Asian Journal of Criminology
https://doi.org/10.1007/s11417-024-09436-y

Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality

You Zhou[1] · Milind Tiwari[2] · Ausma Bernot[3] · Kai Lin[4]

Received: 29 April 2024 / Accepted: 22 July 2024

Abstract

The advent of the metaverse has given rise to metacrime, a novel category of criminal activities occurring in the metaverse, which not only challenges conventional digital criminality but existing law enforcement frameworks. To address the scholarship vacancy, this study examines the intersections and distinctions between metacrime and conventional cybercrime by employing a multi-disciplinary literature review and comparative analysis. We identified five shared characteristics between these two crime types: *crime classification*, *continuous evolution*, *hyper-spatial-temporality (global reach)*, *anonymity*, and *governance challenges*. Crucially, our research highlights the distinct epistemological aspects of metacrime through its criminogenic, victimogenic, etiological, ethical, and regulatory dimensions, exemplified by *virtual-to-physical attacks, immersive virtual reality attacks, victimization superrealism, complexities of human-avatar interactivity, excessive misuse of biometric data, increasingly vulnerable populations, and avatars' liability.* Our findings underscore the imperative need for tailored and forward-thinking regulatory responses to address the intricate challenges of metacrime, thereby ensuring the security and integrity of evolving digital environments.

Keywords Metaverse · Metacrime · Cybercrime · Digital criminality · Virtual reality

Introduction

The evolving landscape of digital criminality, particularly the interplay and distinctions between cybercrime and offline crimes, has sparked extensive scholarly discourse over the years. This discussion has borne a variety of metaphors such as "new wine in old bottles" (Grabosky, 2001), "new wine in no bottles" (Wall, 1999), "new wine in opaque bottles"

✉ You Zhou
you.zhou@monash.edu

[1] School of Social Sciences, Faculty of Arts, Monash University, Melbourne, Australia

[2] Australian Graduate School of Policing and Security, Charles Sturt University, Canberra, Australia

[3] School of Criminology and Criminal Justice, Griffith University, Gold Coast, Australia

[4] School of International Studies and Education, Faculty of Arts and Social Sciences, University of Technology Sydney, Sydney, Australia

Published online: 09 August 2024

(Urbas, 2018), and “old wine in new bottles” (Babanina et al., 2021). This metaphor kaleidoscope not only underscores the persistent essence of conventional criminal behavior manifested in new realms but also elucidates the dynamic spectrum between terrestrial crimes and cyber counterparts. However, the conversation becomes further complicated by the emerging term “metacrime” (Seo et al., 2023), which denotes the criminal activities emerging within three-dimensional immersive online environments, namely, metaverse (Ritterbusch & Teichmann, 2023). The development of metacrime amplifies debates not only on how it diverges from offline crimes but, more importantly, how it differentiates from our understanding of conventional cybercrime.

To navigate through the increasingly blurred boundaries, this study examines the similarities and differences between metacrime and cybercrime. Specifically, the study eschews an exhaustive rectification or philosophical dissection of the myriad variances in terminologies, typologies, and taxonomies distinguishing these forms of digital criminality. Instead, it acknowledges the foundational parallels and delves into multi-dimensional criminal potentials ushered in by the advent and progression of metaverse technologies. By incorporating multi-disciplinary literature and theories, we posit that metacrime, as an evolutionary facet within the spectrum of cyberspace, not only retains inherent similarities with cybercrime but also unveils a plethora of unprecedented criminal opportunities. The findings extend beyond the confines historically observed in terrestrial and conventional cyber contexts, heralding a new era of digital criminality.

The architecture of this study is organized in the following order. Initially, the study will outline the core elements of the metaverse and the emergent criminal activities, referred to as metacrime. Subsequently, we reviewed the existing literature scholarship on cybercrime, underscoring the typical features of cybercrime. Through the analysis, five key parallels between metacrime and cybercrime are articulated. Furthermore, this study delves deeply into the criminogenic, victimogenic, etiological, ethical, and regulatory dimensions, thereby highlighting the unique characteristics of metacrime. The insights of the current study offer valuable perspectives for scholars, practitioners, and policymakers, suggesting that metacrime, which shares the fundamental characteristics of cybercrime, not only introduces wider criminal opportunities but also opens Pandora’s Box to more complex regulatory dilemmas than its predecessors.

Metaverse and Metacrime

The metaverse has been described as various forms of three-dimensional immersive online environments where users interact with others through avatars (Ritterbusch & Teichmann, 2023). Such a virtual world is characterized by its continuity, a perception of being present within it, and the facilitation of social and economic interactions (Lu et al., 2022; Ritterbusch & Teichmann, 2023). Metaverse represents a realm that extends beyond the confines of the physical world by integrating advanced technologies, such as extended reality, blockchain, and artificial intelligence (Lee et al., 2021). Consequently, it enables a multitude of applications across diverse sectors, such as entertainment, socializing, tourism, real estate, retail, fashion, and education (Singh, 2024; Smaili & de Rancourt-Raymond, 2024). For instance, the metaverse functions as an adaptive, dynamic, and expansive digital universe that revolutionizes entertainment and socializing experiences by creating immersive, personalized, and interoperable digital realms that enable seamlessly realistic engagement, user-generated content, and cross-platform interaction (Lee et al., 2021). Besides, the metaverse holds the potential to provide professional training opportunities across long distances, overcoming geographical constraints and thus presenting a cost-effective solution. The investments made by major corporations have demonstrated optimism in the prospects of the metaverse. For example, in July 2021, Facebook committed to invest USD 10 billion over the five next years to become a metaverse company and subsequently rebranded itself as Meta (Kim et al., 2023; Kraus et al., 2022).

However, this technological innovation presents concerns regarding the emergence of opportunities to undertake a range of criminal activities (Dwivedi et al., 2023; Kim et al., 2023). These concerns stem not only from the inherent vulnerabilities within metaverse technologies but also from the absence of a robust regulatory framework. In January 2024, the UK police reported that they were investigating their first case of a virtual reality attack on a minor whose avatar was gang-raped (Camber, 2024). This is not the first case of sexual assault in the metaverse. There are fears—and emergent evidence—that the "gamergate" culture of harassing women in online gaming spaces will spill into the metaverse that cannot be addressed with just technological solutions (Nix, 2024). Additionally, digital assets, such as virtual real estate and wearables offered by metaverse platforms, can also be used to launder money (Annison, 2022). Furthermore, a lack of educational awareness among the platform users provides opportunities for numerous fraudulent schemes, such as Ponzi schemes, rug pulls, and deceptive giveaway scams (Wu et al., 2023). Difficulties in verifying children's age online add extra concerns about grooming and minor abuse. Metaverse companies have responded to these emergent concerns differently but have slowly addressed them overall (Bibri & Allam, 2022).

Above all, it is hard to deny the ample potential of criminal events in the metaverse, which has been termed as metacrime (Seo et al., 2023). As a fresh concept, it is apparently out of doubt that little consensus on metacrime's definition, typology, and taxonomy has been reached. Seo et al. (2023) adopted a loosen definition by referring metacrime to all crimes that occurred in the metaverse, neither partially nor fully. The International Criminal Police Organization (INTERPOL, 2024) provided a crime classification by modus operandi, which categorizes metacrime into ten broader groups, encompassing cybercrime, financial crimes, property crimes, sexual offenses and assault, identity crimes, terrorism, intellectual property crimes, crimes against children, acts intended to cause fear or emotional distress, crimes against public safety. Although this classification encounters some methodological controversies (e.g., conceptual overlap), it provides a comprehensive overview regarding the complexity and multi-dimensionality of metacrime. More recently, Gómez-Quintero et al. (2024) provided an empirically informed taxonomy by a scoping literature review on metacrime followed by the nominal group technique (participant-driven theme generation workshops). They found five high-level categories of metacrime, including (1) fraud, forgery, and financial crimes, (2) property crimes, (3) sex crimes, (4) other crimes against the person, and (5) other crimes. Though the taxonomy can be too broad to illustrate the unique characteristics of metacrime compared to INTERPOL's typology, it provides the very first empirical insights into metacrime categorization.

The current research reckons the complexity of defining and measuring metacrime and thus adopts the broader definition suggested by Seo et al. (2023), which has either been explicitly or implicitly employed in the antecedent studies (e.g., Bovenzi, 2023; Gómez-Quintero et al., 2024; INTERPOL, 2024). Recognizing the emergence of metacrime, a salient research gap comes after the epistemological relationship between metacrime and cybercrime, questioning whether metacrime is another "old wine in new bottles" (Marshall & Tompsett, 2024). Therefore, examining the similarities and differences between the two types of digital criminality will not only advance our understanding of to what extent metaverse and its intricate technologies facilitate original criminal opportunities but also reveal the differential necessity in developing contextualized and targeted regulatory responses for metacrime reduction and prevention.

Cybercrime Characteristics

Historically, an array of terms has been developed to depict the myriad illicit activities that occur within cyberspace. Terminologies such as "cybercrime," "computer crime," "internet crime," "online crime," "digital crime," "electronic crime," "virtual crime," and "E-crime" have been adopted to articulate the phenomenon of cybercriminality. Notably, "cybercrime" has ascended as the predominant term since 1995 and has achieved broad acceptance within the scholarly and practical domains (Phillips et al., 2022). Since the inception of this term, the academic and professional fields have grappled with the challenge of reaching a consensus regarding a universal definition and typology for cybercrime. This has resulted in a diversity of interpretations among scholars, practitioners, and policymakers alike, each contributing their unique perspective to the discourse (e.g., Council of Europe, 2001; Gordon & Ford, 2006; Holt & Bossler, 2016; UN, 2000; Wall, 2007a). Despite the absence of a unified definition, one particularly notable and widely referenced definition posits cybercrime simply as "crimes that occur within cyberspace" (Wall, 2007a). While some may critique this definition for its breadth—arguably glossing over the intricacies and distinct attributes of cybercrimes—it nevertheless provides a versatile framework that accommodates the broad spectrum of criminal activities engendered by the volatile progression of technological evolution.

Extant scholarship has extensively cataloged a diverse array of typologies and taxonomies for the classification of cybercrimes, indicating a profound exploration of this domain (Brenner, 2007; Gordon & Ford, 2006; Holt & Bossler, 2016; Sarre et al., 2018; Wall, 2007a). The binary classification system has achieved notable prominence among both researchers and practitioners, positing that cybercrimes can be bifurcated into cyber-dependent and cyber-enabled crimes (Brenner, 2007; Holt & Bossler, 2016; McGuire & Dowling, 2013; Wall, 2007a). The former encompasses offenses inherently reliant on digital technologies—such as hacking, ransomware, and cyber warfare—whereas the latter encompasses conventional crimes that, although predating the internet's inception, are now expedited by the advent of digital technologies (Holt & Bossler, 2016). While some scholars have evolved these binary distinctions into more nuanced trichotomies—for instance, crimes against machines, crimes using machines, and crimes in machines (Wall, 2007a)—and even more granular classifications (e.g., Marcum & Higgins, 2019; Sarre et al., 2018; Tsakalidis & Vergidis, 2017), the dichotomous framework persists as the most prevalently employed (Phillips et al., 2022).

Despite debates around the notion of "old wine in new bottles," existing scholarship has delineated at least four fundamental characteristics of cybercrimes: technology-driven evolution, hyper-spatial-temporality (global reach), anonymity, and governance challenges. First, cybercriminality is inherently linked to the relentless advancement of technology. Unlike many terrestrial crimes (e.g., violent, property, and sexual crimes) that remain relatively static in their classification, cybercrime is unique in its capacity to evolve in tandem with technological progress (Grabosky, 2001; Wall, 2007a). With the advent of information and communication technologies (ICTs), there has been not only a proliferation of novel criminal activities, such as hacking, ransomware, botnets, and distributed denial of services (DDoS), but also a transformation of offline crimes into their online counterparts, including cyber fraud, cyberbullying, online harassment, and online stalking (Holt & Bossler, 2016). Although some scholars posit that the etiology of newer forms of cybercrimes may not diverge markedly from their historical precedents (Donner et al., 2015; Marshall & Tompsett, 2024), research indicates discernible theoretical and empirical variances in crime prevalence, criminal techniques, cultural contexts, victim-offender overlap, criminal social networks, and the criminal life-course (Kwon et al., 2024; McCuddy & Esbensen, 2017; Weulen Kranenbarg et al., 2018, 2019, 2021). Therefore, the continuous progression of technology casts an ever-present potential for the evolution of criminality within cyberspace.

Cybercrime is devoid of the spatial and temporal convergence between victims and offenders. The routine activity theory posited by Cohen and Felson (1979) suggests that terrestrial crimes necessitate the spatial and temporal convergence of three elements: suitable targets, motivated offenders, and the absence of capable guardians. Yar (2005) scrutinized the relevance of this theory within the cyber context, contending that the prerequisites of spatial and temporal proximity are nullified in cyberspace, which lacks a "recognizable spatial topology" and an inherent "temporal sequence and order." This paradigm shift enables motivated offenders to target victims across vast distances and temporal boundaries effortlessly, underscoring the hyper-spatial-temporality of cybercrime (Hooper et al., 2013; Payne, 2020). For instance, an individual in an Australian university classroom might encounter hate speech originating from another country, even if it was posted in the previous decade, via digital platforms, such as bulletin board systems, social media sites, and online forums. The concept of hyper-spatial-temporality not only facilitates the transnational exposure of a target's value and visibility but also diminishes the deterrence of criminal acts by affecting the swiftness, certainty, and severity of the anticipated punishment (Beccaria, 1764 [2016]).

ICTs and their progressive evolution afford cybercriminals layers of anonymity and pseudonymity, distinguishing them from perpetrators of terrestrial crimes. In contrast to terrestrial offenses, where the facial and biometric features of individuals are at a higher risk of detection by both human observers and digital surveillance mechanisms (e.g., CCTV), cybercrime benefits from a significant degree of "anonymity and plasticity" through the fabrication of online identities (Yar, 2005; Williams, 2006). Within the digital realm, motivated offenders can easily exploit cyberspace's malleable nature by crafting fictitious personas or engaging in identity theft by masquerading as others (Cross & Layt, 2022; Smith, 2013). Such inauthentic identities—encompassing both fabricated identities and stolen ones—serve as precursors to a broad spectrum of cybercrimes, including cyber fraud (Smith, 2013), cyberbullying (Barlett, 2015), cyberstalking (Pittaro, 2007), online money laundering (Mejri et al., 2022), hacking (Merck, 2015), data breaches (Hutchings & Holt, 2017), online illicit markets (Holt & Lee, 2022), and online hate crimes (Castaño-Pulgarín et al., 2021). The veil of anonymity and the utilization of counterfeit identities not only facilitate cybercriminals' evasion from legal scrutiny but also pose substantial legal and regulatory challenges (Brenner, 2006; as further discussed in the subsequent section).

The continuous technological evolution, the inherently global feature of cyberspace, and the prevalent anonymity therein pose significant challenges to the regulation and governance of cybercrime. The swift pace of technological advancements often surpasses the speed of legislation, thereby diminishing the deterrent effect of legal frameworks and the efficacy of timely law enforcement actions (Broadhurst, 2006; Hui et al., 2017). Moreover, the transnational character of cybercrime necessitates international cooperation in law enforcement efforts. Yet, jurisdictional discrepancies and the absence of a comprehensive international legal framework significantly impede the willingness and processes for cross-border collaboration in the investigation, prosecution, and sentencing of cybercriminals (Brenner, 2006, 2007; Broadhurst, 2006). Furthermore, the widespread anonymity complicates ethical considerations for law enforcement, often presenting dilemmas in striking a balance between protecting privacy and facilitating information sharing with technology companies and other public entities (Kennedy, 2009; Nolan, 2015). Given the various factors elaborated above, it is reasonable to assume that the continuous evolution of cybercrime facilitated by technological upgrades may induce increasing dilemmas for crime regulation and governance.

The Similarities Between Metacrime and Cybercrime

Situated within the realm of cybercrime, metacrime exhibits numerous parallels with its counterpart, including crime classification, continuous evolution, hyper-spatial-temporality, anonymity, and governance challenges. Firstly, the classifications of a myriad of deviant and criminal activities within the metaverse are mostly akin to those identified in cybercrimes. As Marshall and Tompsett (2024) assert, the metaverse is no longer a new frontier for crimes, denoting that the sophisticated technologies inherent in immersive online environments do not significantly alter criminogenic etiologies in ways of reaching a qualitative threshold. This observation is further validated through a comparative analysis of the typologies and taxonomies emerging from distinct scholarly inquiries. For instance, Gómez-Quintero et al. (2024) systematically reviewed the criminal activities currently observed in the metaverse, identifying five overarching categories of metacrime: financial crimes, property crimes, sex crimes, crimes against persons, and other crimes. These categories closely correlate with the cybercrime typological framework proposed by Phillips et al. (2022), as evidenced by several comparable criminal activities (e.g., fraud, hacking, sexual assault, stalking, and money laundering). Hence, the metaverse serves as selectable and displaceable platforms that motivated offenders might contemplate during their criminal decision-making processes. However, Gómez-Quintero et al. (2024) noted a few novel criminogenic and victimogenic opportunities unique to the metaverse, including cyber-physical person attacks, cyber-physical property attacks, and cyber-physical infrastructure attacks, which will be discussed further in the subsequent section.

Similar to cybercrime, metacrime is intrinsically dynamic, evolving with the continuous technological advancements and integration of immersion-based technologies. The metaverse, underpinned by a spectrum of cutting-edge technologies, cultivates a conducive environment for the genesis of novel cybercrimes. A broad range of technologies, including ICTs, cloud computing, artificial intelligence (AI), computer vision, blockchain, robotics/Internet of Things (IoTs), user interactivity, and extended reality, are recognized as pivotal enablers of the metaverse (Lee et al., 2021). Each foundational technology not only unveils a multitude of technological and societal vulnerabilities ripe for exploitation by motivated offenders but also their synergy, alongside the introduction of new technologies, invariably generates an escalating number of criminal opportunities within the metaverse. Dwivedi and associates (2023) cataloged a diverse collection of vulnerabilities precipitated by metaverse-centric technologies, encompassing invasive advertising, privacy infringements, identity theft, terrorist exploits, child abuse, and sexual harassment. They further posit that technological advancements are more likely to exacerbate, rather than mitigate, the vulnerabilities individuals face in the forthcoming iterations of the metaverse (Dwivedi et al., 2023).

Thirdly, the metaverse not only mirrors the hyper-spatial-temporality characteristic of cyberspace but also narrows the divide between real and virtual realms through holographic constructs and simulations. As an immersive online environment, the metaverse inherently transcends the physical and temporal constraints that govern interpersonal interactions in the tangible world (Wang et al., 2022). Users of the metaverse can engage in transnational interactions with others utilizing a variety of modalities, including avatars, digital cameras, and head-mounted displays (HMDs; Meta, 2024). Additionally, the advent of digital twins—virtual representations of physical entities—minimizes the gap and obscures the boundaries between actual and virtual spaces (Lee et al., 2021). By employing digital twins, it is conceivable for users from one nation to virtually explore an ancient structure that has ceased to exist in the present day. This hyper-spatial–temporal attribute, facilitated by holographic simulation, redefines and complicates the landscape of location-based criminality. For instance, environmental criminology (e.g., broken window theory, crime pattern theory; Brantingham & Brantingham, 1995; Kelling & Wilson, 1982) that amassed considerable insights regarding the impact of human–environment interaction (e.g., land use, environmental design, population density) on criminal activities remains undeveloped in cyberspace will also encounter theoretical and methodological dilemmas in the metaverse.

Fourthly, the issue of anonymity persists within the metaverse and can be intensified by the widespread adoption of decentralized financial transaction systems, such as cryptocurrencies. As a cyber platform, the metaverse encapsulates nearly every aspect of the challenges associated with anonymity (Dwivedi et al., 2023; Gómez-Quintero et al., 2024; Kim et al., 2023; Mackenzie, 2022; Smaili & de Rancourt-Raymond, 2024). For example, despite Meta (2024) offering options for identity verification, few users avail themselves of this feature, primarily due to privacy concerns (Beltrán & Calvo, 2023; Kürtünlüoğlu et al., 2022). The utilization of personalized avatars, pseudonyms, and the plasticity of identity creates varying degrees of anonymity, which, on the one hand, serves as a safeguard for user privacy and confidentiality but, on the other, presents significant vulnerabilities that malicious actors may exploit to evade legitimate oversight and legal repercussions (Cheong, 2022). Furthermore, the adoption of cryptocurrency as a primary financial mechanism introduces an additional layer of obscurity, compounding the challenges of anonymization in the metaverse. Extensive studies have documented the use of cryptocurrencies in facilitating illicit activities due to their anonymity and the difficulty in tracing transactions, including money laundering (Dyntu & Dykyi, 2018), hacking (Corbet et al., 2020), fraud (Ilker & Aydos, 2020), terrorism (Carroll & Windle, 2018), and geopolitical conflicts (Tiwari et al., 2024).

Lastly, metacrime encapsulates numerous governance challenges analogous to those encountered in the realm of cybercrime. Contemporary legal frameworks (Hui et al., 2017; Kalyvaki, 2023), jurisdictional discrepancies (Broadhurst, 2006; Cheong, 2022), the necessity of international cooperation (Dwivedi et al., 2023; Kshetri, 2021), digital forensic proficiency and capabilities (Holt & Bossler, 2012; Kim et al., 2023), privacy issues (Nolan, 2015; Steele et al., 2020), and a deficiency in public awareness (Smaili & de Rancourt-Raymond, 2024; Wall, 2007b) are among the principal challenges in mitigating and managing both cybercrime and metacrime. Furthermore, unique features of the metaverse, such as holographic simulation and the significant use of avatars, introduce distinct legal and regulatory quandaries. For example, a contentious issue remains on whether and how terrestrial legal principles should be extended to avatars and digital twins (Cheong, 2022; Zoltick & Maisel, 2023; see more detailed discussion below).

The Uniqueness of Metacrime

The Criminogenic Potential of the Metaverse: Virtual-to-Physical Attacks and Immersive Virtual Reality Attacks

The literature has yet to extensively document two significant forms of criminality observed in the metaverse: virtual-to-physical attacks and immersive virtual reality attacks. Both types of aggression are enabled by exploiting and manipulating immersive online environments, HMDs, and associated haptic devices, which seamlessly bridge the virtual-physical continuum. The former predominantly exploits the virtual-physical interface, whereas the latter focuses on manipulating HMDs and haptic suites. These opportunities allow motivated offenders to potentially inflict severe physical repercussions on a wide array of targets (e.g., individuals, properties, and infrastructure), which have been rarely documented in conventional cybercrime contexts.

Virtual-to-physical attacks refer to illicit endeavors that leverage digitally simulated entities (e.g., digital twins) or virtual reality (VR) sensors (e.g., front-facing cameras) to inflict physical harm within the terrestrial realm. Alongside cyber-physical attacks, which primarily depend on the remote exploitation of digital control systems (e.g., inducing facility overloads and blackouts; He & Yan, 2016), virtual-to-physical attacks expand the spectrum of criminal activities transitioning from cyberspace to offline contexts by encompassing broader targets, such as properties and human being. Three categories of virtual-to-physical attacks have been observed: virtual-to-physical person attacks, virtual-to-physical property attacks, and virtual-to-physical infrastructure attacks (Gómez-Quintero et al., 2024). These attacks might extensively exploit digital twins and VR sensors that simulate or monitor dynamic real-world data. For instance, potential terrorists could exploit the digital twins of specific targets (e.g., personnel within the INTERPOL Centre; see INTERPOL, 2023) for premeditated crimes. In personal settings, motivated offenders might illicitly access users' front-facing cameras on VR devices and other vision-based IoTs, surveilling personal spaces and evaluating the targets' vulnerabilities (e.g., value, inertia, and guardianship).

Immersive virtual reality attacks refer to illicit activities aimed at manipulating virtual environments by modifying the technical configurations of immersive HMDs (Casey et al., 2021). Casey and colleagues (2021) delineated four types of immersive virtual reality attacks, discerned through laboratory experimentation: Chaperone Attack, Disorientation Attack, Human Joystick Attack, and Overlay Attack. The Chaperone Attack involves unauthorized modifications to the boundaries of virtual environments. The Disorientation Attack is characterized by deliberate actions to induce dizziness in users by altering the properties of immersive HMDs. The Human Joystick Attack involves covertly manipulating users' physical movements. Lastly, the Overlay Attack entails the unauthorized superimposition of sensory materials (e.g., images, audio, videos, and other content) onto the user's virtual experience.

Distinct from precedent cybercrime, immersive virtual reality attacks increasingly facilitate a broader spectrum of physical harm and more severe psychological distress. On the one hand, such attacks can directly cause ranges of physical harm, including eye dryness (Hirzle et al., 2022), visual vertigo (Pavlou et al., 2012), motion sickness (Bronstein et al., 2013), and neurologic symptoms (Yoon et al., 2021). Apart from the scenario with implanted medical device hacking (Browning & Tuma, 2016), direct physical harm has seldom been observed in conventional online victimization cases (Gupta & Mata-Toledo, 2016). The literature on cybercrime suggests that most physical harms stem from indirect mechanisms, where online victimization and psychological distress act as pivotal mediators (Chang et al., 2023; Holt & Bossler, 2016; Xu et al., 2024; Zhou et al., 2023). On the other hand, immersive VR attacks can inflict more severe psychological harm compared to conventional cybercrimes (e.g., hacking, cyber fraud, cyberbullying, cyber-stalking). Common psychological conditions resulting from online victimization include social anxiety, depression, post-traumatic stress disorder, and insomnia (Espinoza, 2023; Hu et al., 2021; Kwon et al., 2020). Nevertheless, the psychological impact of immersive virtual reality attacks can be more intrusive due to the malicious and coercive overlaying of abusive content within immersive online environments (see more detailed discussion below). In summary, the metaverse opens new criminogenic opportunities, such as virtual-to-physical attacks and immersive virtual reality attacks, which are feasible to cause direct physical harm and more severe psychological penetration.

The Victimogenic Potential of the Metaverse: Superrealism of Victimization Experience

The experience of metacrime victimization may epistemologically differ from that within non-immersive digital platforms. Nesting in the relationships between cybercrime and offline crimes, one of the significant factors distinguishing the former from the latter is the intensity of the fear of crimes. Individuals often report a lower level of fearfulness toward cyber victimization compared to physical victimization (Abdulai, 2020; Henson et al., 2013; Savimäki et al., 2020). A systematic review of the fear of cybercrime (excluding Metacrime) indicated that between 57 and 79% of respondents do not express concern over cyber victimization (Brands & Van Doorn, 2022). However, the fearfulness toward metacrime victimization must be reevaluated because of situationally distinctive factors in the metaverse, such as immersion and plausibility.

The concept of immersion narrows the experiential chasm between cyberspace and the real world by fostering a sense of presence or plausibility (Slater, 2009). This degree of immersion is gauged by the capacity of HMD systems to deliver an "inclusive, extensive, surrounding, and vivid illusion of reality" (Slater & Wilbur, 1997). Enhanced immersion leads to an increased sense of presence, where individuals perceive virtual environments as tangible spaces rather than mere artificial constructs rendered by HMDs (Slater & Wilbur, 1997). Slater (2009) further defines the sensation of "being in real places" as a "place illusion" and the feeling of events "actually happening" as a "plausibility illusion." Influenced by the quality of sensorimotor contingencies and the emotional valence of VR events, individuals may experience varying degrees of place and plausibility illusions (Slater et al., 2020). Once these illusions are induced, individuals perceive events depicted in HMDs as highly realistic and react genuinely in virtual environments (Slater, 2009). A broad array of empirical research has underscored the pivotal role of immersive VR in evoking psychological, physiological, and behavioral responses analogous to those experienced in the physical world (Chittaro, 2014; Chittaro & Buttussi, 2015; Crescentini et al., 2016; Frost et al., 2022; Rose et al., 2018). Thus, the victimological sensations and experiences in virtual environments may become increasingly indistinguishable from reality.

Considering the senses of immersion and plausibility illusion, it stands to reason that metacrime may lead to more severe psychological, financial, and physical damages than conventional cybercrime. A salient example of this is virtual rape, which involves non-consensual sexual acts perpetrated by avatars against other avatars (Horne, 2023). Victims of virtual rape may endure not only visual and psychological trauma but also unwanted physical contact via real-time haptic feedback. While the intensity, intrusiveness, and severity of virtual sexual crimes cannot fully equate to their offline counterparts due to the lack of physical presence (Dripps, 1992), the harm and trauma felt by victims can be significantly more vivid and distressing, contingent on the degree of plausibility illusion prompted by sensorimotor contingencies and event valence. In essence, the superrealism of victimization experiences is a defining characteristic of metacrime, distinguishing it from the majority of conventional cybercrimes.

Human-Avatar Interactivity Brings New Etiology in Metacrime

The avatar functions as a pivotal element within immersive online environments, facilitating the interaction between physical individuals. In the metaverse, users predominantly rely on avatars for various activities, including communication, interaction, education, entertainment, and shopping (Lee et al., 2021). Although avatars are not an invention exclusive to immersive online environments, metaverse avatars exhibit at least two distinctions from avatars/personas utilized in conventional online platforms. For one thing, the metaverse offers extensive autonomy in avatar customization, in stark contrast to the typically limited and preset options for avatar identities and appearances found in non-immersive digital platforms (Saker & Frith, 2022). For another thing, the integration of sensorimotor contingencies and haptic feedback through HMDs facilitates a proprioceptive alignment between users and their avatars (Lee et al., 2021), a feat that is significantly more challenging to achieve within non-immersive digital environments.

Given the fundamental distinctions between immersive and non-immersive avatars, we contend that human-avatar interactivity could herald a novel dimension for criminological etiology within the metaverse. This assertion is underpinned by posing a pivotal inquiry: how might human-avatar interactivity transform the criminal and victimization experiences within the metaverse? A viable avenue for exploring this question lies in examining human-avatar identity connectivity and the potential for attitudinal and behavioral adaptation. Essentially, we aim to scrutinize how customized virtual identities might influence individuals' attitudinal and behavioral reactions, potentially giving rise to new criminological etiologies in both virtual and physical realms.

According to the Proteus theory, the appearance and attributes of digital avatars can significantly affect users' attitudes and behaviors within virtual environments (Yee & Bailenson, 2007). For instance, Yee and Bailenson (2007) discovered that individuals assigned attractive avatars tend to engage more confidently and share more personal information with a confederate avatar controlled by researchers. Subsequent research has demonstrated that the Proteus effect extends into the terrestrial sphere. Experiments by Yee and colleagues (2009) revealed that participants with taller avatars were more inclined to adopt aggressive negotiation tactics in subsequent face-to-face interactions than those with shorter avatars. Additionally, the transmission of avatar-to-person aggression, influenced by virtual persona characteristics such as race and gender, has been observed both online and offline (Ash, 2016; Eastin, 2006; Hawkins et al., 2021). Therefore, it is plausible to posit that the interplay between avatar customization and embodiment may pave the way for a broad spectrum of novel criminological etiologies distinct from those outside metaverse contexts.

We further illustrate our argument by discussing the interplay between harm neutralization and human-avatar interactivity. Neutralization theory denotes that individuals often employ five principal techniques to justify their deviant or criminal actions: denial of responsibility, denial of injury, denial of victim, condemnation of condemners, and appeal to higher loyalties (Sykes & Matza, 1957). Within the context of metacrime, the endorsement of neutralization can be affected by identity embodiment. Schultze (2014) suggests that the embodiment of virtual identity is either representational or performative. The former refers to avatars that directly reflect an individual's self-attributive characteristics (e.g., appearance, gender, and race), while the latter denotes the avatars that encompass expressive, informative, and creative constitutes (e.g., animals, fantasy creatures, and other self-defined objects). The malleability of avatar identities and the sense of embodiment could affect individuals' reliance on neutralization techniques. For instance, due to self-objectification, individuals with performative (e.g., non-human) avatars might more readily deny responsibility for harm with rationalizations such as "It is only a joke as my avatar is not human." This rationale could be intensified if victims also possess non-human avatars (e.g., "I just punched an object rather than a human"). Furthermore, the malleability of virtual avatars could be exploited to justify actions under the guise of intangible harm (e.g., "My actions have no actual consequences to other users"). Above all, it is theoretically reasonable to assume that dynamic human-avatar interactivity will cast differential influences on individuals' attitudinal apprehension and behavioral responses to abusive circumstances in the metaverse.

New Ethical and Regulatory Dilemmas Elicited by Metacrime

Although metacrime shares a battery of ethical challenges with cybercrime, there remains extensive potential for emerging ethical dilemmas that conventional cybercrime has not encountered, such as *excessive misuse of biometric data* and *increasingly vulnerable populations.* Biometric data spans physiological biometrics (e.g., facial recognition, retina and iris scan, and ear geometry) and behavioral biometrics (e.g., gait, keystroke, and movement analyses). Given the prevalent biometric data collected by HMDs and haptics, there is a growing risk that users' biometric data can be excessively misused in unethical and malicious ways (Slater et al, 2020; Christopoulos et al., 2021). For example, data breaches of metaverse biometric service providers may facilitate the growth of health fraud against metaverse users, especially those with physiologically, behaviorally, and psychologically identifiable illnesses (Brown, 2020; Xu et al., 2024; Zhou et al., 2023). Though the concerns over misusing biometric parameters are not new ethical dilemmas in the cyber sphere (Linnartz & Tuyls, 2003), the interoperability and decentralized features of the metaverse provide congregated opportunities and enormous incentives for motivated offenders to initiate biometric data misuse.

On the other hand, given the age divide in accessing the metaverse, certain demographic groups, especially children and adolescents, are becoming more vulnerable to metacrime. According to lifestyle-routine activity theory (Cohen & Felson, 1979; Hindelang et al., 1978; Holt & Bossler, 2008), individuals who have greater exposure to risky situations have a greater propensity to be targeted by motivated offenders, especially in the contexts lacking capable guardians. A recent survey showed that 26% of Americans aged 13–24 held positive attitudes toward the metaverse, while the figures were only 9% and 4% for the groups aged 35–54 and above 55, respectively (Dixon, 2022). Roblox, an immersive online gaming and interaction platform with VR enablers, had 58% of its users under 16 by the end of 2023 (Clement, 2024). The high concentration of young populations in the metaverse may attract predatory offenders from other realms (both offline and online) to commit child-centric offenses, such as unwanted sexual advances, sexual harassment, and sexual coercion (Henry & Powell, 2018). Consequently, certain demographic groups, especially children and adolescents, are becoming more susceptible and vulnerable in the metaverse compared with conventional online settings.

In the regulatory dimension, metacrime presents novel challenges in defining, measuring, and pursuing avatars' liability that conventional cyberspace does not usually confront. In non-immersive digital platforms with role-play functions (e.g., PvP computer games), no explicit legislation or regulations restrict avatars' aggressive and violent behaviors, such as in-game hurting and killing. The interpretations of the lack of relevant frameworks against avatars' behaviors can be threefold. First, there is a consensus on the unconscionability of non-immersive avatars (Chen & Burgess, 2019), suggesting that digitally performed damages caused by avatars have insignificant impacts on physical entities (Franks, 2011). Second, there are statutory classifications regarding the minimal age for accessing violent video games, protecting children and juveniles from exposure to disproportionally violent scenarios (Australian Classification, 2024). Third, industry standards have restricted development and production protocols for manufacturers, service providers, and retailers, upholding the threshold of acceptable violence intensity (eSafety Commissioner, 2024). Given the above factors, avatars' liability and governance have not been notable issues in cyberspace.

Nevertheless, in the context of the metaverse, the unique metaverse criminality, the superrealism of victimization experiences, and complex human-avatar interactivity may substantially stimulate the demands of introducing explicit codes, policies, and legislation in regulating avatars' behaviors. Due to the emergence of virtual-to-physical attacks and immersive virtual reality attacks, metaverse users are increasingly susceptible to physical harm (Casey et al., 2021; INTERPOL, 2023). Even in cases where physical harm is not involved, the sense of superrealism may penetratively jeopardize victims' psychological well-being (Horne, 2023). Moreover, the complexity of human-avatar interactivity, such as the discrete positions of avatar embodiments, further complicates the subjective apprehension of metaverse perpetration and victimization, emphasizing the need for transparent and targeted governance. The absence of statutory, regulatory, and industrial codes against metacrime will place victims into a legally, psychophysically, and socioeconomically vulnerable situation, which not only fails to protect individuals' rights but undermines democratic legitimacy (Chang & Grabosky, 2017; Kumm, 2004).

Above all, to provide a quick overview of the similarities and differences between metacrime and cybercrime, the key findings have been summarized in Fig. 1.

Discussion and Conclusion

In this study, we have delved into the intricate landscape where metaverse criminality converges and diverges with the conventional characteristics of cybercrime. Our analysis underscores the dual nature of technological progression—as it fosters innovation and connectivity, it concurrently engenders novel forms of criminality that challenge existing legal and regulatory frameworks (Grabosky, 2001). Through a multidisciplinary review of recent literature on metaverse and cybercrime, our findings reveal that while metacrime shares fundamental features with antecedent cybercrime (e.g., crime classification, continuous evolution, global reach, anonymity, and governance challenges), it introduces complex new dynamics that necessitate extensive future

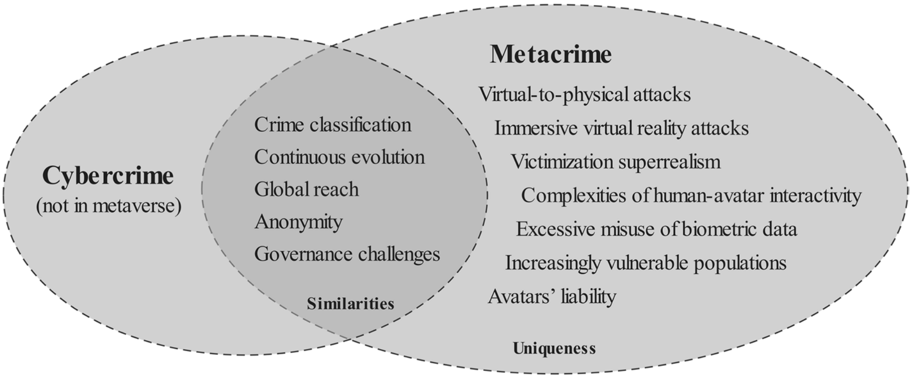
Metacrime
Virtual-to-physical attacks
Immersive virtual reality attacks
Victimization superrealism
Complexities of human-avatar interactivity
Excessive misuse of biometric data
Increasingly vulnerable populations
Avatars' liability
Uniqueness
Cybercrime
(not in metaverse)
Crime classification
Continuous evolution
Global reach
Anonymity
Governance challenges
Similarities

Fig. 1 The similarities and differences between metacrime and cybercrime

research, sophisticated regulatory responses, and networked collaboration to reduce and prevent such emerging criminality. Only by discerning the convergence and divergence between metacrime and cybercrime can we accurately apprehend and assess the metaverse-imposed threats concealed behind the veil of the conventional understanding of cybercrime.

Perhaps under the various metaphors of "bottles and wines," there has been a growing sense of fatigue regarding both exaggerating and underestimating the intimidation posed by technology-facilitated crimes (Parti, 2011; Quigley et al., 2015). From our perspective, we do not endorse any movement and ideologies that incite moral panic or foster emotional apathy toward metacrime. Moreover, we have no intention of fabricating a fantasy concept ontologically diverges from the existing scholarship on cybercrime. Instead, we underscore the significance of recognizing the cyber features of metacrime and emphasize the epistemological uniqueness of metacrime by advocating a balanced and holistic perspective to evaluate its underlying threats and regulatory challenges. We also acknowledge and anticipate that many criminal patterns and characteristics in the metaverse may align with the framework of cybercrime, such as crime classifications, continuous evolution, global reach, anonymity, and difficulties for law enforcement.

Nonetheless, the prevalence of epistemological commonalities between metacrime and cybercrime does not guarantee their invariant parameters. From the criminogenic perspective, metacrime encompasses novel perpetrations, such as virtual-to-physical attacks and immersive virtual reality attacks, that can directly induce physical harm, thereby blurring the lines between cyber abuse and physical victimization. For instance, motivated offenders may exploit simulated digital twins containing personal, spatial, and infrastructural information that is scarcely collected through alternative means (Gómez-Quintero et al., 2024). Such digital exploitation can facilitate groups of offline criminal activities, such as stalking, sexual offenses, and terrorism. Moreover, the manipulation of VR technologies, such as HMDs and haptic suites, enables perpetrators to inflict direct physical harm on metaverse users, such as visual vertigo (Pavlou et al., 2012), motion sickness (Bronstein et al., 2013), and neurologic symptoms (Yoon et al., 2021). Nevertheless, the causality between digital abuse and physical harm has seldom been observed in conventional cybercrime (Gupta & Mata-Toledo, 2016). Therefore, understanding the criminogenic uniqueness of metacrime and introducing correspondent countermeasures are imperative for mitigating threats escalated from digital to physical realms.

Besides, recognizing the salience of victims' perspectives in constructing the epistemology of metacrime victimization is of paramount importance. The superrealism of the immersive online environments will entangle victims into a quagmire where they may acknowledge the virtuality of perpetration but find it challenging to disregard the psychological trauma they experienced. This issue is particularly evident in metaverse-enabled sexual assaults (Camber, 2024), where the traumatic experiences may precipitate anxiety, depression, and post-traumatic stress disorder (Espinoza, 2023; Hu et al., 2021; Kwon et al., 2020). Unfortunately, the antecedent scholarship and regulatory responses have accorded scant weight to victims' perspectives in constructing the epistemology of cyber victimization (Button et al., 2022; Chang et al., 2021; Robalo & Abdul Rahim, 2023). We advocate for extensive attention from researchers, practitioners, and policymakers to explore the role of victimization superrealism in shaping an advanced understanding of metacrime victimization.

Furthermore, given the holographic simulation and user-generated options in the metaverse, the dynamic interactivity between individuals and avatars may reshape the current criminological etiology in the digital realm. We posit that the dynamic human-avatar interactivity will exert differential influences on individuals' attitudinal apprehension and behavioral responses to abusive situations in the metaverse, from both perpetration and victimization perspectives. Specifically, enlightened by the Proteus theory (Yee & Bailenson, 2007) and the neutralization theory (Sykes & Matza, 1957), we elucidated how performative avatars might neutralize perpetrators' apprehension of their harmful behavior. Similarly, the sense of embodiment may also affect victims' perception regarding metacrime victimization, with a higher sense of embodiment presumably leading to a greater sense of victimization penetration. Moreover, based on the existing findings of the Proteus theory (Yee et al., 2009), the Proteus effect may spillover from the metaverse to the terrestrial realm, that is, human-avatar interactivity may (re)shape individuals' attitudes and behaviors in the physical world. One of the typical spillover dispositions has been exemplified by the positive correlation between violent video games and physical aggression (Adachi & Willoughby, 2011; Burkhardt & Lenhard, 2022). Future studies may employ experimental methods to empirically test the influences of human-avatar interactivity in online and offline exploitative scenarios from both perpetrators' and victims' perspectives.

Apart from the common ethical and regulatory challenges confronted by cybercrime, we identified several contemporary dilemmas that have not been prevalently observed in conventional cybercrime. For example, the implementation of HMDs and haptic suites presents a vast opportunity for biometric data misuse in the metaverse. This ethical concern is further exaggerated by the intrinsic feature of interoperability when users' biometric data is transferred across different service providers (Clifford Chance, 2022). Additionally, aligning with the routine activity theory (Cohen & Felson, 1979), populations with greater metaverse usage may experience heightened susceptibility and vulnerability to metacrime. Due to the differential internet skills created by the digital divide (Cullen, 2001; Van Deursen & Van Dijk, 2011), children and adolescents, who occupy a large proportion of active metaverse users, are at increased risk of being targeted by predatory offenders capable of moving across various realms. Moreover, avatars' liability, currently in a legal and regulatory void, may need to be integrated into immersive online environments. In non-immersive digital settings, avatars are considered unconscious and unconscientious, whereas the conditions differ for metaverse avatars, where the extent of superrealism and embodiment is emergent. Future studies should explore adaptive legal frameworks and targeted law enforcement practices to address the unique challenges presented by the metaverse.

Although the current research provides original insights into understanding the relationships between metacrime and cybercrime, particularly the uniqueness of metacrime, the applicability and robustness of the findings are subjected to several exogenous and endogenous factors. First, technological development and hardware limits, such as holographic digital duplication, real-time cloud computing, and display quality, can significantly impact the practical extent of the metacrime uniqueness (Dwivedi et al., 2023). Second, the vast progress in AI (e.g., generative AI, AI-powered neural interface devices, and AI-power holographic HMDs/glasses) may open new avenues for digital criminality, which the current findings may not capture. Third, given the scarcity of literature and scope diversity, this study did not strictly adhere to systematic review guidelines (e.g., Page et al., 2021), potentially leading to omitted findings. Future studies should aim to be more theoretically and methodologically comprehensive by identifying nuanced characteristics of metacrime that may have been overlooked in the present study.

In conclusion, this study highlights the nuanced intersections and epistemological uniqueness of metaverse criminality in the exploration of metacrime versus conventional cybercrime. While metacrime shares foundational elements with cybercrime, it introduces complex new dynamics due to the unique features of the metaverse, necessitating contextualized and advanced understanding and responses to its risk mitigation. The findings underscore the urgency of developing metaverse-specific legal and regulatory frameworks to safeguard the integrity of online virtual immersive interactions, advocating for a comprehensive approach that involves multiple stakeholders to ensure a secure and equitable digital realm.

Funding Open Access funding enabled and organized by CAUL and its Member Institutions. This work was supported by Charles Sturt University under the Sturt Scheme grant and Artificial Intelligence and Cyber Futures Institute (AICF) Seed Funding.

Declarations

Conflict of Interest The authors declare no competing interests.

Ethics Approval This article does not contain any studies with human participants or animals performed by any of the authors.

Informed Consent This article only uses archival data and does not contain any studies with human participants; therefore, it does not require informed consent.

References

Abdulai, M. A. (2020). Examining the effect of victimization experience on fear of cybercrime: University students' experience of credit/debit card fraud. *International Journal of Cyber Criminology,14*(1), 157–174.

Adachi, P. J., & Willoughby, T. (2011). The effect of violent video games on aggression: Is it more than just the violence? *Aggression and Violent Behavior,16*(1), 55–62.

Annison, T. (2022). *The future of financial crime in the metaverse: Fighting crypto-crime in Web 3.0*. Elliptic. https://www.elliptic.co/hubfs/Crime%20in%20the%20Metaverse%202022%20final.pdf. Accessed 4 Mar 2024.

Ash, E. (2016). Priming or Proteus effect? Examining the effects of avatar race on in-game behavior and post-play aggressive cognition and affect in video games. *Games and Culture,11*(4), 422–440.

Australian Classification. (2024). *Does your child play violent video games?* Australian Classification. https://www.classification.gov.au/classification-ratings/whats-ok-for-children/does-your-child-play-violent-video-games#top. Accessed 5 Mar 2024.

Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. *Amazonia Investiga,10*(38), 113–122.

Barlett, C. P. (2015). Anonymously hurting others online: The effect of anonymity on cyberbullying frequency. *Psychology of Popular Media Culture,4*(2), 70.

Beccaria C. (1764) [2016]. *Essay on crimes and punishments*. Transaction Publishers.

Beltrán, M., & Calvo, M. (2023). A privacy threat model for identity verification based on facial recognition. *Computers & Security,132*, 103324.

Bibri, S. E., & Allam, Z. (2022). The metaverse as a virtual form of data-driven smart urbanism: On post-pandemic governance through the prism of the logic of surveillance capitalism. *Smart Cities,5*(2), 715–727.

Bovenzi, G. M. (2023). MetaCrimes: Criminal accountability for conducts in the Metaverse. In *Companion Proceedings of the ACM Web Conference, 2023*, 565–567.

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

Brantingham, P. L., & Brantingham, P. (1995). Crime generators and crime attractors. *European Journal on Criminal Policy and Research,3*(3), 5–26.

Brenner, S. W. (2007). Cybercrime: Re-thinking crime control strategies. In Y. Jewkes (Ed.), *Crime online* (pp. 12–28). Willan Publishing.

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, Law and Social Change,46*, 189–206.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408–433.

Bronstein, A. M., Golding, J. F., & Gresty, M. A. (2013). Vertigo and dizziness from environmental motion: Visual vertigo, motion sickness, and drivers' disorientation. *Seminars in Neurology,33*(3), 219–230.

Brown, E. A. (2020). A healthy mistrust: Curbing biometric data misuse in the workplace. *Stanford Technology Law Review,23*(2), 252–305.

Browning, J. G., & Tuma, S. (2016). If your heart skips a beat, it may have been hacked: Cybersecurity concerns with implanted medical devices. *South Carolina Law Review,67*(3), 637–676.

Burkhardt, J., & Lenhard, W. (2022). A meta-analysis on the longitudinal, age-dependent effects of violent video games on aggression. *Media Psychology,25*(3), 499–512.

Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*. https://doi.org/10.1177/17488958221128128

Camber, R. (2024). *British police probe VIRTUAL rape in metaverse: Young girl's digital persona is sexually attacked by gang of adult men in immersive video game' - sparking first investigation of its kind and questions about extent current laws apply in online world*. Daily Mail. https://www.dailymail.co.uk/news/article-12917329/Police-launch-investigation-kind-virtual-rape-metaverse.html. Accessed 5 Feb 2024.

Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing, Intelligence and Counter Terrorism,13*(3), 285–300.

Casey, P., Baggili, I., & Yarramreddy, A. (2021). Immersive virtual reality attacks and the human joystick. *IEEE Transactions on Dependable and Secure Computing,18*(2), 550–562.

Castaño-Pulgarín, S. A., Suárez-Betancur, N., Vega, L. M. T., & López, H. M. H. (2021). Internet, social media and online hate speech. Systematic review. *Aggression and Violent Behavior,58*, 101608.

Clifford Chance. (2022). *The Metaverse: What are the legal implications?* Clifford Chance. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/02/the-metaverse-what-are-the-legal-implications.pdf. Accessed 16 Feb 2024.

Chang, L. Y. C., & Grabosky, P. (2017). The governance of cyberspace. In P. Drahos (Ed.), *Regulatory theory: Foundations and applications* (pp. 533–551). ANU Press.

Chang, L. Y. C., Mukherjee, S., & Coppel, N. (2021). We are all victims: Questionable content and collective victimization in the digital age. *Asian Journal of Criminology,16*(1), 37–50.

Chang, L. Y. C., Zhou, Y., & Phan, D. H. (2023). Virtual kidnapping: Online scams with 'Asian characteristics' during the pandemic. In R. G. Smith, R. Sarre, L. Y. C. Chang, & L. Y. C. Lau (Eds.), *Cybercrime in the pandemic digital age and beyond* (pp. 109–130). Springer.

Chen, J., & Burgess, P. (2019). The boundaries of legal personhood: How spontaneous intelligence can problematize differences between humans, artificial intelligence, companies and animals. *Artificial Intelligence and Law,27*(1), 73–92.

Cheong, B. C. (2022). Avatars in the metaverse: Potential legal issues and remedies. *International Cybersecurity Law Review,3*(2), 467–494.

Chittaro, L., & Buttussi, F. (2015). Assessing knowledge retention of an immersive serious game vs. a traditional education method in aviation safety. *IEEE Transactions on Visualization and Computer Graphics*, *21*(4), 529–538.

Chittaro, L. (2014). Anxiety induction in virtual environments: An experimental comparison of three general techniques. *Interacting with Computers,26*(6), 528–539.

Christopoulos, A., Mystakidis, S., Pellas, N., & Laakso, M. J. (2021). ARLEAN: An augmented reality learning analytics ethical framework. *Computers,10*(8), 92.

Clement, J. (2024). *Distribution of Roblox audiences worldwide as of December 2023, by age group*. Statista. https://www.statista.com/statistics/1190869/roblox-games-users-global-distribution-age/. Accessed 26 Mar 2024.

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

Corbet, S., Cumming, D. J., Lucey, B. M., Peat, M., & Vigne, S. A. (2020). The destabilizing effects of cryptocurrency cybercriminality. *Economics Letters,191*, 108741.

Council of Europe. (2001). *Convention on cybercrime*. Council of Europe. https://rm.coe.int/1680081561. Accessed 19 Feb 2024.

Crescentini, C., Chittaro, L., Capurso, V., Sioni, R., & Fabbro, F. (2016). Psychological and physiological responses to stressful situations in immersive virtual reality: Differences between users who practice mindfulness meditation and controls. *Computers in Human Behavior,59*, 304–316.

Cross, C., & Layt, R. (2022). "I suspect that the pictures are stolen": Romance fraud, identity crime, and responding to suspicions of inauthentic identities. *Social Science Computer Review,40*(4), 955–973.

Cullen, R. (2001). Addressing the digital divide. *Online Information Review,25*(5), 311–320.

Dixon, S. J. (2022). *Attitudes toward the metaverse among adults and teens in the United States as of May 2022, by age group*. Statista. https://www.statista.com/statistics/1322542/us-attitudes-toward-metaverse-among-adults-teens-by-age-group/. Accessed 22 Feb 2024.

Donner, C. M., Jennings, W. G., & Banfield, J. (2015). The general nature of online and offline offending among college students. *Social Science Computer Review,33*(6), 663–679.

Dripps, D. (1992). Beyond rape: An essay on the difference between the presence of force and the absence of consent. *Columbia Law Review,92*, 1780–1809.

Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., ... Yan, M. (2023). Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse. *Information Systems Frontiers*, 1–44. https://doi.org/10.1007/s10796-023-10400-x

Dyntu, V., & Dykyi, O. (2018). Cryptocurrency in the system of money laundering. *Baltic Journal of Economic Studies,4*(5), 75–81.

Eastin, M. S. (2006). Video game violence and the female game player: Self-and opponent gender effects on presence and aggressive thoughts. *Human Communication Research,32*(3), 351–372.

eSafety Commissioner. (2024). *Industry codes and standards*. eSafety Commissioner. https://www.esafety.gov.au/industry/codes. Accessed 15 Apr 2024.

Espinoza, G. (2023). Personal and witnessed cyber victimization experiences among adolescents at the beginning of the COVID-19 pandemic. *Journal of Child & Adolescent Trauma,16*(3), 509–516.

Franks, M. A. (2011). Unwilling avatars: Idealism and discrimination in cyberspace. *Columbia Journal of Gender and Law,20*, 224.

Frost, S., Kannis-Dymand, L., Schaffer, V., Millear, P., Allen, A., Stallman, H., ... Atkinson-Nolte, J. (2022). Virtual immersion in nature and psychological well-being: A systematic literature review. *Journal of Environmental Psychology*, *80*, 101765.

Gómez-Quintero, J., Johnson, S. D., Borrion, H., & Lundrigan, S. (2024). A scoping study of crime facilitated by the metaverse. *Futures,157*, 103338.

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

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

Gupta, P., & Mata-Toledo, R. (2016). Cybercrime: In disguise crimes. *Journal of Information Systems & Operations Management, 10*(1), 1–10.

Hawkins, I., Saleem, M., Gibson, B., & Bushman, B. J. (2021). Extensions of the Proteus effect on intergroup aggression in the real world. *Psychology of Popular Media,10*(4), 478.

He, H., & Yan, J. (2016). Cyber-physical attacks and defences in the smart grid: A survey. *IET Cyber-Physical Systems: Theory & Applications,1*(1), 13–27.

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse,19*(2), 195–208.

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice,29*(4), 475–497.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Ballinger.

Hirzle, T., Fischbach, F., Karlbauer, J., Jansen, P., Gugenheimer, J., Rukzio, E., & Bulling, A. (2022). Understanding, addressing, and analyzing digital eye strain in virtual reality head-mounted displays. *ACM Transactions on Computer-Human Interaction (TOCHI),29*(4), 1–80.

Holt, T., & Bossler, A. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behaviour,30*, 1–25.

Holt, T. J., & Bossler, A. M. (2012). Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. *Cyberpsychology, Behavior, and Social Networking,15*(9), 464–472.

Holt, T. J., & Lee, J. R. (2022). A crime script analysis of counterfeit identity document procurement online. *Deviant Behavior,43*(3), 285–302.

Hooper, C., Martini, B., & Choo, K. K. R. (2013). Cloud computing and its implications for cybercrime investigations in Australia. *Computer Law & Security Review,29*(2), 152–163.

Horne, C. (2023). Regulating rape within the virtual world. *Lincoln Memorial University Law Review,10*(2), 159–176.

Hu, Y., Bai, Y., Pan, Y., & Li, S. (2021). Cyberbullying victimization and depression among adolescents: A meta-analysis. *Psychiatry Research,305*, 114198.

Hui, K. L., Kim, S. H., & Wang, Q. H. (2017). Cybercrime deterrence and international legislation. *Mis Quarterly,41*(2), 497–524.

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime,18*(1), 11–30.

Ilker, K. A. R. A., & Aydos, M. (2020). Cyber fraud: Detection and analysis of the crypto-ransomware. In *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 0764–0769). IEEE.

INTERPOL. (2023). *Interpol enters the Metaverse* [Video]. YouTube. https://www.youtube.com/watch?v=P5AEedw_r8Q. Accessed 10 Mar 2024.

INTERPOL. (2024). *Metaverse: A law enforcement perspective*. INTERPOL. https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf. Accessed 4 Feb 2024.

Kalyvaki, M. (2023). Navigating the metaverse business and legal challenges: Intellectual property, privacy, and jurisdiction. *Journal of Metaverse,3*(1), 87–92.

Kelling, G. L., & Wilson, J. Q. (1982). Broken windows. *Atlantic Monthly,249*(3), 29–38.

Kennedy, D. C. (2009). In search of a balance between police power and privacy in the cybercrime treaty. In Kennedy (Eds.) *Computer crime*. Routledge.

Kim, D., Oh, S., & Shon, T. (2023). Digital forensic approaches for metaverse ecosystems. *Forensic Science International: Digital Investigation,46*, 301608.

Kraus, S., Kanbach, D. K., Krysta, P. M., Steinhoff, M. M., & Tomini, N. (2022). Facebook and the creation of the metaverse: Radical business model innovation or incremental transformation? *International Journal of Entrepreneurial Behavior & Research,28*(9), 52–77.

Kshetri, N. (2021). *Cybersecurity management: An organizational and strategic approach*. The University of Toronto Press.

Kumm, M. (2004). The legitimacy of international law: A constitutionalist framework of analysis. *European Journal of International Law,15*(5), 907–931.

Kürtünlüoğlu, P., Akdik, B., & Karaarslan, E. (2022). Security of virtual reality authentication methods in metaverse: An overview. *arXiv preprint* arXiv:2209.06447.

Kwon, D., Borrion, H., & Wortley, R. (2024). Measuring cybercrime in calls for police service. *Asian Journal of Criminology*, 1–23. https://doi.org/10.1007/s11417-024-09432-2

Kwon, M., Seo, Y. S., Nickerson, A. B., Dickerson, S. S., Park, E., & Livingston, J. A. (2020). Sleep quality as a mediator of the relationship between cyber victimization and depression. *Journal of Nursing Scholarship,52*(4), 416–425.

Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *arXiv preprint* arXiv:2110.05352.

Linnartz, J. P., & Tuyls, P. (2003). New shielding functions to enhance privacy and prevent misuse of biometric templates. In *International Conference on Audio-and Video-Based Biometric Person Authentication* (pp. 393–402). Springer Berlin Heidelberg.

Lu, Y. (2022). *The metaverse and the NSW government*. Gradient Institute. https://www.digital.nsw.gov.au/sites/default/files/2023-03/the-metaverse-and-the-nsw-government.pdf. Accessed 16 Feb 2024.

Mackenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. *The British Journal of Criminology,62*(6), 1537–1552.

Marcum, C. D., & Higgins, G. E. (2019). Examining the effectiveness of academic scholarship on the fight against cyberbullying and cyberstalking. *American Journal of Criminal Justice,44*, 645–655.

Marshall, A. M., & Tompsett, B. C. (2024). The metaverse—Not a new frontier for crime. *Wiley Interdisciplinary Reviews: Forensic Science,6*(1), e1505.

McCuddy, T., & Esbensen, F. A. (2017). After the bell and into the night: The link between delinquency and traditional, cyber-, and dual-bullying victimization. *Journal of Research in Crime and Delinquency,54*(3), 409–441.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications.* Home Office Research Report.

Mejri, M., Othman, H. B., Al-Shattarat, B., & Baatour, K. (2022). Effect of cultural tightness-looseness on money laundering: A cross-country study. *Journal of Money Laundering Control,25*(2), 414–426.

Merck, M. (2015). Masked men: Hacktivism, celebrity and anonymity. *Celebrity Studies,6*(3), 272–287.

Meta. (2024). *What it the metaverse*. https://about.meta.com/what-is-the-metaverse/. Accessed 13 Mar 2024.

Nix, N. (2024). *Attacks in the metaverse are booming: Police are starting to pay attention*. The Washington Post. https://www.washingtonpost.com/technology/2024/02/04/metaverse-sexual-assault-prosecution/. Accessed 25 Feb 2024.

Nolan, A. (2015). *Cybersecurity and information sharing: Legal challenges and solutions* (Vol. 5). Congressional Research Service.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *bmj, 372*(n71)*,* 1–9.

Parti, K. (2011). Actual policing in virtual reality-A cause of moral panic or a justified need? In Kim, J.J. (Eds.), *Virtual Reality*. InTech Open.

Pavlou, M., Kanegaonkar, R. G., Swapp, D., Bamiou, D. E., Slater, M., & Luxon, L. M. (2012). The effect of virtual reality on visual vertigo symptoms in patients with peripheral vestibular dysfunction: A pilot study. *Journal of Vestibular Research,22*(5–6), 273–281.

Payne, B. K. (2020). Defining cybercrime. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 3–25). Palgrave Macmillan.

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

Pittaro, M. L. (2007). Cyber stalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology,1*(2), 180–197.

Quigley, K., Burns, C., & Stallard, K. (2015). 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly,32*(2), 108–117.

Ritterbusch, G. D., & Teichmann, M. R. (2023). Defining the metaverse: A systematic literature review. *Ieee Access,11*, 12368–12377.

Robalo, T. L. A., & Abdul Rahim, R. B. B. (2023). Cyber victimization, restorative justice and victim-offender panels. *Asian Journal of Criminology,18*(1), 61–74.

Rose, T., Nam, C. S., & Chen, K. B. (2018). Immersion of virtual reality for rehabilitation-review. *Applied Ergonomics,69*, 153–161.

Saker, M., & Frith, J. (2022) Contiguous identities: The virtual self in the supposed metaverse. *First Monday, 27*(3). https://doi.org/10.5210/fm.v27i3.12471

Sarre, R., Lau, L. Y. C., & Chang, L. Y. (2018). Responding to cybercrime: Current trends. *Police Practice and Research,19*(6), 515–518.

Savimäki, T., Kaakinen, M., Räsänen, P., & Oksanen, A. (2020). Disquieted by online hate: Negative experiences of Finnish adolescents and young adults. *European Journal on Criminal Policy and Research,26*, 23–37.

Schultze, U. (2014). Performing embodied identity in virtual worlds. *European Journal of Information Systems,23*(1), 84–95.

Seo, S., Seok, B., & Lee, C. (2023). Digital forensic investigation framework for the metaverse. *Journal of Supercomputing,79*(9), 9467–9485.

Singh, C. (2024). Artificial intelligence and deep learning: Considerations for financial institutions for compliance with the regulatory burden in the United Kingdom. *Journal of Financial Crime,31*(2), 259–266.

Slater, M. (2009). Place illusion and plausibility can lead to realistic behaviour in immersive virtual environments. *Philosophical Transactions of the Royal Society B: Biological Sciences,364*(1535), 3549–3557.

Slater, M., Gonzalez-Liencres, C., Haggard, P., Vinkers, C., Gregory-Clarke, R., Jelley, S., ... Silver, J. (2020). The ethics of realism in virtual and augmented reality. *Frontiers in Virtual Reality*, *1*, 512449.

Slater, M., & Wilbur, S. (1997). A framework for immersive virtual environments (FIVE): Speculations on the role of presence in virtual environments. *Presence: Teleoperators and Virtual Environments,6*(6), 603–616.

Smaili, N., & de Rancourt-Raymond, A. (2024). Metaverse: Welcome to the new fraud marketplace. *Journal of Financial Crime,31*(1), 188–200.

Smith, R. G. (2013). Identity theft and fraud. In Y. Jewkes & M. Yar (Eds.), *Handbook of internet crime* (pp. 273–301). Taylor and Francis.

Steele, P., Burleigh, C., Kroposki, M., Magabo, M., & Bailey, L. (2020). Ethical considerations in designing virtual and augmented reality products—Virtual and augmented reality design with students in mind: Designers' perceptions. *Journal of Educational Technology Systems, 49*(2), 219–238.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review,22*(6), 664–670.

Tiwari, M., Lupton, C., Bernot, A., & Halteh, K. (2024). The cryptocurrency conundrum: The emerging role of digital currencies in geopolitical conflicts. *Journal of Financial Crime, Ahead-of-Print.*https://doi.org/10.1108/JFC-12-2023-0306

Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems,49*(4), 710–729.

United Nations. (2000). *10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders*. United Nations. https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf. Accessed 23 Feb 2024.

Urbas, G. (2018). Old wine, opaque bottles? Assessing the role of Internet intermediaries in the detection of cybercrime. In L. Y. Chang & R. Brewer (Eds.), *Criminal justice and regulation revisited* (pp. 132–146). Routledge.

Van Deursen, A., & Van Dijk, J. (2011). Internet skills and the digital divide. *New Media & Society,13*(6), 893–911.

Wall, D. S. (1999). Cyber crimes: New wine, no bottles? In P. Davies, P. Francis, & V. Jupp (Eds.), *Invisible crimes: Their victims and their regulation* (pp. 105–139). Macmillan.

Wall, D. S. (2007a). *Cybercrime: The transformation of crime in the information age*. Polity.

Wall, D. S. (2007b). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research,8*(2), 183–205.

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials,25*(1), 319–352.

Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J. L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior,40*(1), 40–55.

Weulen Kranenbarg, M., Ruiter, S., & Van Gelder, J. L. (2021). Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders. *European Journal of Criminology,18*(3), 386–406.

Weulen Kranenbarg, M., Ruiter, S., Van Gelder, J. L., & Bernasco, W. (2018). Cyber-offending and traditional offending over the life-course: An empirical comparison. *Journal of Developmental and Life-Course Criminology,4*, 343–364.

Williams, M. (2006). *Virtually criminal: Crime, deviance and regulation online*. Routledge.

Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., & Zheng, Z. (2023). Financial crimes in Web3-empowered metaverse: Taxonomy, countermeasures, and opportunities. *IEEE Open Journal of the Computer Society,4*, 37–49.

Xu, J., Sun, G., Wu, S., Zhu, S., & Zhou, Y. (2024). Understanding health fraud offenders in China: An emotional labour perspective. *Asian Journal of Law and Society,11*(1), 54–69.

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

Yee, N., & Bailenson, J. (2007). The Proteus effect: The effect of transformed self-representation on behavior. *Human Communication Research,33*(3), 271–290.

Yee, N., Bailenson, J. N., & Ducheneaut, N. (2009). The Proteus effect: Implications of transformed digital self-representation on online and offline behavior. *Communication Research,36*(2), 285–312.

Yoon, H. J., Moon, H. S., Sung, M. S., Park, S. W., & Heo, H. (2021). Effects of prolonged use of virtual reality smartphone-based head-mounted display on visual parameters: A randomized controlled trial. *Scientific Reports,11*(1), 15382.

Zhou, Y., Xu, J., Wu, S., & Zhu, S. (2023). Health fraud against the elderly in China: The perspective of vulnerability manipulation. *Victims & Offenders,18*(7), 1354–1372.

Zoltick, M. M., & Maisel, J. B. (2023). Societal impacts: Legal, regulatory and ethical considerations for the digital twin. In N. Crespi, A. T. Drobot, & R. Minerva (Eds.), *The digital twin* (pp. 1167–1200). Springer International Publishing.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.