, a phase in BEA whereby the profiler/investigator examines the evidence looking for behavioral imprints. Behavioral imprints are clues into the offender's personality, modus operandi, and motivation [65].

Balogun and Zuva [74] also proposed a model for profiling cybercrime with a foundation in behavioral evidence analysis. The framework put forth by these authors more fully integrated digital forensics into the reiterative profiling process. The authors argued that this model should be applicable to profiling of all forms of cybercrime. In fact, there are a number of authors [33,61–63,68,71,74,76,80,84,85] who have argued for an integration of criminal profiling and digital forensics, that is, the process of identifying, extracting, analyzing, and reporting digital evidence. In fact, Lickiewicz [66] argued that computer security specialists have taken an interest in integrating an understanding of the cybercriminal into their threat modeling because the offender is the only stable element in the investigation. Disciplines such as cyberpsychology have adopted an integrated research approach. Cyberpsychology is the study of the impact of technology on human behavior, covering a range of research fields from internet psychology to artificial intelligence. A reference to the emerging sub-discipline of forensic cyberpsychology first appeared in Europol's 2014 Internet Organised Crime Threat Assessment Report, noting that "the critical task for cyberpsychology as a discipline is to build up a body of established findings of how human beings experience technology, the critical task in forensic cyberpsychology is to focus on how criminal populations present in cyber environments" ([86], p. 82).

In their conference paper, Kwan, Ray and Stephens [63] differentiated between cybercrime and cybercriminal profiles. The former is created through the process of digital forensic analysis and focuses on the technical elements of cybercrime. The latter, the authors argued, can be developed based on the developed cybercrime profile [63]. The authors did not explicitly state how one would develop the cybercriminal profile from the cybercrime profile. There is recognition of the value of engaging multi-disciplinary teams to contribute to the process of profiling cybercriminals [61,62,80]. A recent pan-European research project regarding human and technical drivers of cybercrime applied such a multi-disciplinary approach by incorporating a wide range of disciplines, including psychology, criminology, anthropology, neurobiology, and cyberpsychology [87].

Casey [62] argued that the early application of profiling to cybercrime investigations can help inform the digital forensic process (i.e., what evidence can be expected to be found and where). Some authors [61] have proposed the automation of profiling methods to deliver cybercrime profiles, although it is unclear how this automation would occur or if it would be capable of addressing all aspects of behavioral analysis.

In his dissertation research, Sutter [79] examined whether there is a connection between cyber attacker actions and human behavior. Using investigative psychology and the work of David Canter as his framework, Sutter [79] used smallest space analysis (SSA) to explore how the technical actions in a cyber attack may cluster and align with human behavioral sub-types identified through research on burglary. While Sutter [79] found that the attack actions did cluster into identifiable facets, these facets could not be aligned with a single behavioral typology. Sutter [79] suggested that the use of SSA to profile cybercrime may not be appropriate.

3.9. Approaches to Profiling Cybercrime

A number of authors have proposed frameworks or models for the application of profiling to cybercrime. The proposed frameworks all emanate from a review of the literature related to criminal profiling. Some frameworks focused exclusively on deductive profiling methods (e.g., [67]), while others have included inductive profiling within their visualizations of the profiling process. Warikoo [37] proposed what he referred to as a hybrid methodology for profiling cybercriminals. In his article, Warikoo [37] outlined profile identification matrices, including: (1) signature, (2) attack method, (3) motivation level, (4) capability factor, (5) attack severity, and (6) demographics (which the author

defined essentially as geography). In addition to these matrices, Warikoo [37] outlined a four-step process of victim profiling, motives behind the attack, statistical analysis to identify trends, and building the cyber profile. At the outset of his work, Warikoo [37] argued that any proposed profiling methodology should be scientific and informed by empirical research. However, it is unclear in the article how the proposed methodology can be considered scientific.

Rogers ([73], p. 47) argued that digital forensics "seems to be enamored with computer science and engineering principles (e.g., hash functions, memory dumps), but apparently is unaware of traditional investigative approaches". The framework for psychological profiling proposed by this author was a five-step process involving content analysis of case information, collection of relevant evidence, statistical analysis to identify trends and establish the target's online behavior, timeline analysis and visualization, and decision/opinion. The collection of relevant evidence involved an integration of digital forensic analysis within the framework [72]. Donato [80] also presented a model of profiling cybercriminals that embedded profiling within the process of digital forensics. In his research, Donato [80] used a honeynet, i.e., a network of connected honeypots, to examine the attack data. He concluded that profiling of cybercrime using the BEA approach was possible, as it was possible to identify aspects of human behavior, modus operandi, and signature through the examination of attack data [80].

Frumento et al. [88] focused their research efforts on one aspect of profiling cybercrimes, that is, victimology. These authors differentiated between technical and human attack vectors. Focusing on the human attack vector (i.e., gaining access by exploiting humans and human behavior), Frumento et al. [88] introduced the concept of the victim communication stack (VCS). The VCS provided a framework for understanding how the human victims of cybercrime were targeted. Kipane [76] indicated that profiling of a cybercriminal consisted of four interrelated and successive stages: (1) victimological aspect, (2) clarifying the motives of the criminal, (3) identification of features/properties (inductive and deductive profiling used to ascertain characteristics of the offender), and (4) digital behavioral analysis, i.e., a process of applying traditional behavioral analysis to the digital footprint of the criminals.

Approaching the task from a cybersecurity/IT systems perspective, Pahi and Skopik [85] presented the cyber attribution model (CAM). The CAM consisted of two parts. The first was an examination of the cyber attack through a technical analysis of the event. The second part was threat actor profiling. In their model, the authors advocated for proactive threat actor profiling through inductive methods. These profiles could then be compared to the information gleaned from part one of the process in order to determine if one could match the current attack to a known threat actor profile [85].

4. Discussion

4.1. Interpretation

A review of the literature pertaining to cybercriminal profiling indicates that this field remains in its infancy, with the majority of articles in the category of literature reviews or discussion pieces. A minority of articles are based on primary data, and these tend to utilize convenience samples of college/university students as opposed to individuals who are part of known hacker communities. Indeed, research in this field has faced a number of challenges that must be overcome for advancements to be made. These challenges include the lack of a universally accepted taxonomy for both cybercrime and profiling, a dearth of specialists working in this field, and a lack of primary data.

4.2. Lack of a Standard Taxonomy

There is no universally accepted taxonomy for either cybercrime [19,63,75,89] or criminal profiling [76]. Cybercrime is one term among many, including computer crime, internet crime, e-crime, and digital crime, that has been used to denote crimes that are committed using or against a computer system. In the absence of standard terminology, it is not

surprising that no standard definition of cybercrime has been adopted [19]. Many different definitions of cybercrime have been proposed in the existing literature. The Council of Europe ([90], p. 2) defines cybercrime as "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalization of such conduct". Phillips et al., [19], in their review of the taxonomies of cybercrime, identified various methods of classification, including dichotomies and trichotomies. Dichotomies break cybercrime into two classes of crime: (1) cyber-dependent (crimes that do not exist without computers and/or the internet and (2) cyber-enabled (traditional crimes that are committed with the assistance of computer and internet technologies). With the trichotomy classification system, an additional class of cybercrime is included: content-related offences. Donato [64] employed a trichotomy when he identified the following types of cybercrime based on his review of the relevant literature: computer-targeted, computer-assisted, and computer incidental. Computer incidental offences were the equivalent of content-related offences, whereby the computer was housing information or data related to an offence.

Criminal profiling has been identified using many different names, including criminal investigative analysis, personality profiling, behavioral analysis, behavioral evidence analysis, and investigative psychology, to name a few. While researchers and practitioners generally agree that there are two types of profiling—inductive and deductive [37,64,72,75–77,81,84]—there are discrepancies in how these approaches have been identified, described, and applied. For example, Nykodym, Taylor and Vilela [31] identified prospective and retrospective as two approaches to profiling. A review of their description of these approaches revealed that the prospective approach was equivalent to inductive profiling and the retrospective approach was equivalent to deductive profiling. However, Steel [71] distinguished between idiographic and nomothetic approaches to profiling. These approaches also roughly translated to deductive and inductive profiling, respectively, whereby the idiographic approach explored at a microlevel (the individual) and the nomothetic approach explored at the macro level (community or group). To avoid confusion and differentiate the application of profiling techniques to cybercrime, as opposed to traditional crimes of interpersonal violence, the authors propose using the term cyber behavioral analysis (CBA).

4.3. A Dearth of Specialists Working in the Field

Consistent with the findings of previous reviews [16–18], there are very few authors who specialize in this field, as evidenced by the number of authors who were found to have contributed only a single article relating to the profiling of cybercrime. Similarly, few journals have published more than a single article on this topic. For the advancement of cyber profiling, there is a need to have both researchers and practitioners specialize in the area (i.e., conducting numerous studies over time) and work in collaboration, with specifically allocated funding to undertake such research. Without the engagement of practitioners, it will be difficult, if not impossible, to establish the efficacy of cyber behavioral analysis as applied to real cybercrime investigations. Cybercrime poses many challenges for global society. Effective investigation will require the development of multi-disciplinary teams of law enforcement, academics, and cybersecurity professionals.

4.4. Lack of Primary Data

Criminal hackers are a notoriously difficult population to access [51]. While the hacker ethic espouses the freedom of information [91,92], this population finds refuge in the Dark web, described in a recent law enforcement report as offender convergence settings [93]. Convergence settings help obfuscate criminal hackers' real identities and allow them to operate almost anonymously. Given the difficulty in accessing this population, many researchers have opted to produce literature reviews or discussion pieces relating to hackers and the profiling of cybercriminals. Empirical research evaluating hacker typologies is

lacking. In fact, the foundation or basis for many of the typologies presented in the research is unknown, theoretical in nature, or based on proxy samples.

Empirical research on the traits and characteristics of cybercriminals is beginning to emerge and the use of inferential statistics in these studies is promising. The samples used in many of these studies, however, limit the value of the findings in terms of their application in cyber behavioral analysis. Many studies use convenience samples of university and college students, which may result in respondent bias. One may certainly find individuals engaged in the commission of cybercrime among student populations, as a recent study found that just under half 47.76% (n = 3808) of the 16- to 19-year-olds surveyed reported to have engaged in criminal behavior online [94]. It is unlikely, however, that student populations accurately reflect the characteristics and motivations of the most prolific cybercriminals. Similarly, case studies provide an in-depth look into the psychology, motivations, and activities of a single or small number of cybercriminals. Research indicates, however, that cybercriminals are a heterogenous population. Therefore, to fully understand cybercriminals, it is necessary to conduct empirical research studies on the many different groups of cybercriminals, based on sufficient samples. A collaboration among academics, law enforcement, and cybersecurity specialists may assist in accessing cybercriminal populations.

4.5. Proposing a Comprehensive Framework for Cyber Behavioral Analysis (CBA)

While still in the early stage, the extant literature on cyber profiling indicates that it is possible to apply traditional profiling methods to cybercrime. There is, however, no agreement on which approach to profiling is best applied to cybercrime investigations, with different authors favoring deductive profiling, inductive profiling, or a combination of the two. What is clear from the literature is that any application of criminal profiling to cybercrime must be adjusted to reflect a digital as opposed to physical crime scene. In their systematic review, Bada and Nurse [18] recommended that future research should focus on the establishment of a common systematic approach to cyber profiling. It is this recommendation that led to the aim of the current review—to propose a comprehensive framework for CBA integrating the approaches identified in the existing literature.

Malin [95] argued that the profiling of cybercrime requires a process of digital behavioral criminalistics. Digital behavioral criminalistics is defined as "the combined application of numerous forensic disciplines—digital forensics, criminalistics, and behavioral sciences—to meaningfully uncover, reconstruct and understand the user thought processes, behaviors, and actions captured in digital media" ([95], p. 557). Taking into consideration Malin's [95] definition of digital behavioral criminalistics and the frameworks proposed in [38,61,64,67–70,73,75,77,81,85,88,89,96], one can identify the important elements for the development of a comprehensive framework for CBA.

4.6. A Comprehensive Framework for CBA

CBA is initiated using a deductive profiling approach, wherein the first step is to thoroughly review the evidence that has been collected in the course of the investigation. Digital forensics is the process of identifying, accessing, acquiring, and analyzing data from the digital crime scene. The cyber behavioral analyst should work closely with digital forensic analysts to help identify the location of potential evidence and prioritize evidence collection.

Case evidence may be collated into different streams, including victim data, open-source intelligence, and modus operandi (MO). Victimology is defined as "the scientific study of crime victims including the study of the relationship between victim and offender and the consequences and effects of being victimized" [97]. In addressing victimology, the cyber behavioral analyst will consider who the victim is, whether the victim is an individual or organization, what made the victim an attractive target, the cybersecurity posture of the victim, the relationship between the victim and offender, and whether the victim was specifically targeted or one of opportunity [88].

Open-source intelligence (OSINT) is defined as "intelligence produced by collecting, evaluating and analyzing publicly available information with the purpose of answering a specific intelligence question" [98]. The cyber behavioral analyst should be familiar with intelligence processes and be able to conduct OSINT, or work with intelligence analysts to gather case-relevant information. Through traditional investigative techniques, digital forensic analysis, and OSINT, cybercrime elements such as identifiers/monikers, accounts, passwords, internet search history, internet protocol (IP) addresses, and associates related to the cybercriminal(s) may be identified. The cyber behavioral analyst may work with intelligence or crime analysts to collect and analyze these data.

Modus operandi (MO) is a Latin term which translates to operating method [99]. An offender's MO is the distinct manner or way in which they commit their crime. In relation to cybercrime, the MO may be comprised of the manner in which the offender gained initial access to a system, the tools or techniques used to conduct reconnaissance, copy, change, or delete information, encrypt data, exfiltrate data, and obfuscate one's actions within the victim's system [100]. Digital forensics can elucidate the MO used by the cybercriminal(s) during an attack. This information must be understood by the cyber behavioral analyst so that it can be assessed for behavioral imprints [65] and indications of criminal sophistication and motive. Evidence gathered and analyzed through the process of digital forensics can also help the cyber behavioral analyst identify a signature, if any, left by the offender. The Federal Bureau of Investigation defines a signature as the offender's calling card, which is a unique aspect of the criminal's behavior that goes beyond the actions required to commit the offence (FBI, 1992). In cybercrime, it is important to examine the digital evidence, including the computer code, for a signature.

CBA is developed through an iterative process of analyzing case-specific evidence as it becomes available. The analysis of all evidence (digital forensics, victimology, and open-source intelligence) through a behavioral lens may allow the cyber behavioral analyst to establish an informed opinion regarding the characteristics of the likely offender and the motive for the offence. The cyber behavioral analyst may then consider the data emanating from an inductive profiling approach. This information may be used to support the conclusion made by the cyber behavioral analyst using deductive profiling methods or to fill in any possible gaps in information. The ultimate goal of CBA is to aid in offender attribution and inform the provision of investigative and interview strategies (Figure 3).

4.7. Limitations of Evidence

Upon exploring the literature, the lack of a common taxonomy with regards to profiling, behavioral analysis, and cybercrime was apparent. For example, the focus of this article was on cybercrime where a computer was the target, i.e., hacking, and did not examine other aspects such as child exploitation or cyber bullying. While some of the literature referred to the latter as cybercrimes, these are crimes facilitated by the internet. Therefore, the eligibility criteria in the present research specified the selection of papers that addressed the profiling of cybercrime where the computer was the target. Another inconsistency in the literature was the use of the term behavioral analysis or behavioral modeling in relation to malware. This systematic review used the definition of behavioral analysis as applied to the human perpetrator, not the software or attack vector. Further, the inclusion and exclusion criteria were implemented, but the lack of a common taxonomy for both cybercrime and criminal profiling, and the fact that there is a dearth of literature that directly explores the criminal profiling of cybercrime, necessitated the boundaries for the inclusion criteria to be less firm. There was a slightly larger body of literature that did not specifically address profiling but did address issues that inform and are of interest to those who perform behavioral analysis.

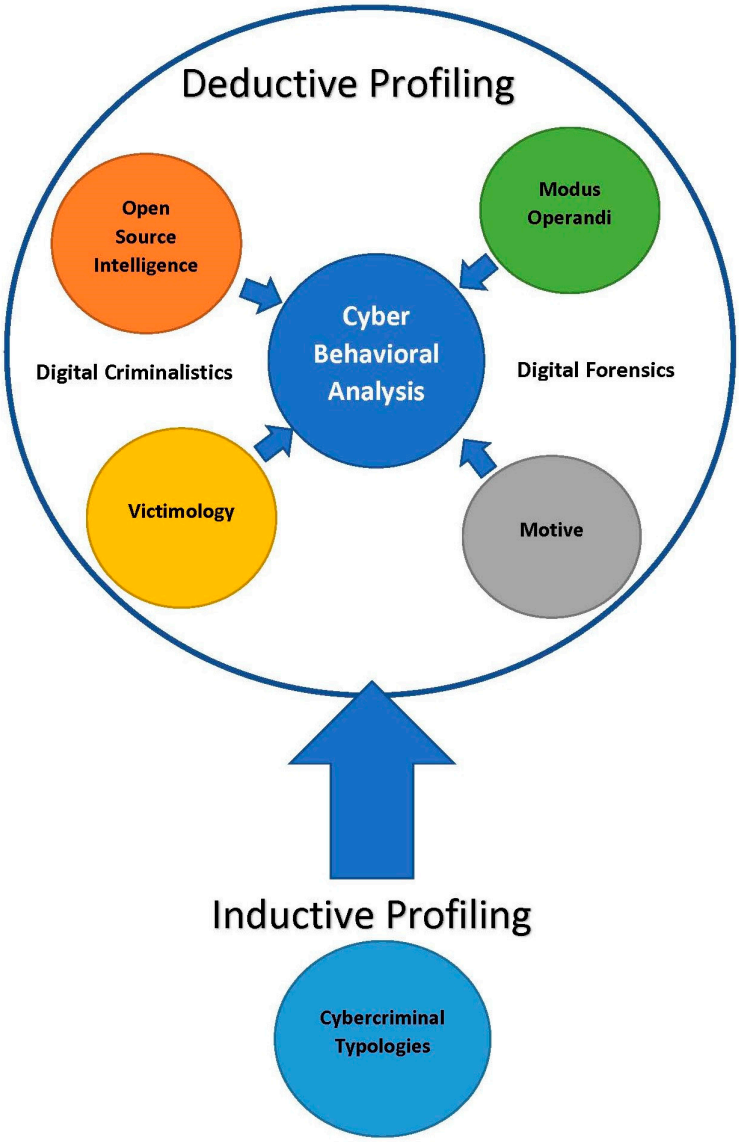

Figure 3. Proposed Framework for Cyber Behavioral Analysis.

4.8. Limitations of Review Processes

The lack of a standard taxonomy for both cybercrime and cyber profiling made it difficult to develop a comprehensive list of keywords from which to formulate queries that would identify all the relevant literature. It is possible, therefore, that additional relevant literature exists that was not identified for review. This is a limitation of this research.

4.9. Implications

This review has identified a number of challenges facing the emerging field of forensic cyber psychology [101], including the lack of a standard taxonomy, data access issues, the lack of specialists, and the potential disconnect between academics and practitioners working in the field. Through the identification of these issues, this review hopes to spark interest among academics and practitioners to work collaboratively to find resolutions. Agreement on a universally accepted taxonomy for both the fields of cybercrime and profiling would eliminate considerable confusion. This review culminated in the proposal of a comprehensive framework for cyber behavioral analysis (CBA). Unlike many existing frameworks, which are based in a single approach to profiling, this framework attempts to integrate the full range of different approaches and is based on a comprehensive review of the literature. It provides a systematic method for approaching CBA, which incorporates

both inductive and deductive profiling methods and integrates digital forensics and digital criminalistics within the process. It is hoped that this framework will be of use to practitioners working in the field of cybercrime investigation. Following a systematic process for cyber profiling will further legitimize the use of this tool in cybercrime investigations in order to ensure a more comprehensive and consistent approach to behavioral analysis.

4.10. Future Research Directions

To advance the field of cyber profiling and ensure pragmatic application of the knowledge gleaned and the frameworks proposed from the extant research, several future research endeavors should be undertaken. In order to more fully implement inductive profiling within cyber behavioral analysis, it will be necessary for researchers or practitioners to establish robust datasets of information pertaining to cybercriminals and cybercriminal activities. Datasets relating to known cybercriminals may alleviate the need for researchers to rely on proxy samples. Using such datasets, it will be possible to evaluate and possibly expand upon the existing cybercriminal typologies. Studies identifying important psychological, sociological, criminological, and demographic factors that differentiate cybercriminals from non-cybercriminals and among cybercriminal groups would also help advance this field. In addition, research focusing on the pathways that lead and motivate individuals to engage in cybercrime can help inform not only CBA but also the development of effective prevention strategies. As the field of cyber profiling matures, it will also be important to conduct research to evaluate suggested frameworks (including CBA) and their application in real cybercrime investigations.

5. Conclusions

Despite four decades of research focusing on cybercriminals, the state of the literature remains at an early stage. Much of what we currently know about cybercriminals stems from the works of authors who provided accounts of the development of the hacker culture or research using proxy samples. The research is heavily weighted with literature reviews and discussion pieces by authors who are not regularly conducting empirical research or contributing new works to the field. The lack of more complex research using primary data and the dearth of a concerted effort by experts to advance knowledge in the field has resulted in limited development. Technology is a field of constant advancement. This constant advancement has led to heterogenous groups of cybercriminals who are adapting new techniques, tactics, and protocols at a considerable pace. Understanding these criminals necessitates a continuous research effort. Hacker typologies that were proposed two decades ago may not adequately reflect today's cybercriminals, just as the typologies developed today may have little relevance to the ever-evolving cybercriminals of tomorrow. This systematic review led to the proposal of a new framework for the application of profiling to cybercrime. Future research efforts should include an evaluation of how this framework performs when applied to cybercrime investigations. The intention of proposing this framework was to consider the existing approaches to profiling and the role that digital forensics may play in the profiling process. CBA incorporates elements of the various approaches reviewed as well as digital forensics to provide a more comprehensive approach to cyber profiling.

Cyberspace could be considered as an almost unintended virtual world emanating from a project to enable military communication and it has been created at a breakneck pace. Cyberspace has become an environment populated by humankind that we now must find a way to secure, in the same way that people are protected in the real world. Law enforcement is faced with the considerable challenge of keeping pace with the adoption of new technologies in order to investigate crimes that take place in the digital world of cyberspace. Advancements in digital forensic analysis have equipped law enforcement with improved methods of identifying, acquiring, and analyzing evidence found on devices. Effective investigative strategies, however, cannot exclusively focus on the technical aspects of cybercrime. An understanding of the human perpetrators behind the keyboard is

essential. This is where CBA can contribute to cybercrime investigations and where the utility of emerging disciplines such as cyberpsychology and forensic cyberpsychology will undoubtedly prove to be invaluable. The efficacy of CBA rests in the use of a systematic approach that is empirically based and integrates digital forensics. Cybercrime is an area of study that will require continuous updating of our knowledge base. Just as anti-virus software requires continuous updating to protect our computer systems, the theories and research that form the basis of CBA must be continuously revised to protect the safety and security of a global citizenry.

Author Contributions: M.M. has contributed to all aspects of the article. E.S. and M.A. have contributed substantially to conceptualization; methodology; use of software; validation; formal analysis; investigation; academic resources; writing—original draft preparation, review and editing; and supervision. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Review Board of Capitol Technology University (protocol code IRB03082023; date of approval 17 March 2023).

Informed Consent Statement: Not applicable.

Data Availability Statement: This systematic review did not involve the collection of new data. The data extraction template is available upon request from the first author.

Acknowledgments: The authors are very grateful to Emily Fox for the support provided during the critical appraisal and selection of articles for inclusion in the systematic review.

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

References

1. Erbschloe, M. *Computer and Internet Crime*; EBSCO Research Starters: Birmingham, AL, USA, 2020.
2. Flath, T. Cybersecurity Experts Failing to Keep Pace with an Explosion in Cybersecurity Threats. LinkedIn. Available online: https://www.linkedin.com/pulse/cybersecurity-experts-failing-keep-pace-explosion-threats-tony-flath?trk=public_profile_article_view (accessed on 3 September 2017).
3. Aiken, M.; Farr, R.; Witschi, D. Cyberchondria, Coronavirus, and Cybercrime: A Perfect Storm. In *Handbook of Research on Cyberchondria, Health Literacy, and the Role of Media in Society's Perception of Medical Information*; IGI Global: Hershey, PA, USA, 2022; pp. 16–34. [CrossRef]
4. Moloney, C.J.; Unnithan, N.P.; Zhang, W. Assessing Law Enforcement's Cybercrime Capacity and Capability. Available online: https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability- (accessed on 9 June 2023).
5. SC Government of Canada. The Daily—Impact of Cybercrime on Canadian Businesses. 2021. Available online: https://www150.statcan.gc.ca/n1/daily-quotidien/221018/dq221018b-eng.htm (accessed on 12 February 2023).
6. Canadian Centre for Cyber Security. National Cyber Threat Assessment 2023–2024. Communications Security Establishment, Threat Assessment, ISSN: 2816-9182. 2022. Available online: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024 (accessed on 9 June 2023).
7. The White House. Executive Order on Improving the Nation's Cybersecurity, Volume 13636. 2021. Available online: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed on 9 June 2023).
8. Federal Bureau of Investigation. Internet Crime Report 2021, Internet Crime Complaint Centre (IC3). 2021. Available online: https://www.documentcloud.org/documents.21504639-fbi-internet-crime-report-2021 (accessed on 9 June 2023).
9. Morgan, S. Cybercrime to Cost the World 10.5 trillion Annually by 2025. Cybercrime Magazine. 2020. Available online: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (accessed on 12 February 2023).
10. Chng, S.; Lu, H.Y.; Kumar, A.; Yau, D. Hacker types, motivations and strategies: A comprehensive framework. *Comput. Hum. Behav. Rep.* **2022**, *5*, 100167. [CrossRef]
11. Cross, M.; Shinder, D.L. *Scene of the Cybercrime*, 2nd ed.; Syngress Pub: Burlington, MA, USA, 2008.
12. Herman, M.; Iorga, M.; Salim, A.M.; Jackson, R.H.; Hurst, M.R.; Leo, R.; Lee, R.; Landreville, N.M.; Mishra, A.K.; Wang, Y.; et al. *NIST IR 8006. NIST Cloud Computing Forensic Science Challenges*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. [CrossRef]
13. Proofpoint. What Is Social Engineering? Definition, Types & More. Available online: https://www.proofpoint.com/us/threat-reference/social-engineering (accessed on 26 June 2023).

14. Turvey, B. Modus operandi, motive and technology. In *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*; Elsevier: Amsterdam, The Netherlands, 2011; pp. 285–304.
15. Dimaggio, J. Ransomware-Centric Collection and Threat Profiling. Analyst1. 2023. Available online: https://analyst1.com/ransomware-centric-collection-and-threat-profiling/ (accessed on 13 March 2023).
16. Dowden, C.; Bennell, C.; Bloomfield, S. Advances in Offender Profiling: A Systematic Review of the Profiling Literature Published Over the Past Three Decades. *J. Police Crim. Psychol.* **2007**, *22*, 44–56. [CrossRef]
17. Fox, B.; Farrington, D.P. What have we learned from offender profiling? A systematic review and meta-analysis of 40 years of research. *Psychol. Bull.* **2018**, *144*, 1247–1274. [CrossRef] [PubMed]
18. Bada, M.; Nurse, J.R.C. Profiling the Cybercriminal: A Systematic Review of Research. In Proceedings of the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 14–18 June 2021; pp. 1–8. [CrossRef]
19. Phillips, K.; Davidson, J.C.; Farr, R.R.; Burkhardt, C.; Caneppele, S.; Aiken, M.P. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sci.* **2022**, *2*, 379–398. [CrossRef]
20. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [CrossRef]
21. Douglas, J.E.; Burgess, A.W.; Burgess, A.G.; Ressler, R.K. *Crime Classification Manual: A Standard System for Investigating and Classifying Violent Crime*; Wiley: Hoboken, NJ, USA, 2013; Available online: https://www.amazon.ca/Crime-Classification-Manual-Investigating-Classifying/dp/1118305051 (accessed on 12 February 2023).
22. Mihas, P. Thematic Analysis—An overview. In *International Encyclopedia of Education*, 4th ed.; Elsevier: Amsterdam, The Netherlands, 2023; Available online: https://www.sciencedirect.com/topics/social-sciences/thematic-analysis (accessed on 15 July 2023).
23. McHugh, M.L. Interrater reliability: The kappa statistic. *Biochem. Medica* **2012**, *22*, 276–282. [CrossRef]
24. Coutourie, L. The computer criminal: An investigative assessment. *FBI Law Enforc. Bull.* **1989**, *58*, 18.
25. Bongardt, S.A. An Introduction to the Behavioral Profiling of COMPUTER NETWORK iNTRUSiONS. *Forensic Exam.* **2010**, *19*, 20–25.
26. Al-Mhiqani, M.N.; Ahmad, R.; Abidin, Z.Z.; Yassin, W.; Hassan, A.; Abdulkareem, K.H.; Ali, N.S.; Yunos, Z. A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations. *Appl. Sci.* **2020**, *10*, 5208. [CrossRef]
27. Madarie, R. Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. *Int. J. Cyber Criminol.* **2017**, *11*, 78–97. [CrossRef]
28. Kirwan, G.; Power, A. *Cybercrime: The Psychology of Online Offenders*; Cambridge University Press: New York, NY, USA, 2013; pp. 21–256. [CrossRef]
29. Chiesa, R.; Ducci, S.; Ciappi, S. *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*, 1st ed.; Auerbach Publications: Boca Raton, FL, USA, 2008.
30. Rogers, M.; Smoak, N.D.; Liu, J. Self-reported Deviant Computer Behavior: A Big-5, Moral Choice, and Manipulative Exploitive Behavior Analysis. *Deviant Behav.* **2006**, *27*, 245–268. [CrossRef]
31. Bachmann, M. The Risk Propensity and Rationality of Computer Hackers. *Int. J. Cyber Criminol.* **2010**, *4*, 643–656.
32. Nykodym, N.; Taylor, R.; Vilela, J. Criminal profiling and insider cyber crime. *Comput. Law Secur. Rev.* **2005**, *21*, 408–414. [CrossRef]
33. Rogers, M.K. A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study. Ph.D. Thesis, University of Manitoba, Winnipeg, MB, Canada, 2001. Available online: https://www.proquest.com/dissertations-theses/social-learning-theory-moral-disengagement/docview/304732918/se-2?accountid=44888 (accessed on 24 April 2023).
34. Rogers, M. The role of criminal profiling in the computer forensics process. *Comput. Secur.* **2003**, *22*, 292–298. [CrossRef]
35. Loper, K. The Criminology of Computer Hackers: A Qualitative and Quantitative Analysis—ProQuest. Unpublished Dissertation, Michigan State University, East Lansing, MI, USA, 2000. Available online: https://www.proquest.com/openview/3587c0a2d0d1a0b1c239fdd26d4e38f9/1?pq-origsite=gscholar&cbl=18750&diss=y (accessed on 9 June 2023).
36. Rogers, M.K. A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digit. Investig.* **2006**, *3*, 97–102. [CrossRef]
37. Zhang, X.; Tsang, A.; Yue, W.T.; Chau, M. The classification of hackers by knowledge exchange behaviors. *Inf. Syst. Front.* **2015**, *17*, 1239–1251. [CrossRef]
38. Warikoo, A. Proposed Methodology for Cyber Criminal Profiling. *Inf. Secur. J. Glob. Perspect.* **2014**, *23*, 172–178. [CrossRef]
39. Becker, J. Who are the computer criminals? *New Sci.* **1980**, *85*, 1198. [CrossRef]
40. Grimes, R.A. 11 Types of Hackers and How They Will Harm You. CSO Online. 2020. Available online: https://www.csoonline.com/article/3573780/11-types-of-hackers-and-how-they-will-harm-you.html (accessed on 9 June 2023).
41. Barber, R. Hackers Profiled—Who Are They and What Are Their Motivations? *Comput. Fraud. Secur.* **2001**, *2001*, 14–17. [CrossRef]
42. Shaw, E.D. The Role of Behavioral Research and Profiling in Malicious Cyber Insider Investigations. *Digit. Investig.* **2006**, *3*, 20–31. Available online: https://www.sciencedirect.com/science/article/pii/S1742287606000090 (accessed on 23 May 2023). [CrossRef]

43. Bissett, A.; Shipton, G. Some human dimensions of computer virus creation and infection. *Int. J. Human-Computer Stud.* **2000**, *52*, 899–913. [CrossRef]
44. McBrayer, J. Exploiting the Digital Frontier: Hacker Typology and Motivation. Master's Thesis, University of Alabama, Tuscaloosa, AL, USA, 2014. Available online: https://www.proquest.com/dissertations-theses/exploiting-digital-frontier-hacker-typology/docview/1562270477/se-2?accountid=44888 (accessed on 24 April 2023).
45. Back, S.; LaPrade, J.; Shehadeh, L.; Kim, M. Youth Hackers and Adult Hackers in South Korea: An Application of Cybercriminal Profiling. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, 17–19 June 2019; pp. 410–413. [CrossRef]
46. Preuß, J.; Furnell, S.M.; Papadaki, M. Considering the potential of criminal profiling to combat hacking. *J. Comput. Virol.* **2007**, *3*, 135–141. [CrossRef]
47. Cayubit, R.; Rebolledo, K.; Kintanar, R.; Pastores, A.; Santiago, A.; Valles, P. A Cyber Phenomenon: A Q-Analysis on the Motivation of Computer Hackers. *Psychol. Stud.* **2017**, *62*, 386–394. [CrossRef]
48. Woo, H.-J. The Hacker Mentality: Exploring the Relationship between Psychological Variables and Hacking Activities. Doctoral Dissertation, University of Georgia, Athens, GA, USA, 2003. Available online: https://esploro.libs.uga.edu/esploro/outputs/doctoral/The-hacker-mentality{-}{-}exploring/9949334952002959 (accessed on 9 June 2023).
49. Palmieri, M.J.H. Decrypting Personality: The Effects of Motivation, Social Power, and Anonymity on Cybercrime. Ph.D. Thesis, University of Massachusetts Lowell, Lowell, MA, USA, 2022. Available online: https://www.proquest.com/dissertations-theses/decrypting-personality-effects-motivation-social/docview/2724700785/se-2?accountid=44888 (accessed on 24 April 2023).
50. Chiu, S.M. Self-Reported Criminal Computer Behavior among University Students in Hong Kong: A Study of Big-Five Personality Traits, Moral Choice, Exploitive Manipulative Behavior, and Addictive Tendencies. Ph.D. Thesis, Alliant International University, Alhambra, CA, USA, 2013.
51. Seigfried-Spellar, K.C.; Villacís-Vukadinović, N.; Lynam, D.R. Computer criminal behavior is related to psychopathy and other antisocial behavior. *J. Crim. Justice* **2017**, *51*, 67–73. [CrossRef]
52. Withers, K.L. A Psychosocial Behavioral Attribution Model: Examining the Relationship between the 'Dark Triad' and Cyber-Criminal Behaviors Impacting Social Networking Sites. Ph.D. Thesis, Nova Southeastern University, Fort Lauderdale, FL, USA, 2019. Available online: https://www.proquest.com/dissertations-theses/psychosocial-behavioral-attribution-model/docview/2208411493/se-2?accountid=44888 (accessed on 3 July 2023).
53. Treadway, K.N. Comparing the Cognitive Abilities of Hackers and Non-Hackers Using a Self-Report Questionnaire. Master's Thesis, Purdue University, West Lafayette, IN, USA, 2017. Available online: https://www.proquest.com/dissertations-theses/comparing-cognitive-abilities-hackers-non-using/docview/1947623946/se-2?accountid=44888 (accessed on 3 July 2023).
54. Virgara, J.L.; Whitten, T. A systematic literature review of the longitudinal risk factors associated with juvenile cyber-deviance. *Comput. Hum. Behav.* **2023**, *141*, 107613. [CrossRef]
55. Young, R.; Zhang, L.; Prybutok, V.R. Hacking into the Minds of Hackers. *Inf. Syst. Manag.* **2007**, *24*, 281–287. [CrossRef]
56. Payne, K.-L.; Russell, A.; Mills, R.; Maras, K.; Rai, D.; Brosnan, M. Is There a Relationship Between Cyber-Dependent Crime, Autistic-Like Traits and Autism? *J. Autism Dev. Disord.* **2019**, *49*, 4159–4169. [CrossRef]
57. Seigfried-Spellar, K.C.; Treadway, K.N. Differentiating Hackers, Identity Thieves, Cyberbullies, and Virus Writers by College Major and Individual Differences. *Deviant Behav.* **2014**, *35*, 782–803. [CrossRef]
58. Kranenbarg, M.W.; Ruiter, S.; van Gelder, J.-L.; Bernasco, W. Cyber-Offending and Traditional Offending over the Life-Course: An Empirical Comparison. *J. Dev. Life-Course Criminol.* **2018**, *4*, 343–364. [CrossRef]
59. Gordon, S.; Ma, Q. Convergence of Virus Writers and Hackers: Fact or Fantasy? Symantec Security Response, White Paper. 2003. Available online: https://silo.tips/download/inside-convergence-of-virus-writers-and-hackers-fact-or-fantasy-symantec-securit (accessed on 9 June 2023).
60. Rogers, M.K.; Seigfried, K.; Tidke, K. Self-reported computer criminal behavior: A psychological analysis. *Digit. Investig.* **2006**, *3*, 116–120. [CrossRef]
61. Preuss, J.; Furnell, S.M.; Lea, S.J. Research in Progress Short Paper: The Adoption of Criminal Profiling for Computer Crime. In Proceedings of the 2004 EICAR Conference, Luxemburg, 1–4 May 2004.
62. Tompsett, B.C.; Marshall, A.M.; Semmens, N.C. Cyberprofiling: Offender profiling and geographic profiling of crime on the Internet. In Proceedings of the Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, Athens, Greece, 5–9 September 2005; pp. 21–24. [CrossRef]
63. Casey, E. The value of behavioral analysis in digital investigations. *Digit. Investig.* **2006**, *3*, 57–58. [CrossRef]
64. Kwan, L.; Ray, P.; Stephens, G. Towards a Methodology for Profiling Cyber Criminals. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, Big Island, HI, USA, 7–10 January 2008; p. 264. [CrossRef]
65. Donato, L. An Introduction to How Criminal Profiling Could Be Used as a Support for Computer Hacking Investigations. *J. Digit. Forensic Pract.* **2009**, *2*, 183–195. [CrossRef]
66. Casey, E.; Turvey, B. Investigative reconstruction with digital evidence. In *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*; Academic Press: London, UK, 2011; pp. 255–284.
67. Lickiewicz, J. Cyber Crime Psychology-Proposal of an Offender Psychological Profile. *Probl. Forensic Sci.* **2011**, *87*, 239–252. Available online: https://arch.ies.gov.pl/images/PDF/2011/vol_87/87_Lickiewicz.pdf (accessed on 23 May 2023).

68. Tennakoon, H. The Need for a Comprehensive Methodology for Profiling Cyber-Criminals. 2011. Available online: http://www.newsecuritylearning.com/index.php/archive/150-the-need-for-a-comprehensive-methodology-for-profiling-cyber-criminals (accessed on 13 May 2023).
69. Long, L. Profiling Hackers | SANS Institute, SANS Institute, White Paper. 2012. Available online: https://www.sans.org/white-papers/33864/ (accessed on 9 June 2023).
70. Donato, L. Profiling cyber offenders. *Cybertalk Mag.* **2014**, *4*, 30–31.
71. Saroha, R. Profiling a cyber criminal. *Int. J. Inf. Comput. Technol.* **2014**, *4*, 253–258.
72. Steel, C. Idiographic Digital Profiling: Behavioral Analysis Based on Digital Forensics. *J. Digit. Forensics Secur. Law* **2014**, *9*, 1. Available online: https://commons.erau.edu/jdfsl/vol9/iss1/1/ (accessed on 31 October 2022). [CrossRef]
73. Rogers, M.K. Psychological profiling as an investigative tool for digital forensics. In *Digital Forensics*; Sammons, J., Ed.; Syngress: Boston, MA, USA, 2016; pp. 45–58. [CrossRef]
74. Zuhri, F. The Profile of a Cybercriminal. Digital Forensic Magazine. Available online: https://digitalforensicsmagazine.com/blogs/wp-content/uploads/2017/05/The-Profile-of-Cybercriminal.pdf (accessed on 23 May 2023).
75. Balogun, A.M.; Zuva, T. Open issues in cybercriminal profiling. In Proceedings of the 2017 1st International Conference on Next Generation Computing Applications (NextComp), Mauritius, 19–21 July 2017; pp. 141–145. [CrossRef]
76. Garcia, N. The Use of Criminal Profiling in Cybercrime Investigations. Master's Thesis, Utica College, New York, NY, USA, 2018. Available online: https://www.proquest.com/dissertations-theses/use-criminal-profiling-cybercrime-investigations/docview/2088464663/se-2?accountid=44888 (accessed on 24 April 2023).
77. Kipane, A. Meaning of profiling of cybercriminals in the security context. *SHS Web Conf.* **2019**, *68*, 01009. [CrossRef]
78. Georgiev, V. Profiling Human Roles in Cybercrime. *Inf. Secur. Int. J.* **2019**, *43*, 145–160. [CrossRef]
79. Spicer, J. Cybercriminal Profiling. *EDPACS* **2019**, *60*, 1–17. [CrossRef]
80. Sutter, O.W. The Cyber Profile: Determining Human Behavior through Cyber-Actions. Ph.D. Dissertation, Capitol Technology University, Laurel, MD, USA, 2020. Available online: https://www.proquest.com/dissertations-theses/cyber-profile-determining-human-behavior-through/docview/2702876139/se-2 (accessed on 24 April 2023).
81. Donato, L.M. Computer Criminal Profiling Applied to Digital Investigations. Ph.D. Thesis, De Montfort University, Leicester, UK, 2021. Available online: https://www.proquest.com/dissertations-theses/computer-criminal-profiling-applied-digital/docview/2685242618/se-2?accountid=44888 (accessed on 22 May 2023).
82. Bednarz, A. Profiling cybercriminals: A promising but immature science. *Netw. World* **2004**, *21*, 46–48.
83. Turvey, B.E. *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*, 2nd ed.; Academic Press: San Diego, CA, USA, 2002.
84. Crimmins, D.M. A Predictive Model for Self-reported Computer Criminal Behavior among College Students. Master's Thesis, Purdue University, West Lafayette, IN, USA, 2015. Available online: https://www.proquest.com/dissertations-theses/predictive-model-self-reported-computer-criminal/docview/1728049327/se-2?accountid=44888 (accessed on 3 July 2023).
85. Pahi, T.; Skopik, F. Cyber Attribution 2.0: Capture the False Flag. *Eur. Conf. Cyber Warf. Secur.* **2019**, *XVIII*, 338–345.
86. Aiken, M.P.; McMahon, C. The Cyberpsychology of Internet Facilitated Organized Crime. Europol Organized Crime Threat Assessment Report (iOCTA). 2014. Available online: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2014 (accessed on 26 June 2023).
87. CC-Driver Project. CC-DRIVER. Available online: https://www.ccdriver-h2020.com/project (accessed on 26 June 2023).
88. Frumento, E.; Freschi, F.; Andreoletti, D.; Consoli, A. Victim Communication Stack (VCS): A Flexible Model to Select the Human Attack Vector. In Proceedings of the 12th International Conference on Availability, Reliability and Security, in ARES '17, Reggio Calabria, Italy, 29 August–1 September 2017; Association for Computing Machinery: New York, NY, USA, 2017. [CrossRef]
89. Somer, T. Taxonomies of Cybercrime: An Overview and Proposal to be Used in Mapping Cyber Criminal Journeys. *Eur. Conf. Cyber Warf. Secur.* **2019**, *XIX*, 475–483.
90. The Council of Europe. *The Council of Europe Cybercrime Convention*; The Council of Europe: Strasbourg, France, 2001. Available online: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed on 9 June 2023).
91. Levy, S. *Hackers: Heroes of the Computer Revolution*, 25th ed.; O'Reilly Media: Sebastopol, CA, USA, 2010. Available online: https://www.amazon.ca/Hackers-Heroes-Computer-Revolution-Anniversary/dp/1449388396 (accessed on 12 February 2023).
92. Wark, M. *A Hacker Manifesto*; Harvard University Press: Boston, MA, USA, 2004. Available online: https://www.amazon.ca/Hacker-Manifesto-McKenzie-Wark/dp/0674015436 (accessed on 12 February 2023).
93. Europol, Europol Spotlight—The Cyber Blue Line. 2021. Available online: https://www.europol.europa.eu/publications-events/publications/europol-spotlight-cyber-blue-line (accessed on 26 June 2023).
94. Davidson, J.; Aiken, M.P.; Phillips, K.; Farr, R. *European Youth Cybercrime, Online Harm and Online Risk Taking: 2022 Research Report*; Institute for Connected Communities, University of East London: London, UK, 2022. Available online: https://www.ccdriver-h2020.com/_files/ugd/0ef83d_a8b9ac13e0cf4613bc8f150c56302282.pdf (accessed on 26 June 2023).
95. Malin, C.H. C32.1Digital Behavioral Criminalistics to Elucidate the Cyber Pathway to Intended Violence. In *International Handbook of Threat Assessment*; Meloy, J.R., Hoffmann, J., Eds.; Oxford University Press: Oxford, UK, 2021. [CrossRef]
96. INDRA. CyberRoad: Development of the CYBER Crime and CYBER Terrorism Research ROADmap. Indra. Available online: https://www.indracompany.com/en/indra/cyberroad-development-cyber-crime-cyber-terrorism-research-roadmap (accessed on 11 June 2023).

97. Victimology Definition & Meaning—Merriam-Webster. Available online: https://www.merriam-webster.com/dictionary/victimology (accessed on 10 June 2023).
98. What Is OSINT (Open-Source Intelligence?). SANS Institute. Available online: https://www.sans.org/blog/what-is-open-source-intelligence/ (accessed on 10 June 2023).
99. Modus Operandi. Criminology. Britannica. Available online: https://www.britannica.com/topic/modus-operandi (accessed on 10 June 2023).
100. MITRE ATT&CK®. Available online: https://attack.mitre.org/ (accessed on 10 June 2023).
101. Connolly, I.; Palmer, M.; Barton, H.; Kirwan, G. *An Introduction to Cyberpsychology*; Routledge: Abingdon, UK, 2016. [CrossRef]