forensic sciences

MDPI

Review

Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies

Kirsty Phillips [1], Julia C. Davidson [1], Ruby R. Farr [1], Christine Burkhardt [2], Stefano Caneppele [2] and Mary P. Aiken [1,*]

[1] Institute for Connected Communities, University of East London, London E15 4LZ, UK; k.phillips@uel.ac.uk (K.P.); j.davidson@uel.ac.uk (J.C.D.); r.farr@uel.ac.uk (R.R.F.)
[2] School of Criminal Justice, University of Lausanne, CH-1015 Lausanne, Switzerland; christine.burkhardt@unil.ch (C.B.); stefano.caneppele@unil.ch (S.C.)
* Correspondence: m.aiken@uel.ac.uk

Abstract: Cybercrime is becoming ever more pervasive and yet the lack of consensus surrounding what constitutes a cybercrime has a significant impact on society, legal and policy response, and academic research. Difficulties in understanding cybercrime begin with the variability in terminology and lack of consistency in cybercrime legislation across jurisdictions. In this review, using a structured literature review methodology, key cybercrime definitions, typologies and taxonomies were identified across a range of academic and non-academic (grey literature) sources. The findings of this review were consolidated and presented in the form of a new classification framework to understand cybercrime and cyberdeviance. Existing definitions, typologies and taxonomies were evaluated, and key challenges were identified. Whilst conceptualizing cybercrime will likely remain a challenge, this review provides recommendations for future work to advance towards a universal understanding of cybercrime phenomena as well as a robust and comprehensive classification system.

Keywords: cybercrime; cyber crime; cyberdeviance; definitions; typology; taxonomy

check for updates

Citation: 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. https://doi.org/10.3390/forensicsci2020028

Academic Editors: Ricardo Dinis-Oliveira, Francisca Alves Cardoso and Pier Matteo Barone

Received: 22 February 2022
Accepted: 7 April 2022
Published: 16 April 2022

1. Introduction

Digital technology and cybercrime are pervasive features of modern life. Approximately 60% of the world's population are internet users and the global adoption of digital technology is rapidly increasing; global internet penetration increased by approximately 7% over the course of one year (from January 2020 to January 2021) [1]. The increased adoption of digital technology has caused an evolution in criminal behavior, resulting in the increased occurrence of 'cybercrime'. However, there continues to be a lack of clarity as to what exactly constitutes a cybercrime.

A clear conceptualization of cybercrime is vital, as even small variations in the conceptualization of cybercrime could affect the measurement of, and response to, cybercrime behaviors [2]. In fact, Barn and Barn [3] argue that one possible factor leading to difficulties in estimating cybercrime is the lack of well-formed definitions and classification systems capable of accounting for the range of cybercrimes. This problem is further compounded by the fact that cybercrime legislation across jurisdictions is neither systematic nor uniform; moreover, the legislation itself is often dispersed across various criminal and civil statutes, which in turn results in fragmented international efforts to tackle cybercrime as well as cybercrimes being weighted and considered differently across jurisdictions [4,5]. Additionally, this is further complicated by the fact that in relation to many individual cybercrimes, there is variability across jurisdictions as to what constitutes a criminal offence. For an example, see the ICMEC's global legislative review of 'Online Grooming' [6].

Problems in defining cybercrime begin with the terminology itself: "A veritable arsenal of terminology is used, sometimes in combination with the prefixes cyber, computer, e-, internet, digital or information. Terms are bandied around, applied randomly, reflect overlap in content or reflect important gaps" (quote from Van der Hulst and Neve [7] (p. 19), cited in Paoli et al. [8]). Alternative terminology for cybercrime includes, for example, 'cyberspace crime'; 'computer crime'; 'computer-related crime'; 'electronic crime'; 'e-crime'; 'technology-enabled crime'; 'high-tech crime' [2,9,10]. The variability in cybercrime terms and language highlights the lack of a shared lexicon amongst professionals working in the field.

Given the current ambiguity surrounding cybercrime as a construct, this paper aims to explore and consolidate cybercrime definitions, typologies and taxonomies found in current academic and grey literature, using a structured literature review methodology. Furthermore, identified definitions, typologies and taxonomies are evaluated, and recommendations are given to advance future work in the field.

Review Methodology

This paper aimed to conduct a broad review of the key definitions, typologies, and taxonomies of cybercrime, as used in academia and industry. A parameterized literature review methodology, appropriate to the research aims and objectives, was utilized; this type of review allows for an examination of current literature, without requiring a complete and comprehensive search, or quality assessment [11]. To maintain a rigorous approach to this review, search parameters were incorporated to approximate a systematic search and accommodate for practical restrictions (e.g., time limitation).

The following parameters were adopted to conduct this literature review:

1. A Boolean search string ((Cybercrime OR "computer crime") AND (definition* OR typology* OR classification* OR categories* OR taxonomy*)) was used to identify sources via an academic search engine, namely Google Scholar;
2. Included sources were English Language publications published from 2017 onwards;
3. The first 100 (when ordered by most relevant) sources were assessed for relevance;
4. Sources were rapidly assessed for relevance according to two stages: firstly, inclusion or exclusion according to the relevance of the title or abstract, and secondly only sources were included when the majority of the content discussed cybercrime definitions and typologies;
5. In addition to the final sample (that meets criteria 1–4), references within said sources were included if highly relevant to the aims and objectives;
6. Meta-analyses, review-type materials, keystone articles, or articles that are highly relevant were prioritized when preparing research findings.

Findings of this review form a narrative and were arranged under three themes [11] (p. 94), according to the following research objectives:

1. To identify key cybercrime definitions from academia and key definitions used by organizations;
2. To identify key cybercrime typologies and taxonomies developed by academics and organizations;
3. To evaluate identified definitions, typologies, and taxonomies of cybercrime, considering the wider implications for policy, practice, and future research.

The search was conducted on 9th June 2020 and identified 38,700 relevant materials. When limited according to pre-defined parameters (as listed above), the final sample was comprised of 23 materials, 10 of which were prioritized based on their quality and relevance. Other highly relevant articles or sources referenced by materials in the final sample have also been included, resulting in 64 sources in total informing this review.

2. Origin of the Term 'Cybercrime'

Various terms have been used to describe 'cybercrime' since the inception of the field, as shown in Table 1, and continue to be used in labelling this phenomenon. The prefix 'cyber' historically originated in cybernetics and had particular meaning within the field. However, as the popularity of technology and the use of technology increased in the 1980s and 1990s, 'cyber' became a buzzword as it became synonymous with almost anything related to computers and the internet, e.g., cyberspace, cybershopping, and cybersurfing [12].

Table 1. Cybercrime terminology in the periods 1995–2000 and 2001–2018.

	Number of Occurrences	
Terminology	**1995–2000**	**2001–2018**
Cybercrime	1476	28,100
Cyber crime		17,900
Computer crime	2760	19,000
E crime	585	15,800
Internet crime	236	7500
Digital crime	50	3830
Online crime	49	3120
Virtual crime	43	1100
Techno-crime	19	55
Netcrime	17	216

Note. Copyright 2020 by Routledge, from McGuire, M. It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In *The Human Factor of Cybercrime*; Leukfeldt, R., Holt, T.J., Eds.; Routledge: New York, NY, USA, 2020; p. 8 (Table 1.1 and 1.2). Reproduced by permission of Taylor and Francis Group, LLC, a division of Informa plc.

Early in the field, the dominant term for the misuse of information technology was 'computer crime', or 'crime by computer' and this persisted up until approximately the year 2000 [2,13]. Over time the positive associations of the prefix 'cyber' dropped away as the use of 'cyber' in relation to everyday activities was abandoned; ultimately, only the negative connotations remained, as the term 'cyber' continued to be used in relation to harmful or illicit activities (e.g., cybercrime, cyberbullying, cyberterrorism, and cyberstalking) [12]. Therefore, the predominant descriptive term is now the single-word configuration 'cybercrime' closely followed by the two-word configuration 'cyber crime' [12], as shown in Table 1; thus, "regardless of its merits or demerits the term 'cybercrime' has entered the public parlance and we are stuck with it" [14] (p. 11). Therein lies a fundamental problem, namely a lack of a systematic and reasoned approach in defining and labelling cybercrime.

Cybercrimes include a diverse set of offences and harmful behaviors; the content of Table 2 provides an indicative list of cybercrime offences and cyberdeviant acts, partly informed by the list collated by Tsakalidis and Vergidis [15] (p. 710). This illustrates the range of crimes that fall under this umbrella term, including a combination of traditional crimes as well as crimes unique to the cyber landscape. Notably, no sources identified in this review provided an exhaustive list of known cybercrimes. This is likely to be in part due to the diverse set of behaviors that fall under this term, but also because the phenomenon is continuously evolving, and the field is rapidly expanding.

Table 2. An illustrative list to demonstrate the scope of cybercrime offences and cyberdeviant acts.

Botnets
CSAM/CSE
Coercion
Computer-related forgery
Computer-related fraud
Copyright infringements
Criminal communications
Cyber troops
Cyberbullying
Cyberfraud
Cyberwarfare
Grooming
Harassment
Hate speech
Heist
Identity theft
Illegal access (hacking/cracking)
Illegal data acquisition
Illegal gambling
Illegal gaming
Illegal interception
Image based abuse
Pornographic material
Radicalisation
Ransomware
Religious offenses
Sex tourism
Sex trade
Sex trafficking
Sexting
Sextortion
Spam
Stalking

Table 2. *Cont.*

Data interference	Inciting violence	System interference
Deep fakes	Laundering	Terrorism
Digital piracy	Misuse of devices	Trademark related offenses
Drug trade	Money muling	Trolling
Espionage	Phishing	Xenophobia
Extortion (e.g., Romance Fraud)	Political interference	

Table Abbreviations: Child sexual abuse material (CSAM); child sexual exploitation (CSE).

3. Definitions of the Term 'Cybercrime'

A principal finding of this review, and the only consensus within the literature, is that there is no single clear, precise and universally accepted definition of cybercrime [4,5,8,10,16–18]: a fact that is acknowledged by both academics and organizations alike [5,8,17,19]. Additionally, the articles in this review did not identify a jurisdiction in the world that has a specific single offence of 'cybercrime' [2,20]. Therefore, the veracity of working cybercrime definitions continues to be debated in academic literature.

3.1. A Single Term to Encapsulate a Diverse Set of Criminal and Harmful Behaviors

'Cybercrime' encompasses a wide number of acts, crimes or illicit conduct perpetrated by both individuals or groups against computers, computer-related devices, or information technology networks, as well as traditional crimes that are facilitated or maintained by the use of the internet and/or information technology [16] (p. 403). Therefore, even though there is no single agreed-upon and unified definition of cybercrime, it is broadly acknowledged that the term is used to account for a variety of crimes and harmful behaviors. Wall [20] (p. 3) defines cybercrime as "the occurrence of a harmful behavior that is somehow related to a computer," and whilst such definitions are arguably too broad and imprecise, they are, however, essentially correct.

3.2. Most Frequently Cited Definitions of the Term 'Cybercrime'

According to a recent literature review by Akdemir, Sungur, and Başaranel [18], the two most commonly cited academic definitions of cybercrime have been put forward by Thomas and Loader [21] and Gordon and Ford [22]. Thomas and Loader (in 2000) define cybercrime as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks" [21] (p. 3), whereas Gordon and Ford (in 2006) define cybercrime as "any crime that is facilitated or committed using a computer, network, or hardware device" [22] (p. 14).

3.3. Institutional and Organizational Definitions of the Term 'Cybercrime'

At an organizational level, there are differences globally in cybercrime definitions, as demonstrated by the definitions included in Table 3. Furthermore, some organizations do not provide any definition of cybercrime. For example, the U.S. Government does not provide an official definition of cybercrime which would enable cybercrime to be distinguished from other common criminal offences or other forms of cyberthreats (e.g., cyber warfare or cyberterrorism) [15]. Table 3 provides an overview of the various definitions of cybercrime currently used by key European and international organizations; the table highlights the differing uses of terminology and cybercrime concepts. It is important to note that, arguably, most of the definitions identified here refer to cybersecurity crimes and do not adopt the broad interpretation of 'cybercrime' as defined in academic literature.

Table 3. Organizational definitions of cybercrime.

Year	Organization	Definition of Cybercrime
1994	The United Nations	"The United Nations manual [23] on the prevention and control of computer-related crime (1994) uses the terms, computer crime and computer-related crime interchangeably. This manual did not provide any definition" [18] (p. 116)
2000	The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders	1. "any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them." 2. "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network" [24] (p. 5)
2001	The Council of Europe Cybercrime Convention (also known as The Budapest Convention)	"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 criminalisation of such conduct" [25] (p. 2)
2007	The Commission of European Communities	"criminal acts committed using electronic communications networks and information systems or against such networks and systems" [26] (p. 2)
2013	Shanghai Cooperation Organization (SCO) Agreement	"the use of information resources and (or) the impact on them in the informational sphere for illegal purposes" (cited in Malby et al. [27] (p. 15))
2013	Cybersecurity Strategy of the European Union	"a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target" [28] (p. 3)
2016	Commonwealth of Independent States Agreement	"a criminal act of which the target is computer information" (cited in Akhgar et al. [29] (p. 298))

Note. Text definitions were collated by Akdemir, Sungur, and Başaranel [18].

4. Categorizing or Developing 'Typologies' of Cybercrime

As demonstrated in the previous section, single definitions of the term 'cybercrime' are often overly reductive, lack utility and are limited in terms of conveying a comprehensive understanding of the concept of 'cybercrime'; therefore, more popularly used definitions of cybercrime refer to categorizations of cybercrime. This section explores such classification systems that define cybercrimes according to two ('dichotomies') or three ('trichotomies') categories.

4.1. Dichotomies of Cybercrime

This section discusses the two-category ('dichotomies') classifications identified in this review. These broad classifications separate cybercrimes based on the role that technology plays in the commission of the crime or act; therefore, across all typologies identified in this review, the role of technology is the key feature by which cybercrimes are categorized [2,16].

4.1.1. Categorical Approach: 'Cyber-Enabled' vs. 'Cyber-Dependent' Crime

The categorization system that distinguishes between 'cyber-enabled' and 'cyber-dependent' crime is the most widely used and has been consistently adopted by researchers and policy makers [8,10,30]. This two-factor categorization is based on a definition originally put forward by Brenner in 2007 [31], in which specific cyber offences were distinguished from so-called real-world crime migrating into cyberspace.

Cyber-dependent crimes are crimes that arose with the advent of technology and cannot exist (i.e., dependent) outside of the digital world, e.g., hacking, such as ransomware attacks or hacktivism [30]. To add to the definitional complexity, different authors use different terminology to describe this same category. Alternative terminology includes 'computer-focused crimes' [32], 'computer-crime' [17], or 'technological crime' [4]. In contrast, cyber-enabled crimes are traditional crimes that predate the advent of the technology, and are now facilitated or have been made easier (i.e., enabled) by cyber technology. Cyber-enabled crimes range from white-collar crime to drug trafficking, to online harassment, terrorism [30] and beyond. Alternative terminology for this category includes 'computer-assisted crimes' [32], 'computer-related' [17], or 'people crime' [4].

This categorization system (distinguishing between cyber-dependent vs. cyber-enabled crimes) dominates the field; therefore, different categorizations that make distinctions based on alternative dimensions are less popular. This review identified one other example of a two-category classification system, where the defining property was the motive behind the criminal act: 'interpersonal cybercrime' (i.e., personal attacks) vs. 'property cybercrime' (i.e., where the primary motive is financial gain) [4,33].

4.1.2. Continuum Approach: Type I to Type II as Proposed by Gordon and Ford

An alternative two-factor classification system is the spectrum approach proposed by Gordon and Ford in 2006 [22]; this is the only system identified within this review that conceptualizes cybercrimes as being on a spectrum. Gordon and Ford [22] proposed that Type I and Type II cybercrimes represent the opposite ends of a cybercrime spectrum.

Type I cybercrimes are considered to be more technical in nature, for example, hacking, similar to 'cyber-dependent' crimes as described above. In contrast, Type II cybercrimes are generally considered to involve more human contact, for example, online gambling, similar to 'cyber-enabled' crimes as described above [10,22]. Therefore, there is some broad agreement between the categorical approach and the spectrum approach as to what the two factors are, and what the defining characteristic ought to be, namely to what extent technology is integral to the commission of the crime.

Crucially, however, Gordon and Ford [22] stress that cybercrimes should not be conceptualized as being one category or another; rather, Type I and Type II represent opposite ends of a continuum. The continuum or spectrum-type approach is supported by other recent work in this area; for example, see Davidson et al. [34] for a discussion of how online harassment and image-based abuse represent a spectrum of online harms (online harms are online behaviors or content that cause harm, but may not be illegal in all circumstances [35]). Future classification systems within this field could conceptualize cybercrimes as existing on a spectrum, and could also consider the use of multiple dimensions, including the role of technology (in agreement with Gordon and Ford's [22] system) or links to traditional crime, as well as alternative dimensions, for example, the severity of the act, the motivation of the perpetrator, or the context in which the crime was committed.

4.2. Trichotomies of Cybercrime

This section discusses the three-category ('trichotomies') classifications identified in this review. The trichotomies presented here adopt two different approaches: by either proposing a new three-factor classification of cybercrime based on the role of technology in a criminal act (similar to the above dichotomies) or by seeking to extend the above dichotomies with an additional category.

4.2.1. Categorization Systems That Define Three Categories of Cybercrimes

The Wall 2007 [14] three-category classification system was one of the first reported in academic literature and is therefore often cited (e.g., see Viano [5], Tsakalidis and Vergidis [15], and Tsakalidis, Vergidis and Madas [36]). However, the two-category classification system ('cyber-enabled' vs. 'cyber-dependent' crime, as described above) is the most widely used having been adopted by both researchers and policy makers [8,10,30]. Wall's [14] classification system distinguishes between:

1. 'Crimes against the machine', also known as computer integrity crimes, e.g., hacking, cracking and Denial of Service (DoS)/Distributed Denial of Service (DDoS);
2. 'Crimes using the machine', also known as computer-assisted crimes, e.g., piracy, robberies and scams;
3. 'Crimes in the machine', also known as computer content crimes, e.g., online hate, harassment, pornography.

The same three-category distinction was also adopted a few years later in 2013 by The European Commission [37] (pp. 3–4). However, the specific terminology used differs from that of Wall [14], e.g., rather than 'crimes against the machine' or 'computer integrity crime', the first category is described as 'offences unique to computers and information systems.' The European Commission [37] uses the following terminology to describe the same three categories:

1. 'Offences unique to computers and information systems (e.g., attacks against information systems, denial of service and malware)', i.e., analogous to Wall's [14] computer integrity crimes;
2. 'Traditional offences (e.g., fraud, forgery, and identity theft)', i.e., analogous to Wall's [14] computer-assisted crimes;
3. 'Content-related offences (e.g., online distribution of CSAM or incitement to racial hatred)' i.e., analogous to Wall's [14] computer content crimes.

Across the approaches described so far, there is agreement on the first category of cybercrime (labelled: 'cyber-dependent' crime; 'Type I' cybercrimes; 'computer integrity crime'; or 'offences unique to computers and information systems'). However, the three-category classification systems are arguably advantageous over two-category approaches as there is a greater appreciation of the breadth of behaviors that are encompassed within the category of 'cyber-enabled' crimes (as described in the previous section), defined here as constituting two new distinct categories that distinguish between crimes against property and crimes against people.

4.2.2. Extending Dichotomies of Cybercrime to Trichotomies

This review also identified two examples in academic literature where the two-category classification systems (as described in the previous section) were extended to form a three-category classification system; however, these are more recent, less popular and not widely adopted.

In the first example, Wall [38] (also cited in McGuire [2]) proposed an extension of the two-factor categorical approach (distinguishing between 'cyber-dependent' vs. 'cyber-enabled' crimes), the approach most popular in the field and commonly used by academics, institutions and policy makers. To extend this classification, Wall [38] adds a third category of 'cyber assisted crimes', to account for the pervasive, yet incidental, role of technology in the operation of crime. Therefore, Wall [38] proposes a three-category classification system distinguishing between:

1. Cyber-dependent crimes or true cybercrimes, where the computer is the target and the crime could not happen without a computer, i.e., truly new opportunities for crime, e.g., hacking, malware, and DoS/DDoS;
2. Cyber-enabled crimes or hybrid crimes, where the computer plays a role, but the crime could still be committed without the involvement of the computer, i.e., new opportunities for traditional crime, e.g., frauds, scams, and phishing;
3. Cyber-assisted crimes or the use of computers in traditional crime, where the computer's involvement is incidental to a real-world crime and simply increases the opportunity for traditional crimes, e.g., criminal communications.

The second example, proposed by Sarre, Lau, and Chang [10], extends Gordon and Ford's [22] two-factor spectrum approach (where Type I and Type II represent opposite ends of the continuum) with 'Type III' crimes to account for the use of advanced technology in the commission of crimes. Therefore, Sarre, Lau, and Chang [10] propose a three-factor spectrum system where:

1. Type I cybercrimes refer to crimes that are technical in nature (e.g., hacking);
2. Type II cybercrimes refer to crimes that involve human contact (e.g., cyberbullying);
3. Type III cybercrimes refer to crimes that are perpetuated by Artificial Intelligence, robots/bots or self-learning technology.

Interestingly, these two approaches extend the two-factor systems (discussed in the previous section), but these extensions are at opposite ends of cybercrime concepts: one end being the use of advanced self-learning technology in the commission of crimes and the other end being where the use of technology is least integral in the commission of a crime. This is indicative of the broad interpretation of cybercrime among those working in the field.

5. Taxonomies of 'Cybercrime'

This section explores key taxonomies identified by this review. It is acknowledged that an exhaustive review would identify further taxonomies. However, the taxonomies included here are the commonly referenced attempts to comprehensively classify cybercrimes and are sufficient to identify overlaps and gaps and to assess the literature landscape.

5.1. The Council of Europe's Convention of Cybercrime (2001)

The Council of Europe's (COE) Convention of Cybercrime [25], also known as The Budapest Convention, is the single most important classification system as it represents "the only globally recognized agreement around cybercrime" [2] (p. 19); this ratified instrument, for cybercrime prevention, classified specific offences under four distinct categories as shown in Table 4. This taxonomy was supplemented by an Additional Protocol [39] which saw the inclusion of category 5 pertaining to the criminalization of racist and xenophobic acts using a computer system (also shown in Table 4).

Table 4. Table summarizes the cybercrime typology described by The Council of Europe's 2001 Convention of Cybercrime (also known as The Budapest Convention) with the addition of category 5 in 2003 [39]. In total this five-category classification system contains 14 different cybercrime offences.

Category 1	Category 2	Category 3	Category 4	Category 5
Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems	**Computer-Related Offences**	**Content-Related Offences**	**Offences Related to Infringements of Copyright and Related Rights**	**Acts of a Racist and Xenophobic Nature Committed through Computer Systems**
Article 2—Illegal access Article 3—Illegal interception Article 4—Data interference Article 5—System interference Article 6—Misuse of devices	Article 7—Computer-related forgery Article 8—Computer-related fraud	Article 9—Offences related to child pornography	Article 10—Offences related to infringements of copyright and related rights	Article 3—Dissemination of racist and xenophobic material through computer systems Article 4—Racist and xenophobic motivated threat Article 5—Racist and xenophobic motivated insult Article 6—Denial, gross minimization, approval or justification of genocide or crimes against humanity Article 7—Aiding and abetting

Other law enforcement agencies beyond Europe have used an alternative offence-based framework to identify cybercrime statutes; for example, the U.S Department of Justice Computer Crime and Intellectual Property Section Criminal Division [40] introduced a substantially larger framework that includes a broad range of offence types. However, this framework does not constitute a taxonomy, and is therefore outside the scope of this review; rather, the framework lists 'unlawful online conduct', i.e., cybercrimes, and identifies applicable legal statutes (for a summary, see [40] (pp. 149–155)).

Furthermore, included here to illustrate how law enforcement frameworks conceptualize cybercrime, the European Union's Directive 2013/40/EU [41], shown in Table 5, established the minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It is key to note that this framework only includes security-based offences, and considerably overlaps with category 1 of the Council of Europe's Convention of Cybercrime classification system (Table 4, first column); it, therefore, does not constitute a comprehensive taxonomy of cybercrime.

Table 5. Table summarizes The European Union's Directive [41], which describes the definition of criminal offences and sanctions in the area of attacks against information systems.

The European Union's Directive (2013) in Categorizing Cybercrime
Article 3—Illegal access to information systems
Article 4—Illegal system interference
Article 5—Illegal data interference
Article 6—Illegal interception
Article 7—Tools used for committing offences
Article 8—Incitement, aiding and abetting and attempt

Tsakalidis and Vergidis' (2017) Update of the COE's Convention of Cybercrime (2001) Taxonomy

In a recent article, Tsakalidis and Vergidis [15] adopt the COE's Convention of Cybercrime [25] Taxonomy to underpin their new classification framework. Therefore, Tsakalidis and Vergidis' [15] taxonomy (see Table 6) closely mirrors that of the COE's Convention of Cybercrime [25] classification system, as acknowledged by the authors, but with a few key alterations. These alterations include the addition of 'Illegal data acquisition' under Type A (or 'Category 1′) offences, 'Identity theft' under Type B (or 'Category 2′) offences, 'Trademark-related offences' under Type D (or 'Category 4′) offences and 'Racism and hate speech on the internet' is subsumed into Type C (or 'Category 3′) offences, rather than separated as an individual category. Tsakalidis and Vergidis [15] make significant alterations to Type C (or 'Category 3′) offences (adding 6 other content-related offences to include pornographic material, religious offences, cyberbullying, illegal gambling and online games, spam and related threats, and racism and hate speech on the internet). Tsakalidis and Vergidis [15] also propose the addition of Type E or 'combinational offences' to include "acts that combine a number of different offences in sole acts" [15] (p. 716).

Table 6. Tsakalidis and Vergidis' taxonomy.

Type A	Type B	Type C	Type D	Type E
Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems	**Computer-Related Offences**	**Content-Related Offences**	**Offences Related to Infringements of Copyright and Related Rights**	**Combinational Offences**
A1. Illegal access (hacking, cracking) A2. Illegal data acquisition (data espionage) A3. Illegal interception A4. Data interference A5. System interference A6. Misuse of devices	B1. Computer-related forgery B2. Computer-related fraud B3. Identity theft	C1. Pornographic material C2. CSAM/CSE C3. Religious offences C4. Cyberbullying C5. Illegal gambling and online games C6. Spam and related threats C7. Racism and hate speech on the internet	D1. Copyright-related offences D2. Trademark-related offences	E1. Phishing E2. Cyber laundering E3. Cyberwarfare E4. Terrorist use of the internet

Note. Copyright 2017 IEEE. Reprinted, with permission, from Tsakalidis, G.; Vergidis, K. A systematic approach toward description and classification of cybercrime incidents. IEEE Trans. Syst. Man Cybern. Syst. 2017, 49(4), 710–729; p.716 (Table VI). Table Abbreviations: Child sexual abuse material (CSAM); Child sexual exploitation (CSE).

5.2. Wall's (2001) Taxonomy: An Alternative Framework Popular in Academic Literature

Wall's [20] early taxonomy (see Table 7) was one of the first attempts to develop a taxonomy and is frequently cited in academic literature (e.g., see Viano [5] and McGuire [2]); incidentally, this taxonomy coincides with the period during which the Council of Europe's Convention of Cybercrime [25] classification system was being developed. However, the two classification systems differ considerably, and it is important to note that all of the academic frameworks identified within this review diverge from an offence-based framework. The COE's Convention of Cybercrime Taxonomy [25] is an example of an offence-based framework; this taxonomy has greater focus and delineates different offences in relation to cyber security, fraud, forgery and copyright infringement. In contrast, Wall's [20] four-category taxonomy is equally weighted in relation to person-target and computer-target-based offences. Wall's [20] taxonomy also differentiates between two types of content-based offences, sexual violence online and online harassment or hate offences, unlike the COE's Convention of Cybercrime [25] Taxonomy. However, as demonstrated in a recent review, see Davidson et al. [34], the scope of online harms is even greater than accounted for in Wall's [20] early typology.

Table 7. Table summarizes the four-category typology as described in Wall [20].

Cyber-Trespass	**Cyber-Deception/Theft**	**Cyber-Pornography and Obscenity**	**Cyber-Violence**
Defined as the crossing of virtual ownership boundaries, e.g., attempting to gain access to systems, networks or data. Offences: Hacking	Defined as the use of ICT to either steal information or valuable items. This is typically achieved by cyber-trespass. Offences: Hacking, piracy, spam	Defined as the use of ICT to access sexually explicit and illegal sexual content. Offences: Pornography, CSAM/CSE, sex trade, sex tourism, sex trafficking	Defined as causing harm in both virtual and real-life environments. Offences: Online harassment, bullying, terrorism, politically motivated hacking, organized crime

Note. This typology was cited in Viano [5] (pp. 5–7) and McGuire [2] (p. 18). Table Abbreviations: Child sexual abuse material (CSAM); child sexual exploitation (CSE); information communication technology (ICT).

Marcum and Higgins' (2019) Taxonomy: Another Example of an Alternative Framework Found in Academic Literature

Marcum and Higgins' (2019) [42] taxonomy is another example of a cybercrime taxonomy identified in academic literature that also diverges from the COE's Convention of Cybercrime [25] Taxonomy. This taxonomy is a five-category classification system (shown in Table 8). Marcum and Higgins [42], similar to Wall's [20] taxonomy, also place greater emphasis on person-target-based offences by including categories for sexual violence online and online harassment, although importantly online hate acts are not included in this example. However, unlike the other taxonomies identified in this review, Marcum and Higgins [42] further distinguish between different subtypes of hacking and cyberbullying, demonstrating that even single cybercrime offences encompass a broad range of behaviors.

5.3. Taxonomies of Single Offences or Single 'Types' of Cybercrime

Taxonomies of certain types of cybercrime have been developed; see Aiken, Davidson and Amann [43] and Broadhead [17] for a review of the different offences related to hacking (i.e., security-based offences) and the Luxembourg Guidelines (also known as 'The Terminology Guidelines for the protection of children from sexual exploitation and sexual abuse') [44] describes the different types of offences related to child sexual exploitation (CSE) and abuse (CSA). However, these taxonomies are excluded from this review as they do not represent or claim to be a comprehensive taxonomy of all cybercrime behaviors.

Table 8. Table summarizes the five-category typology described in Marcum and Higgins [42] (pp. 460–467).

1	2	3	4	5
Cyberbullying and Cyberstalking	**Digital Piracy**	**Hacking and Malware**	**Identity Theft**	**Sex-Related Crimes Online**
Cyberbullying (5 types): 1.Denigration; 2. Exclusion; 3. Flaming; 4. Harassment; 5. Outing. Cyberstalking Cyber dating abuse	Digital Piracy	Hacking (6 types): 1. Accessing a computer system without permission; 2. Development or use of viruses; 3. Destruction or altering of a computer file without permission; 4. Theft of services; 5. Fraudulent use of a credit card; 6. Infiltration of software. Malware	Identity Theft	Sexual solicitation Grooming Sexting CSAM Revenge porn Sextortion

Table Abbreviations: Child sexual abuse material (CSAM).

6. Consolidating Findings: A New Cybercrime and Cyberdeviance Classification Framework

The typologies and taxonomies of this review have been collated to form a new classification framework of cybercrime and cyberdeviance (including online harms). Cyberdeviance refers to deviant online behaviors which violate societal norms and may or may not overlap with cybercrimes, and therefore describes a broader set of harmful online behaviors [45] (pp. 17–18). The inclusion of the concept of cyberdeviance circumvents the issue of variability in cybercrime legislation across different jurisdictions.

The purpose of this new framework is to map and facilitate discussion and analysis of the many inter-related topics and dynamics included under the umbrella term of 'cybercrime,' along with a range of harmful behaviors online that are not necessarily legislated against at present (i.e., cyberdeviant behaviors).

As shown in Figure 1, there is the overarching spectrum from technology-based crimes (Type I) to human contact crimes (Type I I), or where the use of technology is incidental; future and more technologically advanced (Type I II) crimes are represented by the extension to 'Type I'. There is also the overarching division between cyber-dependent and cyber-enabled crimes. These overarching categories are then further subdivided into subcategories (I–VI); I = 'Crimes against the machine', II = 'Crimes using the machine', III = 'Crimes in the machine' or content-based offences, IV = 'Incidental technology use', V = 'Organized crime, Deep Web markets, Illegal virtual marketplaces and Cybercrime-as-a-Service', and VI = 'Information and behavioral manipulation'. The last two categories cut across multiple other categories as well as being stand-alone, hence why these are represented differently. Under this framework of cybercriminal and cyberdeviant acts, there are eight subtypes, three of which are further subdivided (A/B).

This new classification framework of cybercrime and cyberdeviance is informed by scientific advances in established disciplines such as psychology and criminology, and by findings from emerging disciplines such as forensic cyberpsychology, described as follows; "*Cyberpsychology is the study of adverse effects on human mind and behavior due to its interaction with cyberspace, and its application in court of law for the administration of justice is called Forensic Cyberpsychology*." (See Pradeep K P. Forensic Cyberpsychology in Pandemic Period. *Journal of Forensic Sciences & Criminal Investigation*. 2020; *14(3)*: 555887. DOI: 10.19080/JFSCI.2020.14.555887. (p. 33).) The proposed framework allows for flexibility; for example, new groupings have been included that were not found within this review, e.g., attacks against data and systems owned by nations or states, mass information manipulation and organized crime. The framework reads left to right from technical to human (top of figure); the corresponding 'solutions' context also reads from left to right (bottom row of the figure) from existing cyber security measures to cyber safety measures offered by the emerging online safety technology or ‘SafetyTech’ sector [46].

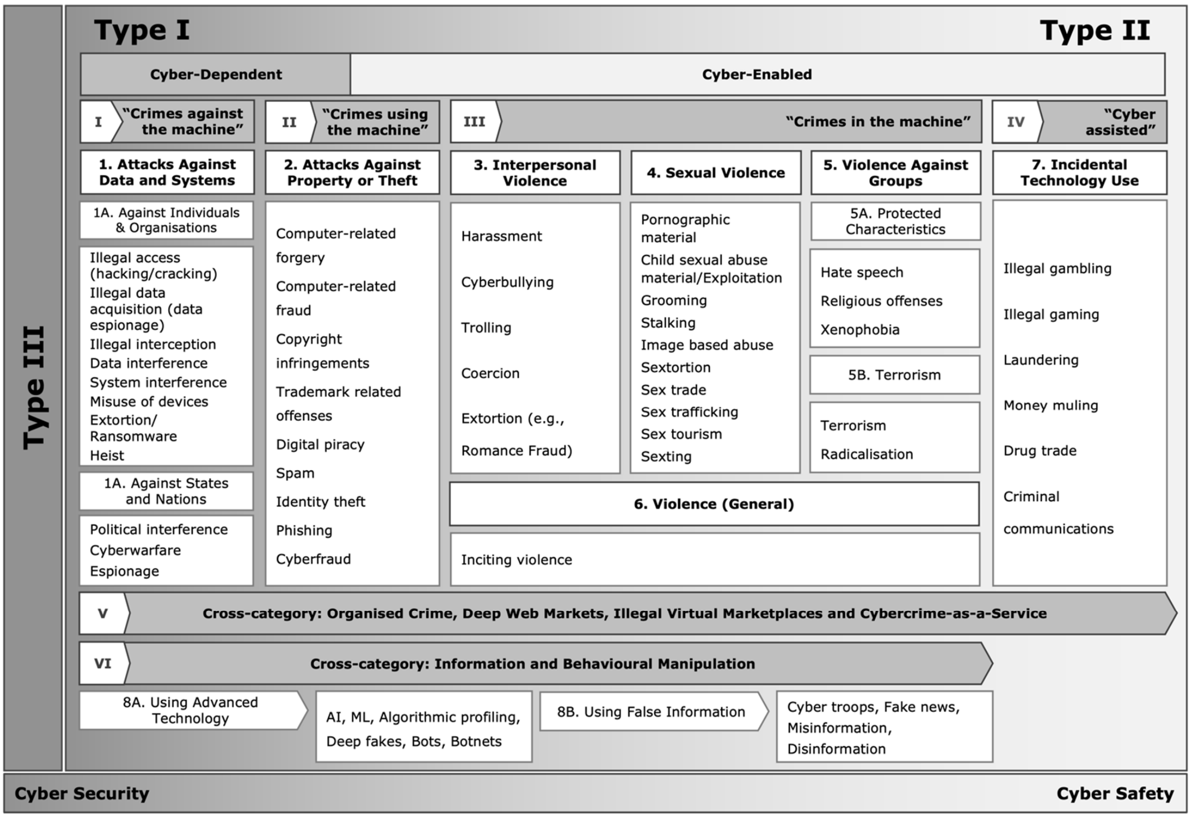
Type I
Type II
Type III
Cyber-Dependent
Cyber-Enabled
I “Crimes against the machine”
II “Crimes using the machine”
III “Crimes in the machine”
IV “Cyber assisted”
1. Attacks Against Data and Systems
2. Attacks Against Property or Theft
3. Interpersonal Violence
4. Sexual Violence
5. Violence Against Groups
7. Incidental Technology Use
1A. Against Individuals & Organisations
Illegal access (hacking/cracking)
Illegal data acquisition (data espionage)
Illegal interception
Data interference
System interference
Misuse of devices
Extortion/ Ransomware
Heist
1A. Against States and Nations
Political interference
Cyberwarfare
Espionage
Computer-related forgery
Computer-related fraud
Copyright infringements
Trademark related offenses
Digital piracy
Spam
Identity theft
Phishing
Cyberfraud
Harassment
Cyberbullying
Trolling
Coercion
Extortion (e.g., Romance Fraud)
Pornographic material
Child sexual abuse material/Exploitation
Grooming
Stalking
Image based abuse
Sextortion
Sex trade
Sex trafficking
Sex tourism
Sexting
5A. Protected Characteristics
Hate speech
Religious offenses
Xenophobia
5B. Terrorism
Terrorism
Radicalisation
6. Violence (General)
Inciting violence
Illegal gambling
Illegal gaming
Laundering
Money muling
Drug trade
Criminal communications
V Cross-category: Organised Crime, Deep Web Markets, Illegal Virtual Marketplaces and Cybercrime-as-a-Service
VI Cross-category: Information and Behavioural Manipulation
8A. Using Advanced Technology
AI, ML, Algorithmic profiling, Deep fakes, Bots, Botnets
8B. Using False Information
Cyber troops, Fake news, Misinformation, Disinformation
Cyber Security
Cyber Safety

Figure 1. A new cybercrime and cyberdeviance classification framework to consolidate the findings of this review.

7. Evaluating Identified Definitions, Typologies and Taxonomies

Crime phenomena are typically conceptualized according to two dimensions, the behavioral and definitional: “There is, therefore, always a dual problem of explanation—that of accounting for the behavior as behavior, and equally important, accounting for the definitions by which specific behavior comes to be considered crime or non-crime” [47] (p. vi). This tension is explored within the following sections of this review.

7.1. An Evaluation of Cybercrime Definitions

A key finding of this review is the lack of a single commonly accepted cybercrime definition [4,5,8,10,16–18], a fact that has resulted in various working definitions being put forth by academics, institutions, and industry [5,15]. However, these working definitions are domain specific and arguably therefore not objective [2,36,48]. Additionally, the literature in this field is dominated by the Global North [10], making working definitions Western centric as opposed to globally applicable.

It has been explored within this review that the problems in establishing a definition for the term ‘cybercrime’ manifest as follows: firstly, various terms are used to describe the same phenomena, and secondly the diverse set of offences that constitute ‘cybercrime.’ Therefore, single definitions that try to encapsulate the term ‘cybercrime’ are often overly reductive, lack utility and are limited in conveying a comprehensive understanding of the concept of ‘cybercrime’; therefore, it would appear that the more popularly used definitions of cybercrime are those that refer to broader categorizations (typologies or taxonomies) of cybercrime.

7.2. An Evaluation of Cybercrime Typologies

Simple categorizations of cybercrime (two-category and three-category classification systems) are broadly similar. Two-factor categorization and spectrum classification systems ('cyber-dependent' or 'Type I' vs. 'cyber-enabled' or 'Type II) demonstrate agreement between what the opposing categories or ends of the spectrum ought to be, with the defining characteristic being whether or not the crime is dependent on the use of technology. The two-factor categorical approach (using the terms 'cyber-dependent' and 'cyber-enabled') is dominant in the field, as the most popularly and consistently used approach by various professionals in this sphere. This may be due in part to the fact that this approach makes a simple but clear distinction between types of cybercrimes.

Three-category classification systems either extend the pre-existing two-factor classification systems or further differentiate between behaviors that are encompassed under 'cyber-enabled' crime. The latter approach further differentiates between traditional offences that can be committed online, by distinguishing between offences against property online (including piracy or identity theft) and offences against people (including hate, harassment and sexual violence). However, in both examples of the latter approach, the terminology used for this final category is 'content based' crimes, which implies the exclusion of offences that can lead to contact (e.g., online grooming). This final category should perhaps be conceptualized more generally to encompass all offences against people, as demonstrated in Figure 1.

Alternatively, in the former approach, extensions of the two-factor classification systems increase the range at opposite extremes (from the role of advanced self-learning technology to where the role of technology is most incidental in the commission of the crime). However, both extensions reflect the likely future of cybercrime behaviors; arguably most crimes will become assisted by some form of technology in the future and as technology continues to advance, the role of complex technologies in the commission of crimes needs to be considered. Currently, both of these extremes are largely unaccounted for by other definitions, typologies or taxonomies, and the divergence between the two extremes is arguably also indicative of the lack of common understanding as to what constitutes cybercrime among those working in the field.

7.3. An Evaluation of Cybercrime Taxonomies

The premise of institutional conventions and treaties, forming frameworks such as the COE's Convention of Cybercrime [25] Taxonomy and the European Union's Directive 2013/40/EU [41], is to implement a comprehensive and unified framework of legal principles which subsequently represents a robust taxonomy of offences associated with cybercrime. However, as this review affirms, a complete classification framework of cybercrime has not yet been developed by institutions or academia; each approach has identifiable gaps and each approach weighs cybercrimes differently. The taxonomies identified here illustrate the extent of the variation between prominent and most up-to-date classifications in academic literature and in use by law enforcement organizations, and evidence that the scope of cybercrimes is even greater than accounted for in current typologies (addressed by the broad scope as shown in Figure 1).

To effectively classify existing and emerging cybercriminal behaviors, a comprehensive framework is essential, one that is compatible with international and national legislation or policies, the work of the public and private cybersecurity sectors, and can accommodate future research findings as cybercrime continues to evolve [8]. Difficulty in classifying cybercrimes hinders the introduction of cybercrime-specific laws and regulations, which leads to significant challenges in policing and prosecuting cybercrime due to the limited understanding and capacity to respond [18].

8. Key Challenges

8.1. Problems with Prioritizing Response over Definitions

Similar to a number of complex, fuzzy and abstract concepts in the social sciences, conceptualizing cybercrime continues to be a challenge [2,48]. To circumvent the issues in defining cybercrime, some institutions de-emphasize the need to establish a single definition [16]. This viewpoint mirrors the philosophical approach of 'instrumentalism', viewing definitions as tools rather than commitments to concepts, thereby considering the importance of establishing a clear definition of cybercrime as secondary to the need to respond to cybercrime [2,49]. However, this approach proves problematic both in attempts to study cybercrime phenomena (e.g., how to measure cybercrime without defining cybercrime) and in responding to cybercrime [2]. Imprecise conceptualizations of real-world phenomena may lead to real-world negative consequences, for example, socioeconomic consequences for at-risk societal groups, excessive criminalization, miscarriages of justice or increased prevalence of online harms [2].

8.2. Lack of Consensus on Basic Terminology and Scope of Offences

The challenge in defining and classifying cybercrime begins with the ambiguity surrounding the basic terminology; this ambiguity cascades further to a fundamental lack of clarity and agreement on what constitutes a cybercrime, i.e., what level of involvement of technology is required for a criminal act to be considered a cybercrime [2], as demonstrated by different 'scopes' across the taxonomies identified in this review. As the term 'cybercrime' encompasses a diverse set of crimes (i.e., both traditional crimes and new criminal acts), notably absent in the literature is a comprehensive and unified list of cybercrimes [14]. Consolidation of the terminology and scope across disciplines and jurisdictions would be the first step in developing an effective classification system, and a necessary condition in being able to develop a comprehensive and cohesive classification of cybercrime.

Due to the breadth of behaviors that constitute 'cybercrime', there is also no obvious corresponding profile of what constitutes a 'cybercriminal' [2]. Additionally, it is unclear whether cybercriminals ought to be conceptualized as individuals, groups, organizations/institutions, or, even, nation-states [2]. Previous attempts to classify cybercrimes have focused on the criminal act itself; however, clarity could be gained by accounting for the characteristics of perpetrators (e.g., individuals, organized crime groups, and coordinated individuals) and their motivations.

8.3. Placing the Role of Technology at the Forefront of Developing Cybercrime Classifications

As demonstrated by the typologies and taxonomies identified within this review, the role of technology itself has been made the central defining factor in classifying cybercrime. This is fundamentally problematic, as technology will always outpace systematic academic work and the development of legal statutes. Cybercriminals are adeptly adaptive, as demonstrated by the various methods cybercriminals were able to modify for their modus operandi to take advantage of the COVID-19 pandemic. Furthermore, the use of the same technology may be used to commit different offences or for different motives. Therefore, future work may consider alternative or multiple core defining characteristics (e.g., perpetrators, victims, motivation, or resulting harm); see Tsakalidis, Vergidis and Madas [36] for an example of where this type of system has been proposed.

8.4. The Problem of 'Nullen Crimen Sine Lege' (No Crime without Law)

The taxonomies identified in this review primarily focus on cybercrime offences as defined by legal statutes, which introduces a second fundamental problem of 'nullen crimen sine lege' that is to say there is 'no crime without law' [20]. However, an offence-based framework is troublesome for three reasons: firstly, technology and cybercriminal behaviors will always outpace academic literature, policies and legislation; secondly, the problem of circularity (as cybercrime definitions and classifications are informed by legal statutes, which in turn inform legal statutes); thirdly, the lack of universal applicability as cybercrime legislation differs across jurisdictions [2,4].

Legislation across jurisdictions is not systematic or uniform, resulting in non-uniform international efforts to tackle harmful online behaviors, and this is compounded by the fact that cybercrimes are weighted differently across jurisdictions and change over time [4,5]. Another key concept to consider is that of 'cyberdeviancy'; "the distinction between defining cybercrime as deviance rather than as criminal behavior is that the focus shifts to societal norms rather than legally proscribed rules" [45] (pp. 17–18).

Incorporating the concept of 'cyberdeviancy' (deviant online behaviors which violate societal norms and may or may not overlap with cybercrimes) to include harmful behaviors that are not yet legislated against across all jurisdictions will make definitions and classification systems universally applicable until cybercrime terminology and scope is consolidated across jurisdictions. Alternatively, future classification systems may consider alternative approaches, aside from an offence-based framework; for example, behavioral profiles [14,17] or an ontological approach [16].

8.5. Accounting for Ideological Standpoints

Similar to the above, definitions and broader understandings of cybercrime can differ significantly, often due to the disciplinary schools of thought, theoretical standpoints, or purposes for which they originate. Underlying ideologies originate from historical established sociological criminological theories, for instance drawing on left realist perspectives of crime to investigate and better explicate cybercrime and cyberdelinquency (e.g., see Sparks [50]). Criminological theory has sought to question the value and accuracy of definitions, and these same lessons can be applied to the field of cybercrime. Some key examples include Howard Becker, who disputed standard definitions of deviance [51]; Stanley Cohen, who explored the criminological impacts of youth focused moral panics, the development of criminal and deviant subcultures, and societal hysteria [52]; Matza, who coined the concept of 'drift', offered wider sociological explanations of crime and incorporated the wider environment of a perpetrator into theorizing, defining and understanding categories of criminal behaviors [53]. There are examples of where criminology theory has been applied to understandings of cybercrime; for instance, attempts have been made to explore cybercrime as a moral panic [54] and an attempt has been made to adopt labelling theory as a guide for investigating the patterns, characteristics, and sanctions surrounding a sample of cybercrimes [55], with the aim of identifying how these cybercrimes are socially constructed in comparison to traditional crime. When adopting cybercrime definitions or conceptualizations, future work may seek to evaluate these underlying factors and assess their utility in unifying an understanding of cybercrime phenomena.

8.6. Allowing for Future Concepts: Incorporating Complexity and Evolving Nature of Technology

Increased attention must be paid to the complexity and constantly evolving nature of cybercrimes and the underlying technology [15]. Current classifications are arguably oversimplified and too reductive, reducing a complex and varied phenomenon to 2–5 categories, with a limited number of offences as illustrators. Therefore, there is a need to expand classification systems to allow for complexity but also flexibility, to account for the constantly evolving technological environment, and concomitant evolving cybercriminality, emerging harmful online behaviors (e.g., interpersonal abuse taking place online) [4], and increasing opportunities and methods to commit crime using technology [16].

With relatively limited research focusing on the classification of cybercrime [16], there is a need to scrutinize the evolving landscape of technology that brings with it new cybercriminal behaviors (see McGuire [2]). This review highlights the need for further empirical studies regarding the criminal use of advanced technologies such as Artificial Intelligence (AI), Machine/Deep Learning, Deep Fakes and Virtual Reality, which are relatively unaccounted for by current classification frameworks, as well as the use of technology for terror-related activities including extremism and radicalization. Key to future work in this field is developing a 'live system' by which cybercrime definitions and typologies can be adapted and regularly updated.

In particular, the impact of the COVID-19 pandemic on cyber criminality has created a 'new normal' worldwide. Cybercrime evolutions have altered the way criminals behave in order to exploit the current crisis (as described in a recent EUROPOL report [56]), highlighting the readiness of cybercriminals to adapt their modus operandi to take advantage of human and technological vulnerability. Further work needs to consider the implications of global crises such as the pandemic on society along with ever-evolving and changing cybercriminal behaviors in the areas of child sexual exploitation, criminal hacking, the sale and distribution of drugs online, fraud, counterfeit goods, and disinformation. Ultimately, the COVID-19 pandemic and its impact on cybercrime globally demonstrate that cybercrime classifications need to be adaptive and regularly updated to be effective and continue to stay relevant to the phenomenon they represent.

9. Towards a Comprehensive Classification System

Developing a clear conceptualization of cybercrime is needed not only to delineate the problem, but for estimating the impact of cybercrime on society, and developing effective legal and policy responses [3,8,16]. To effectively classify current and emerging cybercriminal behaviors, a comprehensive classification framework is essential, one that is compatible with international and national legislation or policies, the work of the public and private cybersecurity sectors, and can accommodate future research findings [8]. The difficulties in classifying cybercrime hinder the introduction of cybercrime-specific laws and regulations, which in turn can pose further challenges to policing cybercrime due to the limited capacity to respond [18]; therefore, the following is a list of preliminary recommendations for future work in the field.

9.1. A Shared Cybercrime Lexicon

To effectively combat cybercrime, a universally agreed-upon definition that determines key terminology and scope, along with a standardized method of cybercrime classification, must be devised and adopted to harmonize future decision making [17]. The introduction of a common language will be a key feature to the universal acceptance of cybercrime concepts that are in line with international treaties, as well as national legislation and policy (see Barn and Barn [3], and Viano [5]). Meaningful discussions, therefore, need to be actively encouraged to clarify and implement common language on an international scale [18]. Establishing a shared lexicon will be useful to all professionals working in the field, from policy makers discussing and proposing effective solutions to front-line workers seeking practical guidance on what does and what does not constitute a cybercrime [15].

9.2. Adopting a Multidisciplinary and Multijurisdictional Approach

Establishing a shared cybercrime lexicon necessitates an enhanced multidisciplinary and multijurisdictional approach encompassing key stakeholders at an international and localized level. Key stakeholders, for example, include policy makers, law enforcement agencies, industry intelligence and security agencies, the public sector, and academics. Collaboration among these main actors is critical to assess the sustainability and effectiveness of a comprehensive and cohesive cybercrime classification system. Furthermore, definitions can be enhanced by the application of criminological theoretical standpoints and ideologies of other academic disciplines, to be positioned within the most up-to-date scholarly thinking.

It is crucial that front-line workers also be included as key stakeholders. It is a continuing problem that police officers do not feel capable of taking responsibility to respond to cybercrime reports [4]. There is evidence that, due to the lack of adequate training, some local police officers lack the technical skills and knowledge of specific legislation to respond to cybercrime incidents [57–59], which in turn impedes their willingness to conduct cyber investigations [60]. Further, a significant factor affecting front-line workers is the ambiguity surrounding the definition of cybercrime [61].

9.3. Research-Driven Classification System and Transparency in Development

As identified by this review, approaches are fragmented and flawed; therefore, a key recommendation for future work is to develop a systematic, purposeful, and holistic classification system, that is evidence based, flexible, readily updated, supported by a dedicated research initiative, and incorporates multidisciplinary input and international cooperation. Furthermore, greater transparency is required to justify the decisions that underpin the development of cybercrime classification systems, to meaningfully evaluate and update established frameworks, and to account for key challenges (as described in detail above in Section 8).

9.4. Reconceptualizing the Boundaries between Cybercrime Categories

The spectrum approach allows for a more faithful representation of the complexity and variations intrinsic to cybercrime and cybercrime offences; this approach also allows for a flexible and effective classification system that can be readily adapted and updated to reflect the ever-changing cyber landscape. Sharp divisions between types of offences made by categorical approaches (as identified and described in this review) are likely artificial, meaning they do not accurately reflect likely overlaps or 'pathways' [43] between types of cybercrime offences, evolutions of cybercriminal behaviors or modus operandi, and the use of similar technologies across a range of cybercrime offences. For example, Deepfakes or AI-based crime can be used in a variety of different offences, from the distribution of CSAM [62] to political subversion [63]. Additionally, certain types of cybercrimes are not exclusively cyber dependent or cyber enabled; cybercriminal behaviors in practice are much more complex. For example, 'grooming' is an offence that predates digital technology but has since been perpetuated and facilitated by the use of internet technology, necessitating legislation against 'online grooming' [6]. This offence would seemingly be categorized under 'cyber enabled'. However, it is now recognized that online grooming does not necessarily involve offline contact, meaning the offence occurs solely in cyberspace [6]; therefore, in some contexts, the offence could be considered as 'cyber dependent'.

Future classification systems ought to adopt a spectrum-based approach to accurately capture the complexity of cybercrime offences and the evolution of cybercriminal behaviors. Furthermore, to avoid over-simplified and reductive classification systems, additional defining characteristics ought to be considered (e.g., the characteristics of perpetrators, the characteristics of victims, criminal motivations, and resulting harms of crimes).

9.5. Application of Feminist Theory to Cybercrime Definitions

While there is a plethora of definitions for the concept of "cybercrime", there is an ongoing, widespread dispute regarding the presence of a universal 'female voice' in criminological and legal theorizing. Feminist scholars have historically argued that approaches and law enforcement policies that claim to be gender neutral are mostly male dominated, and exclude female perspectives in their entirety [64]. Given that there is male dominance in the field of cybercrime and cybersecurity, and the high prevalence of gender-based crimes online, arguably, the application of feminist approaches to both defining and exploring cybercrime is lacking. Future contributions to the field should look to apply criminological feminist contributions and perspectives of cybercrime, in particular to crimes that manifest as sexual violence online.

10. Conclusions

This review identified and consolidated key cybercrime definitions, typologies and taxonomies from a range of academic and non-academic sources, as illustrated in the culmination of a new classification framework for conceptualizing cybercrime and cyberdeviance (Figure 1). As demonstrated within this review, the lack of clarity surrounding the term cybercrime has a significant impact on society, cybercrime policy, legal intervention and academic research. While each of the classification approaches identified within this review had its own strengths and weaknesses, the fact remains that no single classification system fully encapsulated cybercrime concepts or accurately reflected the nebulous nature of cybercrime acts. Furthermore, widely adopted classification systems are typically unidimensional and make sharp distinctions between types of cybercrimes, whereas cybercriminal and cyberdeviant behaviors may perhaps be better conceptualized as existing on a spectrum. This review demonstrates that tying the term 'cybercrime' to specific uses of technologies or existing cybercrime legislation prevents a complete understanding of cybercrime behaviors, and does not allow for a forward-leaning approach, by not allowing for the consideration of evolving or future cybercrime phenomena. Future approaches may find that alternative classification dimensions based on motivations and intentions of cybercriminal offenders may provide greater explanatory power. Currently, there is remaining ambiguity as to what exactly constitutes a cybercrime and a clear conceptualization of cybercrime will likely continue to be a challenge. This paper has outlined the key challenges as well as made recommendations for future work in the field to advance a collective understanding of cybercrime phenomena and more importantly move towards developing a robust and comprehensive classification system.

Author Contributions: Conceptualization, K.P., J.C.D., C.B., S.C. and M.A.; methodology, K.P., J.C.D., C.B., S.C. and M.A.; investigation and writing (original draft preparation), K.P.; writing (review and editing), K.P., J.C.D., R.R.F., C.B., S.C. and M.A.; supervision and funding acquisition, J.C.D., S.C. and M.A. All authors have read and agreed to the published version of the manuscript.

Funding: The contents of this research are based on work completed under CC-Driver (Combating Cyber Criminality by Understanding Human and Technical Drivers), a project funded by the European Union's Horizon 2020 research and innovation program under grant agreement No. 883543.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: This research was completed by CC-Driver (Combating Cyber Criminality by Understanding Human and Technical Drivers) partners at the University of East London and the University of Lausanne. The authors would like to thank the other partners of the CC-Driver consortium and William Dugdale for supporting the development of this review and the ongoing CC-Driver research program.

Conflicts of Interest: The authors declare that there is no conflict of interest.

Abbreviations

AI	Artificial Intelligence
ICMEC	International Centre for Missing and Exploited Children
CC-Driver	Combating Cyber Criminality by Understanding Human and Technical Drivers
COE	Council of Europe
CSA	Child Sexual Abuse
CSAM	Child Sexual Abuse Material
CSE	Child Sexual Exploitation
DoS	Denial of Service
DDoS	Distributed Denial of Service
EU	European Union
ICT	Information Communications Technology

References

1. Kemp, S. Digital 2021: Global Overview Report. 27 January 2021. Available online: https://datareportal.com/reports/digital-2021-global-overview-report (accessed on 12 May 2021).
2. McGuire, M. It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In *The Human Factor of Cybercrime*; Leukfeldt, R., Holt, T.J., Eds.; Routledge: New York, NY, USA, 2020; pp. 3–28.
3. Barn, R.; Barn, B. An ontological representation of a taxonomy for cybercrime. In Proceedings of the 24th European Conference on Information Systems (ECIS 2016), Istanbul, Turkey, 12–15 June 2016.
4. Black, A.; Lumsden, K.; Hadlington, L. 'Why Don't You Block Them?' Police Officers' Constructions of the Ideal Victim when Responding to Reports of Interpersonal Cybercrime. In *Online Othering: Exploring Violence and Discrimination on the Web*; Lumsden, K., Harmer, E., Eds.; Palgrave Macmillan: Basingstoke, UK, 2019; pp. 355–378.

5. Viano, E.C. Cybercrime: Definition, Typology, and Criminalization. In *Cybercrime, Organized Crime, and Societal Responses*; Viano, E.C., Ed.; Springer International Publishing: Cham, Switzerland, 2017; pp. 3–22.
6. ICMEC. *Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review*; International Centre for Missing & Exploited Children: Alexandria, VA, USA, 2017.
7. Van der Hulst, R.C.; Neve, R.J. *High Tech Crime Literature Review about Crimes and Their Offenders*; WODC (Research and Documentation Centre): The Hague, The Netherlands, 2008.
8. Paoli, L.; Visschers, J.; Verstraete, C.; Van Hellemont, E. *The Impact of Cybercrime on Belgian Businesses*; Intersentia: Cambridge, UK, 2018.
9. Chang, L.Y. *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*; Edward Elgar Publishing: Cheltenham, UK, 2012.
10. Sarre, R.; Lau, L.Y.C.; Chang, L.Y. Responding to cybercrime: Current trends. *Police Pract. Res.* **2018**, *19*, 515–518. [CrossRef]
11. Grant, M.J.; Booth, A. A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Inf. Libr. J.* **2009**, *26*, 91–108. [CrossRef] [PubMed]
12. Yar, M.; Steinmetz, K.F. *Cybercrime and Society*, 3rd ed.; SAGE Publications Ltd.: London, UK, 2019.
13. Parker, D. *Crime by Computer*; Charles Scribner's Sons: New York, NY, USA, 1976.
14. Wall, D.S. *Cybercrime: The Transformation of Crime in the Information Age*; Polity Press: Cambridge, UK, 2007.
15. Tsakalidis, G.; Vergidis, K. A systematic approach toward description and classification of cybercrime incidents. *IEEE Trans. Syst. Man Cybern. Syst.* **2017**, *49*, 710–729. [CrossRef]
16. Donalds, C.; Osei-Bryson, K.M. Toward a cybercrime classification ontology: A knowledge-based approach. *Comput. Hum. Behav.* **2019**, *92*, 403–418. [CrossRef]
17. Broadhead, S. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Comput. Law Secur. Rev.* **2018**, *34*, 1180–1196. [CrossRef]
18. Akdemir, N.; Sungur, B.; Başaranel, B.U. Examining the Challenges of Policing Economic Cybercrime in the UK. *Güvenlik Bilimleri Derg. (Int. Secur. Congr. Spec. Issue)* **2020**, *Özel Sayı*, 113–134. [CrossRef]
19. Gillespie, A.A. *Cybercrime: Key Issues and Debates*; Routledge: New York, NY, USA, 2015.
20. Wall, D.S. Introduction: Cybercrime and the Internet. In *Crime and the Internet*; Wall, D.S., Ed.; Routledge: New York, NY, USA, 2001; pp. 1–17.
21. Thomas, D.; Loader, B. Introduction-Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. In *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*; Thomas, D., Loader, B., Eds.; Routledge: London, UK, 2000.
22. Gordon, S.; Ford, R. On the Definition and Classification of Cybercrime. *J. Comput. Virol.* **2006**, *2*, 13–20. [CrossRef]
23. United Nations. *United Nations Manual on the Prevention and Control of Computer-Related Crime*; United Nations: New York, NY, USA, 1994.
24. UN Congress Crimes Related to Computer Networks. *10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders*; United Nations: Vienna, Austria, 2000. Available online: https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf (accessed on 6 April 2022).
25. Council of Europe. *Convention on Cybercrime*; European Treaty Series No. 185; Council of Europe: Budapest, Hungary, 2001; pp. 1–25. Available online: https://rm.coe.int/1680081561 (accessed on 6 April 2022).
26. Commission of the European Communities. *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: Towards a General Policy on the Fight against Cyber Crime*; Commission of the European Communities: Brussels, Belgium, 2007; Volume 267.
27. Malby, S.; Mace, R.; Holterhof, A.; Brown, C.; Kascherus, S.; Ignatuschtschenko, E. *Comprehensive Study on Cybercrime*; United Nations Office on Drugs and Crime: Vienna, Austria, 2013.
28. European Commission. *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*; European Commission: Brussels, Belgium, 2013.
29. Akhgar, B.; Choras, M.; Brewster, B.; Bosco, F.; Veermeersch, E.; Luda, V.; Puchalski, D.; Wells, D. Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism. In *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*; Akhgar, B., Brewster, B., Eds.; Springer: Cham, Switzerland, 2016; pp. 295–321.
30. McGuire, M.; Dowling, S. *Cybercrime: A Review of the Evidence: Summary of Key Findings and Implications*; Home Office: London, UK, 2013.
31. Brenner, S. Cybercrime: Re-thinking crime control strategies. In *Crime Online*; Jewkes, Y., Ed.; Willan Publishing: Cullompton, UK, 2007; pp. 12–28.
32. Furnell, S.M. *Cybercrime: Vandalizing the Information Society*; Addison Wesley: London, UK, 2002.
33. Burns, S.; Roberts, L. Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prev. Community Saf.* **2013**, *15*, 48–64. [CrossRef]
34. Davidson, J.; Livingstone, S.; Jenkins, S.; Gekoski, A.; Choak, C.; Ike, T.; Phillips, K. *Adult Online Hate, Harassment and Abuse: A Rapid Evidence Assessment*; Department for Digital, Culture, Media and Sport (DCMS): London, UK, 2019.

35. Department for Digital, Culture, Media & Sport. Consultation Outcome: Online Harms White Paper, 15 December 2020. Available online: https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper (accessed on 13 May 2021).
36. Tsakalidis, G.; Vergidis, K.; Madas, M. Cybercrime Offences: Identification, Classification and Adaptive Response. In Proceedings of the 5th International Conference on Control, Decision and Information Technologies (CoDIT), Thessaloniki, Greece, 10–13 April 2018; pp. 470–475.
37. European Commission. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7 February 2013. Available online: www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed on 12 July 2021).
38. Wall, D.S. The Internet as a Conduit for Criminals. In *Information Technology and the Criminal Justice System*; Pattavina, A., Ed.; Sage: Thousand Oaks, CA, USA, 2005; pp. 77–98, (Chapter revised March 2010).
39. Council of Europe. *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*; Council of Europe: Strasbourg, France, 2003.
40. Jarrett, H.M.; Bailie, M.W.; Hagen, E.; Eltringham, S. *Prosecuting Computer Crimes*; US Department of Justice, Computer Crime and Intellectual Property Section Criminal Division, Office of Legal Education Executive Office for United States Attorneys: Washington, DC, USA, 2010.
41. European Union. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. *Off. J. Eur. Union* **2013**, *218*, 8–14. Available online: https://data.europa.eu/eli/dir/2013/40/oj (accessed on 6 April 2022).
42. Marcum, C.D.; Higgins, G.E. Cybercrime. In *Handbooks of Sociology and Social Research*, 2nd ed.; Krohn, M.D., Hendrix, N., Hall, G.P., Lizotte, A.J., Eds.; Springer: Cham, Switzerland, 2019; pp. 459–475.
43. Aiken, M.; Davidson, J.; Amann, P. *Youth Pathways into Cybercrime*; Paladin Capital Group: London, UK, 2016.
44. The Interagency Working Group Terminology. *Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*; ECPAT International and ECPAT Luxembourg: Bangkok, Thailand, 2016.
45. Payne, B.K. Defining Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*; Holt, T.J., Bossler, A.M., Eds.; Springer International Publishing AG: New York, NY, USA, 2020; pp. 3–25.
46. Donaldson, S.; Davidson, J.; Aiken, M. *Safer Technology, Safer Users: The UK as a World-Leader in Safety Tech, Perspective Economics & University of East London*; Department for Digital, Culture, Media & Sport (DCMS): London, UK, 2020.
47. Vold, G. *Theoretical Criminology*; Oxford University Press: New York, NY, USA, 1958.
48. Weber, M. Objectivity in social science and social policy. In *The Methodology of the Social Sciences*; Shils, E.A., Finch, H.A., Eds.; Free Press: Glencoe, Illinois, USA, 1949.
49. Worrall, J. Scientific realism and scientific change. *Philos. Q.* **1982**, *32*, 201–231. [CrossRef]
50. Sparks, R. Reason and unreason in "left realism": Some problems in the constitution of the fear of crime. In *Issues in Realist Criminology*; Matthews, R., Young, J., Eds.; SAGE Publications Ltd.: London, UK, 1992.
51. Becker, H.S. *Outsiders: Studies in the Sociology of Deviance*; Free Press: New York, NY, USA, 1963.
52. Cohen, S. *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*; Routledge: London, UK, 2002.
53. Matza, D. *Delinquency & Drift*, 2nd ed.; Taylor & Francis: Abingdon, UK, 1990. [CrossRef]
54. Lavorgna, A.; Cyber-organised crime. A case of moral panic? *Trends Organ. Crime* **2019**, *22*, 357–374. [CrossRef]
55. Payne, B.K.; Hawkins, B.; Chunsheng, X. Using Labelling Theory as a Guide to Examine the Patterns, Characteristics, and Sanctions Given to Cybercrimes. *Am. J. Crim. Justice* **2019**, *44*, 230–247. [CrossRef]
56. EUROPOL. *Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse during the COVID-19 Pandemic*; European Union Agency for Law Enforcement Cooperation: The Hague, The Netherlands, 2020.
57. Bossler, A.M.; Holt, T.J. Patrol officers' perceived role in responding to cybercrime. *Polic. Int. J.* **2012**, *35*, 165–181. [CrossRef]
58. Bond, E.; Tyrrell, K. Understanding revenge pornography: A national survey of police officers and staff in England and Wales. *J. Interpers. Violence* **2018**, *36*, 2166–2181. [CrossRef] [PubMed]
59. Hadlington, L.; Lumsden, K.; Black, A.; Ferra, F. A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Polic. J. Policy Pract.* **2021**, *15*, 34–43. [CrossRef]
60. Lee, J.R.; Holt, T.J.; Burruss, G.W.; Bossler, A.M. Examining English and Welsh Detectives' Views of Online Crime. *Int. Crim. Justice Rev.* **2021**, *31*, 20–39. [CrossRef]
61. Hadlington, L.J. Employees attitudes towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *Int. J. Cyber Criminol.* **2018**, *12*, 262–274.
62. Ratner, C. When "Sweetie" is not so Sweet: Artificial Intelligence and its Implications for Child Pornography. *Fam. Court. Rev.* **2021**, *59*, 386–401. [CrossRef]
63. Paterson, T.; Hanley, L. Political warfare in the digital age: Cyber subversion, information operations and 'deep fakes'. *Aust. J. Int. Aff.* **2020**, *74*, 439–454. [CrossRef]
64. Carrabine, E.; Cox, P.; Lee, M.; Plummer, K.; South, N. *Criminology: A Sociological Introduction*; Routledge: Abingdon, UK, 2009.