Futures 157 (2024) 103338

Contents lists available at ScienceDirect

Futures

journal homepage: www.elsevier.com/locate/futures

A scoping study of crime facilitated by the metaverse

Juliana Gómez-Quintero [a], Shane D. Johnson [a,b,*], Hervé Borrion [a], Samantha Lundrigan [c]

[a] UCL Department of Security and Crime Science, University College London, UK
[b] Dawes Centre for Future Crime at UCL, University College London, UK
[c] Policing Institute for the Eastern Region (PIER), Anglia Ruskin University, UK

ARTICLE INFO

Keywords:
Metaverse
Crime
Future threats
Nominal group technique

ABSTRACT

The metaverse is an emerging convergence of technologies (e.g., virtual reality and blockchains) that enables users to experience mixed/extended realities for various legitimate purposes (e.g., gaming, tourism, manufacturing and education). Unfortunately, the crime and security implications of emerging technologies are often overlooked. To anticipate crimes that the metaverse might facilitate, we report the findings of a nominal group technique (NGT) study, which involved a state-of-the-art scoping review of the existing literature and elicitation exercises with two groups of experts (one a diverse group from the UK and Europe, the other representing international law enforcement) with a wide range of expertise. A total of 30 crime threats were identified in the literature or by participants. The elicitation exercises also explored how harmful, frequent, achievable and defeatable participants anticipated that the crimes identified would be. Ratings for these aspects were largely consistent across the two samples, with crimes of a sexual nature (e.g., child sexual abuse material), and crimes against the person (e.g., hate crime) being rated as presenting the highest future risks (i.e. being high harm and high frequency) and being the most difficult to address. The findings illuminate understanding of the most (and least) harmful and likely crime threats the metaverse could facilitate and consequently help stakeholders to prioritise which offences to focus on. In discussing how the crime threats might be addressed, we consider roles and responsibilities and how theory about the management of physical places might inform crime prevention in the metaverse(s).

1. Introduction

While the term “metaverse” was initially coined by Neil Stephenson in 1992 in his novel Snow Crash, it is only relatively recently that social media, technology, and gaming companies have started to buy into and develop the technology required to make it a reality. However, these developments are significant. For example, in October 2021 Facebook announced their transition to become known as Meta and their ambition to create the “metaverse”. Their acquisition of Oculus, a manufacturer of Virtual Reality headsets, exemplifies their commitment to this vision. Meanwhile, Microsoft has invested in the development of Mesh for Microsoft Teams, a platform where

* Correspondence to: Dawes Centre for Future Crime at UCL, University College London, 35 Tavistock Square, London, WC1H 9EZ, UK
E-mail address: shane.johnson@ucl.ac.uk (S.D. Johnson).

https://doi.org/10.1016/j.futures.2024.103338
Received 19 April 2023; Received in revised form 17 November 2023; Accepted 4 February 2024
Available online 12 February 2024

people in separate locations will be able to interact in a shared virtual environment using holograms (Roach, 2021). The company also purchased Activision Blizzard, a major gaming company. This acquisition is intended to grow Microsoft's gaming division and provide the foundations for developing the metaverse (Microsoft News Center, 2022). Fortnite, Roblox,[1] Minecraft, Sandbox and Decentraland are examples of existing platforms that are already starting to offer virtual reality and immersive experiences (McKinsey & Company, 2022), and companies to include Google and Amazon are also leading developments in this space (for more details on companies involved, see Ning et al., 2021). With this level of investment, Bloomberg estimates that the metaverse industry will be worth USD 800 billion by 2024 (Kanterman & Naidu, 2022), and McKinsey & Company (2022) estimate that it may generate up to USD 5 trillion by 2030.

As a recent concept, it is still being determined what precisely the metaverse is or will be. Academic discussions tend to focus more on virtual reality, whilst news and social media comment on economic and social factors (Green & Works, 2022). However, both academics and industry have used terms such as virtual worlds (Grayscale Investments LLC, 2021; Krotoski, 2022); a technology platform (Callaghan, & Kanterman & Naidu, 2022), a network (Ball, 2021; Ma, 2022; Parisi, 2021), a combination of virtual and mixed reality (Lovich, 2022), a shared virtual space (Sin & Kanterman, 2022), and a new paradigm that will succeed the Internet (Ball, 2021; Callaghan, n.d.; Deloitte, 2022; Foutty & Bechtel, 2022; Harris, 2022; McKinsey & Company, 2022; McKinsey Technology Council, 2022a; Morini Bianzino, 2022; Newton, 2021; Parisi, 2021; Wang et al., 2022). Kanterman and Naidu (2022, p. 1) combine many of these terms to argue that "*the metaverse is the convergence of the physical and digital realms in the next evolution of the internet and social networks using real-time 3D software*". In terms of use cases, as discussed in more detail below, it is anticipated that these will be varied but will include entertainment, hospitality and tourism, work and collaboration, manufacturing, education and training, retail and advertising, and health and wellbeing.

Unfortunately, when new products and services are introduced, it is common for their crime and security implications to be overlooked, or inadequately addressed. This can result in what Pease (1997) refers to as a crime harvest, whereby offenders exploit the crime opportunities the new technology affords (Norman, 2013) (see also, Norman, 1988; Walker, 2017) until these are addressed. Crime harvests have been observed for many products and services in recent decades, including vehicles in the 1990 s (e.g., Laycock, 2004), mobile phones in the noughties (e.g., Mailley et al., 2008) and cryptocurrencies most recently (e.g., Trozze et al., 2022). The metaverse may be added to this list, and many have started to point out potential crimes that may be of concern. Misuses may be perpetrated by users of the metaverse(s), *or* those who own the infrastructure or provide metaverse services. For example, in the 'Gaming' episode of the 'The Future Of' series (Lebowits, 2022) the presenter notes that if users wish to play AR-games in their homes, they will have to provide detailed spatial data about such private spaces. In this scenario, an important question concerns the uses to which these types of data will be put by those who collect it. On the other hand, users of the metaverse may themselves engage in malicious activity, such as the forms of cybercrime that we already see happening on the internet and Social Networks (e.g., scams, fraud, harassment, and using bots or trolls). For example, in the Sum of Us (2022) report on the metaverse, the authors describe several incidents in which users testing Meta's Horizon Worlds platform reported that avatars, controlled by other users, used violent and sexually abusive vocabulary to harass or force them into virtual sexual and non-consensual interactions (e.g., closely approaching female looking avatars from behind and simulating arousal). While many of these crimes may be possible on the internet as we experience it today, as we will discuss below, the immersive nature of the metaverse(s) will (for example) likely make the experience of some of these harms (e.g. hate crime and sexual offences) more traumatic.

Apropos how the metaverse may influence crime opportunity from a theoretical perspective, consider the routine activity approach. This is an ecological theory which states that crime is more likely to occur when a motivated offender encounters a suitable target in the absence of capable guardianship (Cohen & Felson, 1979). Capable guardians are not limited to the police or security guards but include anyone or anything that can act to deter offenders or protect a potential target. Place managers (Eck & Madensen-Herold, 2018) – those who have the legal authority to exert control over a place (however defined) – can also play an important role by designing spaces to make them more secure, or by training staff (or others) to provide the necessary guardianship. Changes to any of the ecological conditions described (e.g., the availability of suitable targets) will affect the likelihood of crime. Unlike the physical world, activity in existing online environments is not limited by space, which increases the "mobility" of offenders, targets, and guardians, changing the likelihood with which they will interact. The metaverse(s) will also enable such hyper-mobility but will also extend the types of interaction possible, and hence the impact that these may have on people, including victims of crime.

Considering uses cases, the metaverse has the potential to substantially shape the routine activities of specific individuals but also users at large, thereby affecting crime opportunity at scale. Of course, crime does not simply occur when offenders and targets encounter each other. According to the rational choice perspective, this depends on offender perceptions of the risk, effort and reward involved in offending (Cornish & Clarke, 1987). The metaverse may disrupt all three. For example, unless adequate place management strategies are implemented, or informal guardianship is effective (e.g., if others present in situations intervene when offences are likely), for some forms of offending, relative to existing on- or off-line situations, the perceived (and possibly the actual) risk and effort involved in offending in the metaverse(s) may be relatively low, while the perceived rewards may be relatively high.

Although there is much uncertainty about the actual crimes that could be enabled by the metaverse, anticipating the possible threats now is important. So doing can help stakeholders such as policing agencies, regulators, governments, and service providers to prepare for what might be to come and ideally address such threats before new crime harvests emerge. To this end, in this paper we

[1] For example, Roblox supports different technologies to enable 3D and virtual reality (VR) experiences, although it has some limitations in the sensors used and the tracking that is possible; it has been used in educational settings (e.g., used of VR to explore sculptural heritage in urban settings), for concerts (One World) and uses its own virtual currency (Park & Kim, 2022).

report the findings of a "futures" study – a form of study intended to explicitly examine future uncertainties (see Craig, 2018). This involved a state-of-the-art scoping review of the existing literature, which was followed by two workshops. The key aims of the workshops were to discuss the risks identified in the scoping review, identify further potential crimes that exist now or that may emerge in the future, and to elicit expert opinion on which of the threats are of most concern. The first workshop involved a diverse range of participants from academia, law enforcement, industry, the voluntary sector, and government, mostly from the UK and mainland Europe. To elicit more of an international perspective, the second workshop was conducted with law enforcement officers from around the world. To give the reader a little more context about the metaverse and the crime opportunities that it might facilitate, the next section of the paper provides a brief discussion of the technologies and attributes that are commonly associated with the metaverse. Subsequently, we describe the search methodology employed to conduct the systematic scoping review of the literature. This is followed by a description of the workshops conducted and the findings from them. The paper concludes with a discussion of our findings and potential measures that could be implemented to prepare for and prevent crimes that might be facilitated by the metaverse.

1.1. Technologies and attributes of the metaverse

Myriad technologies will be required to enable the metaverse. Virtual Reality (VR) and Augmented Reality (AR) devices already serve as types of access points through which individuals will access the metaverse (Deloitte China, 2022). However, in the future, smart phones, and laptops, along with other emerging devices (e.g., mixed-reality devices – MR, or brain-computer interfaces – BCI) are expected to serve as entry points (McKinsey & Company, 2022). These technologies and others, including GPS and the Internet of Things, will also facilitate intelligent sensing to capture data about individuals (location, movements, biometrics, etc.) and use this as input to actions in the virtual environment. Extended reality[2] (XR) technologies will allow the blending of physical and virtual entities into one experience. Blockchain technology will provide the metaverse with unique identifier and authentication mechanisms that will underpin transactions and the ownership of digital assets (Deloitte China, 2022). For example, cryptocurrencies and Non-Fungible Tokens (NFTs), which are already used by platforms such as Decentraland and Sandbox (Lovich, 2022), will enable economic transactions in the metaverse. Other technologies expected to facilitate the decentralisation of the metaverse include the broader set of Decentralized Finance (DeFi)[3] functionalities and Decentralized Autonomous Organizations (DAOs) which allow decision making by communities rather than a central authority (Parisi, 2021). Network and computing technology will be required to ensure continuous large-scale multi-user activity that allows seamless, real-time immersive interactions in the metaverse(s). Example technologies include Space-air-ground-sea integrated networks – SAGSIN – (Tang et al., 2022), supercomputers, cloud computing (Singh, 2022), 5 G and edge computing (McKinsey Technology Council, 2022b). Artificial Intelligence (AI) technologies (e.g., machine learning and natural language processing) will enable immersive experiences by optimising how digital user representations and virtual entities interact (Deloitte China, 2022). AI will also operate in the background to customise the user experience (Harris, 2022) and overall, will contribute to operation in real time and multidimensional interaction (Deloitte China, 2022).

Despite variation in descriptions of what the metaverse(s) is, there is some degree of consensus on what its attributes are or will be. For example, Forster (2022) recently published a taxonomy of ten attributes that will characterise the metaverse: multiuser, multi-purpose, user-generated, spatial, immersive, persistent (e.g., digital assets will not expire when a game ends), multiplatform (i.e., there will likely be multiple interconnecting platforms), interoperable (e.g., users will be able to move between platforms), and involve ownership (of digital assets such as land, cryptocurrencies etc) and avatars (i.e., there will be digital representations of users). Many other authors discuss these attributes (for examples, see defintions in Deloitte, n.d.; Deloitte China, 2022; Herrman & Browning, 2021; Krotoski, 2022; Lovich, 2022; Ma, 2022; McKinsey & Company, 2022; Mystakidis, 2022; Ravenscraft, 2022; Wang et al., 2022), although some note that avatars may or may not be necessary (Parisi, 2021). Other suggested attributes include synchronicity, as in synchronous communications, interactions, and transactions (Clark, 2021; Ernst & Young Global Ltd, 2022; Grayscale Investments LLC, 2021), virtual-physical hybridity (i.e., where what an individual experiences is a mixture between the physical and virtual worlds) (Deloitte, 2022; Grayscale Investments LLC, 2021; McKinsey & Company, 2022; McKinsey Technology Council, 2022b), open (meaning that anyone can create content) (Grayscale Investments LLC, 2021; Parisi, 2021), live (Ernst & Young Global Ltd, 2022), decentralised (Ball, 2021; Deloitte China, 2022; Parisi, 2021), hyper spatiotemporal (i.e., the ability to switch from one virtual space to another seamlessly), scalable (i.e., remaining efficient despite a growing number of users, interactions and complexity), and heterogeneous (e.g., in terms of platforms, devices, data types, and communication modes) (Wang et al., 2022).

1.2. Metaverse applications

As a multipurpose virtual world, the metaverse will offer a diverse range of applications and use cases. As listed in Table 1, the main sectors are likely to be gaming, art and entertainment, hospitality and tourism, work and collaboration, education and training, retail and advertising, and health and wellbeing. Relevant to many of these applications is the creation of digital twins (DTs); that is, "digital

[2] XR is an umbrella term for VR, AR and MR. These technologies involve different degrees of immersion in the virtual world, starting from AR (a superposition of virtual elements on the physical environment), then MR (a mixture of physical and virtual elements where these can interact), ending with VR (a fully virtual environment) (Ziker et al., 2021).

[3] DeFi are "a new breed of consumer-facing financial applications composed as smart contracts, deployed on permission-less blockchain technologies" (Jensen et al., 2021, p. 46)

Table 1
Examples of applications of the metaverse in different sectors.

Sector	Examples of metaverse applications	Source (s)
Gaming	Sandbox, an immersive virtual world using blockchain where users can create 3D games and monetise them.	(Christodoulou et al., 2022)
Entertainment	Virtual Concerts held in immersive platforms (e.g., Roblox)	(Park & Kim, 2022)
Creative industry	Computer-rendered imagery (e.g., virtual photography and cinema, 3D digital portraits); virtual calligraphy using AI; production of audio and musical material using AI.	(Lee et al., 2021)
Hospitality and tourism	Virtual flights; using VR to experience outdoor adventures (e.g., kayak in a remote location); data about locations provided via AR to tourists; virtual tours and hotels (e.g., so that clients can try before booking); experiencing destinations in-person and virtually using DT.	(Gursoy et al., 2022)
Work and collaboration	Meetings and office spaces (e.g., Branch, Gather, Teamflow).	(Park & Kim, 2022)
	Conferences.	(Thomason, 2021)
Manufacturing and logistics	Testing products; optimising production processes (e.g., BMW uses Ominverse to coordinate car production across their factories).	(Alkazzi & Rizk, 2020; Chang et al., 2022)
Education, and training	Immersive learning-by-making experiences (e.g., building virtually; virtually visiting places with cultural heritage (e.g., Taj Mahal); practicing high-risk scenarios virtually (e.g., fire escapes and surgeries); immersive experiences of past eras; gaming to develop skills (e.g., problem solving and critical thinking).	(Kye et al., 2021)
Retail and Advertising	Virtual environments for brand merchandising and immersive buying experiences (e.g., Nike; Sketchers; Puma).	(Kim, 2021)
	Brands creating digital representations (e.g., Gucci introduced a virtual sneaker that can be worn via AR); luxury brand collectibles as NFTs; digital fashion (i.e., companies dedicated to designing purely virtual attires – e.g., Dress X)	(Joy et al., 2022)
	Several brands have filed trademarks for selling virtual goods and creating metaverse environments (e.g., Johnson & Johnson, L'Oreal, Chuck E. Cheese and McDonald's).	(Gonzalez, 2022)
Health and wellbeing	Surgical procedures using AR; socialisation and gamification of services; dynamic monitoring of health and sports training.	(Thomason, 2021)
	Testing of machines, systems and procedures using DT; using AR, real-time guidance could be provided to a surgeon within their field of view during a surgery; AI supported decision making to tailor medical decisions to patients; surgical simulations; diagnostic imaging; using a move-to-earn approach to rehabilitation (e.g., playing metaverse games to motivate patients as physiotherapy),	(Chen & Zhang, 2022)
Social media	Immersive virtual places where people can meet and interact (e.g., VR Chat); VR experiences created by influencers for followers	(Huq et al., 2022)

replications of living as well as non-living entities that enable data to be seamlessly transmitted between the physical and virtual worlds" (El Saddik, 2018, p. 87). For example, platforms such as NIVIDIA's Omniverse allow companies to create DTs of factories, health care facilities and other 3D spaces with realistic detail (Accenture, 2022; Deloitte China, 2022). Use cases for DTs include the optimisation of the output and efficiency of processes (El Saddik, 2018), and preparedness training for low-frequency high–impact events, such as the policing of terrorist attacks (in replicas of real locations), or the handling of volatile materials in high-stress scenarios.

In the sections that follow, we discuss the methods used for the scoping review of the literature and the expert elicitation exercises.

2. Scoping review methodology

Systematic reviews (Gough et al., 2017) have emerged as a transparent method for synthesising evidence on a particular topic. Unlike ad-hoc literature reviews, they include the use of an explicitly stated and repeatable search strategy, and the adoption of clear inclusion/exclusion criteria which are used to identify articles that are within the scope of the review. Scoping reviews (Grant & Booth, 2009) are a type of systematic review typically used to synthesise existing evidence when there are high levels of uncertainty regarding what is known (Arksey & O'Malley, 2005; Peters et al., 2020) about a topic, as is the case when investigating future crimes. They are conducted with the same rigour as a systematic review but often have more open aims than do systematic reviews. A growing number of studies (e.g., Akartuna et al., 2022; Trozze et al., 2022) have adopted this approach as an initial step towards understanding future crime risks, and it is this approach that we employ here. In conducting the review, we followed the Preferred Reporting Items for Systematic reviews and Meta-Analyses extension for Scoping Reviews or PRISMA-ScR, which details what should be included in a scoping review and how it should be reported (Tricco et al., 2018). This includes reporting the electronic databases searched, the study eligibility criteria employed, and so on.

2.1. Search strategy

We used ProQuest Central (a multidisciplinary data base covering topics such as business, health, social sciences and technology, which also includes a wide range of sources including academic journals, preprints, magazines, newspapers, industry and market reports and dissertations), ACM (which provides coverage of the computer science and information security literature) and IEEE Xplore (which covers journals, conference and book materials on electrical engineering, computer science, and electronics) to identify academic records. ProQuest was also used to identify records in newspapers, magazines, dissertations, preprints, and market reports. A Google search was conducted to identify potentially relevant (industry and other) reports produced by organisations that do not

publish in academic journals and that would not be captured by the other search engines. All searches were completed in August 2022. Experts invited to the workshops (see below) were also contacted to identify additional records. Collectively, these steps ensured that we covered all relevant forms of literature, including the "grey literature".

Before conducting the search, search terms were piloted and refined to achieve a balance between *sensitivity*, i.e., retrieving a high proportion of relevant articles, and *precision*, i.e., retrieving a low proportion of irrelevant articles (Tompson & Belur, 2016). For example, to capture articles concerned with the Metaverse, we considered including the terms "Augmented Reality, AR, Virtual Reality, VR, Extended Reality, XR" and similar concepts. However, pilot searches revealed that these phrases identified articles that were specific to these technologies but not to the metaverse. Moreover, the inclusion of such terms would imply the need to also search for all metaverse supporting technologies such as blockchain, AI, and VR. This would widen the scope of the search, and substantially reduce precision. For these reasons, we decided to use terms that an initial review of papers suggested were used interchangeably with the term "metaverse" (see Table 2),[4] to search the titles and abstracts of all records indexed by the search engines. To increase the precision of the Google search we used only "metaverse" as a keyword for the technology component of the search.

To capture articles concerned with crime, we used general terms typically used in the criminology literature such as crime, offense, and so on (see Table 2). The term fraud was also used as it was evident from our initial searches that this type of crime was commonly discussed in the literature. However, the exclusion of this term led to the identification of the same (number of) articles for synthesis and hence excluding this term would not have affected the results that follow.

An academic librarian was consulted to validate the databases and search terms selected, and we circulated the search strategy to the INTERPOL Innovation Centre for comment prior to conducting the searches (no changes were requested).

2.1.1. Eligibility criterion

Records had to meet several criteria to be included in the scoping review (SR). They had to be written in English, discuss the metaverse and at least one crime that could potentially occur in this environment. National level threats, including terrorism, were outside the scope of this study. To make our search as broad as possible, we included studies or reports employing any type of study design (e.g., qualitative and quantitative, including systematic reviews and meta-analyses, RCTs, cohort studies, case-control studies, cross-sectional surveys, case reports, position papers, book chapters). We also included all forms of articles including blogs, magazines, or newspaper articles. Records that were behind a paywall that we did not have access to were excluded. Finally, to ensure their relevance (as technology advances quickly), as is common with reviews of this kind, records had to have been published from 2017 onwards.

To test for Inter-rater reliability (IRR) in the application of the inclusion criteria, two researchers independently screened the titles and abstracts of 10% of the records identified. IRR was assessed based on two coding categories (i.e., inclusion versus exclusion) using the prevalence- and bias-adjusted kappa (PABAK) statistic, which controls for chance agreement. 100% agreement was achieved between the two reviewers on the first attempt and hence one researcher screened the remainder of the records.

2.1.2. Study selection and characteristics

Fig. 1 shows the PRISMA-ScR (Moher et al., 2009) flow diagram for the SR. A total of 360 records were identified in academic databases and 14 additional records were either already known by the researchers via a preliminary literature review, supplied by experts invited to the sandpit, or identified through backward searches. An additional 49 records were identified through the Google search. After duplicates were removed, 380 records remained. The titles and abstracts of the remaining records were screened for relevance, and 182 proceeded to the full text review. As shown in Fig. 1, 143 records were excluded because they did not meet the inclusion criteria (58), they only mentioned crime threats but did not describe scenarios (46), were duplicates of records (18), were behind a paywall or the full text did not exist (e.g., it was an abstract presented at a conference) (4) or they were not the primary source (17). In the latter case, the source record was identified and included in the review.

2.2. Data extraction and synthesis

A proforma *(*i.e*., a template)* was developed to extract information from each included article (see Table 3). The initial version was piloted by three researchers on a sample of articles to ensure that relevant information was captured reliably, and the proforma updated, as needed.

To identify crime threats, we did not use an existing classification of crime types such as those developed by the UK Home Office,[5] or other organisations. The reasons for this are that definitions of crime types vary by jurisdiction, and while such classifications are useful for official statistics and prosecution, they often lack the detail necessary to understand a problem. For example, the UK Home Office counting rules associated with computer misuse are effectively limited to the "unauthorised access of computers", which is too broad for the research described here where the intent is to understand the specific ways in which the technology might be misused for criminal purposes. Also problematic is the fact that there is a considerable latency associated with the incorporation of modern forms of offending in official classifications, and future crime risks are excluded from them. For these reasons, and because researchers

[4] The use of these additional terms (as opposed to using only the term "metaverse") did, of course, increase the number of articles that had to be manually checked, but this reduced the likelihood of excluding articles that were about a metaverse but that did not use the term explicitly in the abstract or title of the paper.

[5] See, https://www.gov.uk/government/publications/counting-rules-for-recorded-crime.

Table 2
Search strings used for searches on academic databases and Google.

Database	Search string
Databases (ProQuest, ACM & IEEE)	(Metaverse OR "virtual worlds" OR "immersive internet" OR "multiuser virtual environment") AND (crim* OR offen* OR risk* OR threat* OR vulner* OR abus* OR security OR fraud*)
Google	"Metaverse" (crime OR offense OR risk OR threat OR vulnerability OR abuse OR security OR fraud)

NOTE: *indicates a wildcard which is used to search for variations of a word (e.g., crim* would find words such as "crime" and "criminal"). Unlike the other search engines, Google does not allow the use of wildcards (although it does identify variants e.g., "crime" and "crimes"). Consequently, we included the full terms for the Google search.

described the crime threats in a variety of ways and in varying levels of detail, to allow the crime threats (including future risks) to emerge, a thematic approach (Thomas & Harden, 2008) was taken to (inductively) identify themes/crime threats in the literature. In addition to capturing crime types, we also captured *crime threat scenarios* by which we mean a description of how a crime could be committed in the metaverse. Only crime threat scenarios that do or could take place in the metaverse were included. For example, crimes involving the use of IoT devices to eavesdrop in people's homes (Blythe & Johnson, 2021) that did not involve other metaverse features or technologies (e.g., using a metaverse virtual space to access IoT devices, using Digital Twins to identify IoT) were excluded.

3. Expert consensus method

3.1. Workshop 1

3.1.1. Participant recruitment

As per Rowe and Wright (1999), we aimed to elicit opinion from a diverse range of stakeholders with appropriate knowledge. Our selection criteria required that they had expertise in the context of crime, and that they had knowledge either of metaverse technologies, or of crimes that are currently facilitated by the internet (e.g., online sex offending). Participants were identified through our SR, online searches, through professional networks, and snowballing. Initially, 59 participants were contacted, of which 27 participated (41% female), which is a similar rate of participation to that reported in other recent Delphi studies (e.g., Elgabry et al., 2022; Flood et al., 2023). Participants were from academia (N = 3), government agencies/departments (N = 7), industry (N = 5), law enforcement (N = 9), and the voluntary sector (N = 4). Academic attendees had expertise in the law, online offending, and the misuse of technology for crime in general. The government agency/department stakeholders represented were those that had expertise in, and the responsibility for, crime and/or online environments. Their professional responsibilities included futures and foresight, understanding how technology affects homeland security, reducing online offending, and the development of science and technology for policing contexts. Industry representatives included two large technology companies involved in the development of VR and/or metaverses, a company that specialises in the investigation of offences committed on the dark web or using crypto-assets, and one that provides services to keep families safe online. Law enforcement stakeholders were from INTERPOL, EUROPOL, two UK national policing organisations responsible for the policing of volume crime, or serious and organised crime in the UK, a UK regional organised crime unit involved in the policing of online crime, and a stakeholder from a European police force with expertise in the misuse of technology and online offending. Voluntary sector participants had expertise in technology and offending online, policing and crime, and the prevention of abuse, aggression and violence (on and offline). Collectively, participants had expertise in a broad range of crime types.

3.1.2. Procedure

The first expert elicitation exercise was a two-day event conducted in September 2022. An in-person event was preferred as, given the novelty of the metaverse, we wanted to provide participants with the opportunity to share knowledge about the technology and discuss their ideas about its use and misuse as well providing independent opinions. With this in mind, we employed a version of the nominal group technique. The Nominal Group Technique (NGT) is similar to the Delphi method commonly used in futures research (e.g., Elgabry et al., 2022; Flood et al., 2023). Both involve the independent generation of themes or ideas by participants, the synthesis of those themes, and one or more rounds in which participants indicate the extent to which they agree with them, or rate them along one or more dimensions. The key differences between the two approaches are that Delphi participants are not usually aware of who the other participants are, which creates anonymity, and consequently Delphi studies are usually conducted remotely (e.g., Landeta et al., 2011). There are clearly strengths and weaknesses to each approach (see Landeta et al., 2011; Rowe & Wright, 1999), but the NGT was considered more practical for the present study and maximised interactions that we sought to facilitate.

The programme for day 1 included presentations from the authors and attendees with expertise about the technologies that are or could be used in the metaverse (e.g., blockchain, haptics, and VR), current and future use cases (see Table 1) of the metaverse (to stimulate thinking regarding possible crime opportunities that they might facilitate) and policing crime online. In the penultimate session of day 1, the authors described the (N = 22) crime threats and the accompanying descriptions of them (i.e., what we refer to as scenarios in this paper) identified in our SR (which are discussed below). Participants were then invited to generate any existing or future crime threat scenarios that might be facilitated by the metaverse that had not been identified in the SR.

To do this, participants were seated at tables of 5–6 people, organised to ensure that there was a variety of expertise at each table. Each table also had a facilitator who took notes and clarified any ambiguities about the tasks. As per the NGT, participants were first given

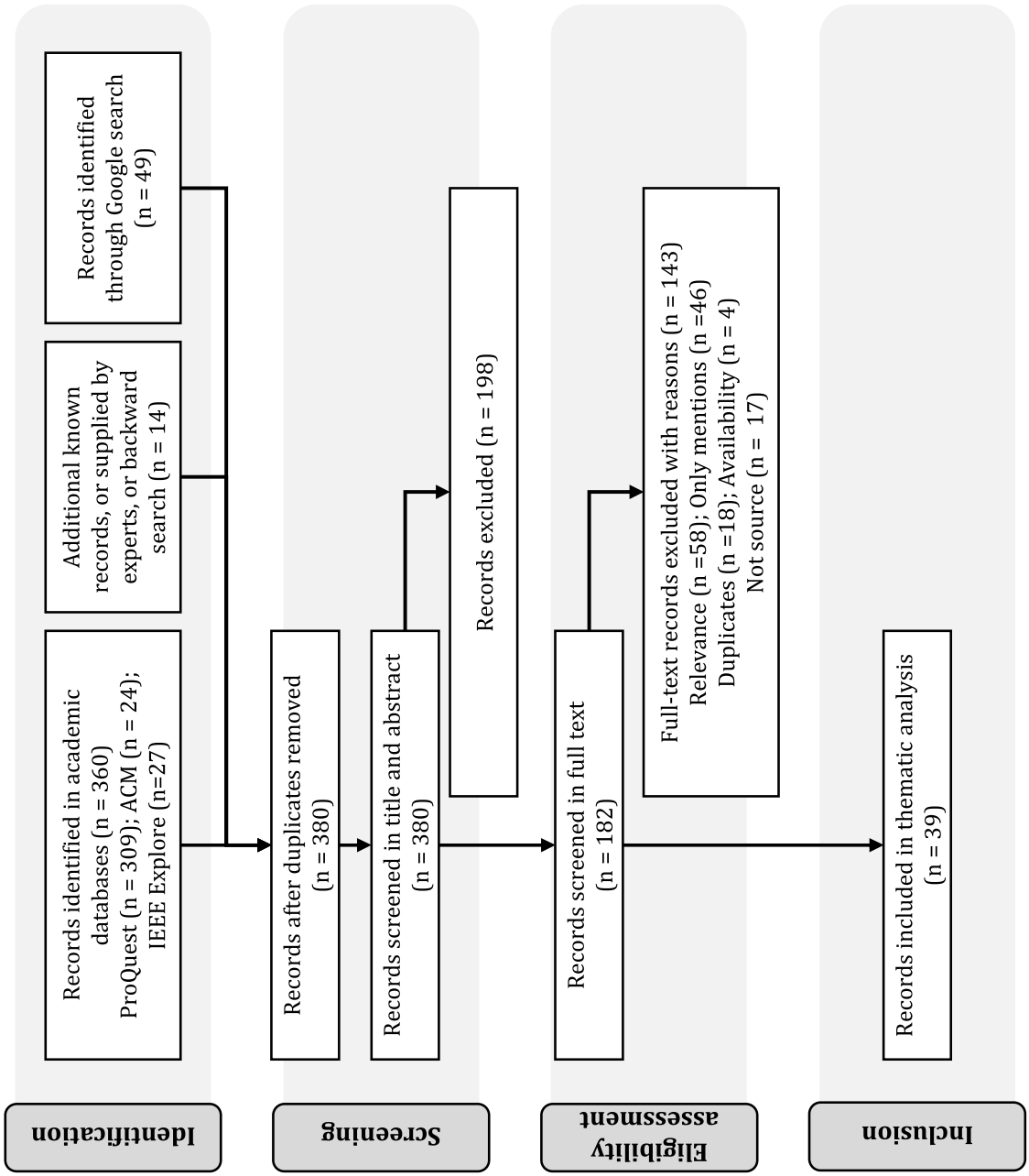

Fig. 1. PRISMA-ScR flow diagram for the scoping review (search conducted in August 2022).

Table 3
Characteristics of the data extracted from records.

Item label	Description
Author(s)	First author's last name and first name initials plus the abbreviation et al. as appropriate / Full name of publisher when no specific person was identified as author.
Publication date	Full date if available (DD/MM/YYY) or year of publication (YYYY).
Publication type	Peer reviewed, blogs, broadcasts, conference papers, documentaries, news/magazine articles, reports or preprints.
Data source	ProQuest, ACM, IEEE, Google, provided by expert, known record or backward search
Crime types	Crime types associated with the crime threat scenarios (see below)
Crime threat/future scenarios	Descriptions of how the crimes could be or were being committed in the metaverse.

10 min to generate crime threat scenarios individually and silently. In their small groups, they were then asked to list one crime threat at a time in a round-robin fashion (without interruption), until all the crime threat scenarios they had generated had been listed. Next, they were invited to discuss the possible crime threats listed, add new ones and to remove duplicates. They were given 50 min to do this. In the final session of the day, each table was asked to feedback to the whole group regarding the crime types and threat scenarios identified, and participants were invited to nominate any further crime threats that had occurred to them over the course of the discussion. At the end of Day 1, the crime threats nominated by participants were analysed (inductively) using a thematic analysis. Those that overlapped with the threats identified during the SR (see below) were merged, while unique threats were added to the list of threats.

Day 2 commenced with a recap of day 1 and a rating exercise for which participants were asked to consider all the threats identified and to rate them (using a 10-point scale – ranging from low to high) along four dimensions, namely: harm severity, frequency, achievability, and defeat-ability (see Table 4). The threats were presented one at a time and participants asked to rate them individually (and anonymously) using an online survey platform (Mentimeter). Participants were given 70 min for this exercise. We anticipated that participants would have varying degrees of expertise about the crime threats identified (or the specific technologies involved) and the ease with these might be committed. Consequently, for each rating, participants were also asked to indicate how confident they were about that response (e.g., Ogden et al., 2005) using a 10-point scale from 1(guessing)– 10(completely certain). Three participants (one each from industry, law enforcement, and government) could not participate on day 2 due to operational or work-related reasons. They were from well represented sectors in our sample and so their absence on day 2 did not negatively impact the composition of the group. Consequently, 24 participants took part in the rating exercise.

3.2. Workshop 2

3.2.1. Participant recruitment

The second workshop was conducted during the 2023 INTERPOL STRATalks Annual Expert Meeting, which was a two-day meeting organized by the INTERPOL Innovation Centre in November 2022. STRATalks offers a forum for strategic thinkers in the global law enforcement community including senior advisers, strategic planners, chief innovation officers, analysts, and foresight practitioners, to meet regularly, exchange findings from their environmental scanning and provoke new ideas. There were 31 participants (of which 38% were female), comprising 28 law enforcement officers from 16 countries, 2 members of the INTERPOL General Secretariat and 1 representative from EUROPOL. Of these, 42% represented European, 35% APAC, 16% MENA and African, and 6% American countries. As for workshop 1, collectively, participants had expertise across a wide range of offences.

3.2.2. Procedure

A similar programme was used to Workshop 2, but the presentations were abridged versions of those from the previous workshop. However, the same amount of time was allocated to the idea generation and rating exercises discussed above, and participants were presented with the set of crime threats identified in the scoping review and the first workshop. As before, the data were collected anonymously using Mentimeter.

Table 4
Dimensions for crime threat scenario ratings.

Dimension	Definition
Harm Severity	Victim and/or social harm. Physical or emotional harm associated with an offence, financial loss to an individual, or undermining trust in public institutions would all be considered harmful (1 = low harm, 10 =high harm).
Frequency	The likely number of times the scenario would occur in a given period of time (1 =low frequency, 10 =high frequency).
Achievability	How easy would it be to perform the offense, accounting for likely readiness of the necessary technology and its availability. For example, does it depend on very expensive hardware or access to hard to acquire data, or the use of sophisticated techniques? (1 =difficult to achieve, 10 = easy to achieve).
Defeat-ability	How easy would it be to develop/apply measures to prevent, detect or render the offence unprofitable. Consideration given to whether defeat measures are unobvious; simple or complex; and/ or needing behavioural change. For example, could the crime be circumvented unobtrusively by a company such as Google or does it require every computer user in the world to be equipped with a biometric scanner? (1 =difficult to defeat, 10 =easy to defeat).

4. Results

4.1. Crime threat scenarios

The SR and first expert consensus exercise[6] led to the identification of 30 crime threat scenarios, of which 22 (73%) were identified during the SR. For presentation and analytic purposes, we grouped these 30 scenarios into five higher-level categories: 1) fraud, forgery, or financial crimes, 2) property crimes, 3) sex crimes, 4) other crimes against the person, and 5) other crimes. For parsimony, Tables 5–9 provide abridged descriptions of the scenarios and their provenance. The descriptions used for the expert consensus exercises are direct extracts from the records identified in the SR[7] and can be found in Appendix 1.

As shown in Table 5, around one-third (N = 9) of the crime threats identified were financial crimes, all of which were identified in the SR. These included offenses that would require sophisticated Blockchain attacks to steal currency or digital assets from users, impersonation scams facilitated by the metaverse (e.g., Broker Imposter Scams would prey on those who wish to move digital assets from one metaverse space to another) and Tax evasion schemes for which offenders would exploit ambiguities in regulatory frameworks to avoid paying income taxes.

Three of the crime threat scenarios concerned property crime, of which one was identified during the workshops (see Table 6). These varied quite considerably, with the first concerning the misuse of data obtained via metaverse technologies to plan real-world burglaries, while another concerned the misuse of digital twins by offenders with the aim of planning attacks on physical infrastructure. While the first two threats exploit the cyber-physical hybridity of the metaverse, the final property crime identified concerned trespassing solely in the metaverse.

Given the visual and immersive nature of the metaverse – and the range of sexual offenses that currently occur on the internet (Neto et al., 2013) – it is perhaps unsurprising that a range of sexual offenses were identified as threats that could be facilitated by the metaverse. As noted in some of the crime threat scenarios, haptic suits, and related technologies (e.g., teledildonics[8]) could make these offenses rather immersive for offenders and even more traumatic for victims.

As shown in Table 8, eight of the identified crime threat scenarios concerned offenses against individuals, of which three were generated during workshop 1. These varied from those that had a direct physical component (cyber-physical attacks), to those that currently occur on the internet but the effects of which could be significantly amplified by the level of immersion associated with the metaverse (e.g., hate crime, incitement to self-harm), to those that enable activity that is impossible in the real-world (e.g., the use of invisibility in the context of stalking in the metaverse).

The final four crime threats (see Table 9) included conspiracy to commit crime (which is an offense in its own right), impersonating a law enforcement officer, and the denial of access to services that are likely to emerge in the metaverse, such as healthcare and education. While the conspiracy example overlaps with the Cyber-physical infrastructure attacks threat discussed in Table 6, the former potentially includes any type of offending, while the latter is a very specific consistency with very particular risks, and hence we kept these two examples separate.

4.2. Rating of crime threat scenarios by experts

For each of the dimensions rated, we computed a variety of descriptive statistics using the raw values. These included the mean, median and inter-quartile range (IQR). Following Beiderbeck et al. (2021), we consider an IQR of ≤ 2.5 to indicate consensus.

However, it was evident that participants varied in the confidence they expressed in their responses for each crime threat. Consequently, to give more weight to more confident responses, we also computed confidence weighted means scores for each crime threat and each rating dimension using Eq. 1. These confidence-weighted means for workshop 1 participants are shown in Table 10. This table also indicates where consensus existed for each crime threat and each rating dimension (i.e., where the IQR values for the unweighted values were less than or equal to 2.5).

$$Confidence \quad Weighted \quad Mean = \frac{\sum_{i=1}^{N} x_i \times c_i}{\sum_{i=1}^{N} c_i} \tag{1}$$

Where, N is the sample size, x_i is the rating for the dimension of interest for participant i, and c_i is the confidence expressed by participant i in that rating.

In addition, we computed a simple indicator of risk (Craig, 2018) for each crime threat scenario by taking the product of the confidence-weighted mean harm severity and frequency scores for that crime threat.

[6] An additional two scenarios were identified during the second workshop. However, they are not presented in the main text as they were only rated during the second workshop, and they did not feature in the top 10 threats. Details of these crime threat scenarios can be found in Appendix 1.

[7] Minor modifications were made to shorten or clarify some scenarios.

[8] For example, see https://www.wired.co.uk/article/teledildonics-hacking-sex-toys. Last accessed 01/04/2023.

Table 5
Crime threat scenarios for fraud, forgery and/or financial crimes.

Crime threat	Scenario	Source (s)
Blockchain attacks	Vulnerabilities in blockchain technology could be exploited to steal digital assets and/or currency from users.	(Annison, 2022; Huq et al., 2022)
Broker Imposter Scam	Malicious actors could pose as brokers of digital assets that move them between metaverse platforms (e.g., Decentraland and Roblox) with the purpose of stealing or defrauding owners.	(Huq et al., 2022)
Copyright infringement	Sound, software, pictorial and graphical material, among other copyrightable works specifically produced for the metaverse could be reused and slightly edited to be used in user spaces, infringing copyrights.	(Goossens et al., 2021; Zhao et al., 2022)
Counterfeiting	Malicious actors could create counterfeit digital goods (including NFTs) posing as licit products from brands (e.g., fake digital Gucci bags).	(Cheong, 2022; Goossens et al., 2021; Huq et al., 2022; Zhao et al., 2022)
Identity theft for financial gain	Malicious actors could use avatars to pose as fake financial actors (e.g., virtual bank teller) to access users' financial information for financial gain.	(Abdulsattar Jaber, 2022; Bell, 2022; Cunha Barbosa, 2022; Dey, 2022; Howell, 2022; Huq et al., 2022; Identity Management Institute, 2022; Khitrov, 2022; Li & Lalani, 2022; Pinnock, 2022; Rosenberg, 2022; Smaili & de Rancourt-Raymond, 2022; Williams, 2021)
Impersonation scam	Criminals can potentially impersonate service providers like doctors and give false medical advice to patients in return for payment.	(Bell, 2022; Cunha Barbosa, 2022; Huq et al., 2022; Pinnock, 2022)
Investment scam	Offenders could exploit the novelty and hype to invest in the metaverse, and the limited knowledge on security measures to commit a range of scams, including giveaway scams, fake metaverses, wearable minting scam, technical support scams, fake land expansions, rug pulls and pump and dump.	(Annison, 2022; Banaeian Far & Imani Rad, 2022; CITIC Telecom International, 2022; Combs, 2022; Dataquest, 2022; Huq et al., 2022; Kadar, 2022; Mackenzie, 2022; PCQuest, 2022; Shen, 2022; Smaili & de Rancourt-Raymond, 2022; Targeted News Service, 2022)
Money laundering	Malicious actors could use metaverse-based assets (e.g., crypto currency and assets, virtual land, wearables) to launder illicit funds.	(Annison, 2022; Banaeian Far & Imani Rad, 2022; Huq et al., 2022; Pinnock, 2022)
Tax evasion	A company that exists only in the metaverse may lack a logical jurisdiction and, for example, could effectively avoid paying income taxes.	(Huq et al., 2022)

Table 6
Crime threat scenarios for property crimes.

Crime threat	Scenario	Source (s)
Cyber-physical burglary	VR, AR and other intelligent sensing material could be exploited by malicious users to gain information (e.g., location, access, valuables) about properties and attempt a burglary in the physical locations.	(Huq et al., 2022; Nichols, 2022; Wang et al., 2022)
Cyber-physical infrastructure attacks	Digital twins and connection of infrastructure to the metaverse via IoT and other technologies could be exploited by malicious actors to plan and perpetrate attacks to infrastructure.	(Huq et al., 2022)
Trespassing in the metaverse	Offenders could trespass in the metaverse into virtual properties or virtual events with access control.	Expert consensus

$$Risk = \frac{\sum_{i}^{N} h_i}{N} * \frac{\sum_{i}^{N} f_i}{N} \quad (2)$$

Where, N is the sample size, h_i is the harm severity rating for participant i, and f_i is the frequency rating for participant i.

Table 10 is rank ordered by this estimate of risk for group 1 and colour coded to highlight differences across the crime threats. Each crime threat scenario was also allocated to one of the five general crime categories. We repeated the above analyses for those who participated in the second workshop (group 2). However, rather than show the full set of results (which can be found in Appendix 2), for parsimony and to allow comparisons, in Table 10 we show the overall risk rating for that sample and the consensus indicators.

Considering the general categories of crime first, we see that the sexual offenses tended to be rated as being a high risk. In all cases, the mean (confidence-weighted) harm rating was high, and in most cases so too was the weighted-mean rating for the expected (future) frequency of offending. Apropos the IQR values, we see that consensus was reached for the harm dimension in most cases for both groups. For non-consensual sexual image offenses, for group 1 the IQR value of 3 just exceeded our threshold criteria. With respect to the ease with which these types of offenses could be achieved, participant's mean ratings indicated that they believed such crimes would be relatively easy to commit, although a consensus view was not reached for both groups for all offenses. For example, for child grooming, only group 2 formally reached consensus about the achievability of this crime threat. For group 1, the IQR of 3.25 exceeded

Table 7
Crime threat scenarios for sex crimes.

Crime threat	Scenario	Source (s)
Child grooming	In a virtual setting, children's avatars could be approached by other avatars operated by adults to engage them in sexual activities.	(Crawford & Smith, 2022; Li & Lalani, 2022; Reed & Joseff, 2022; Rice, 2022; Russia Business News, 2022; Sum of Us, 2022)
Doxing	Malicious actors could exploit the rich information that will be collected from users (e.g., bio data and eye tracking) to extort or shame users.	(Buck & McDonnell, 2022; Vladimirov et al., 2022)
Non-consensual sexual image offenses	Malicious actors could exploit personal, sensitive, and explicit material shared among users for virtual reality non-consensual sex acts. This could also involve the use of deepfakes.	(Annison, 2022; Li & Lalani, 2022)
Sexual assault	In a virtual setting, a user could be approached indecently and forcefully by other avatars operated by malicious actors with the purpose of sexual assault.	(Allen & McIntosh, 2022; Cheong, 2022; Clayton, 2022; Huq et al., 2022; Li & Lalani, 2022; Reed & Joseff, 2022; Rice, 2022; Shanker & Zytko, 2022)
Child sexual abuse material	Pay-for immersive streaming of child sexual abuse material could involve offenders and victims in distanced locations. The harms could be made worse with the use of haptic suits and other immersive equipment.	Expert consensus
Virtual trafficking of people for sexual exploitation	Avatars of vulnerable users could be sexually exploited in the virtual setting repeatedly without the need to cross borders or disappearing.	Expert consensus

Table 8
Crime threat scenarios for other crimes against the person.

Crime threat	Scenario	Source
Cyber-physical person attacks	VR, AR, haptic suits and other wearables could be misused by malicious actors to cause harms to users (e.g., by tampering with the physical activity boundaries set in the apparatus).	(Huq et al., 2022; Nichols, 2022; PCQuest, 2022; Wang et al., 2022)
Harassment	In a virtual setting, a user could be approached by other avatars to harass them; they could even be chased across different metaverse platforms.	(Allen & McIntosh, 2022; Buck & McDonnell, 2022; Cheong, 2022; Combs, 2022; Di Pietro & Cresci, 2021; Howell, 2022; Identity Management Institute, 2022; Reed & Joseff, 2022; Shanker & Zytko, 2022; Sum of Us, 2022; Zhao et al., 2022)
Hate crime	In a virtual setting, a user could be approached by other avatars with the purpose of committing hate crime.	(Allen & McIntosh, 2022; Li & Lalani, 2022; Rice, 2022; Sum of Us, 2022; Zhao et al., 2022)
Stalking	A malicious actor could stalk a user across different metaverse platforms without the need to be present at the same physical location; they could even use invisible avatars to avoid detection.	(Di Pietro & Cresci, 2021; Huq et al., 2022; Wang et al., 2022; Zhao et al., 2022)
Radicalisation	AI designed to be empathetic avatars and multiuser spaces could be used to radicalise vulnerable users (e.g., underaged individuals).	(Abdulsattar Jaber, 2022; Buck & McDonnell, 2022; Howell, 2022; Reed & Joseff, 2022)
Incitement to self-harm	Several users could come together in a virtual setting and incite a vulnerable user to self-harm. AI designed avatars could be made to be more empathetic, and to even incite massive self-harm.	Expert consensus
Preying on addicted users for extortion, coercion or incitement purposes	Vulnerable individuals could be preyed on by loan sharks and criminal organisations to exploit them financially or incite them to commit crimes.	Expert consensus
Child labour and modern slavery to develop metaverse content	The demand for digital goods, assets and services will create an opportunity to undercut competitors by using child labour and modern slavery.	Expert consensus

Table 9
Crime threat scenarios for other crimes.

Crime threat	Scenario	Source (s)
Impersonating a LEA	Criminals can pretend to be law enforcement authorities in the metaverse for a variety of purposes, including gaining intelligence.	(Bell, 2022; Cunha Barbosa, 2022; Huq et al., 2022; Pinnock, 2022)
Conspiring	Malicious actors could use virtual spaces resembling the physical world in detail, like digital twins, to plan and train to commit crime in the physical world.	(Allen & McIntosh, 2022; Huq et al., 2022; Wang et al., 2022)
Unauthorised adversary (mis)use of training materials	Malicious actors could exploit virtual scenarios designed for training and preparing for high impact events (e.g., organised crime) to understand how to bypass law enforcement measures.	Expert consensus
Denial of essential services	Malicious actors could deny access to a multitude of users to essential services being provided in the metaverse such as healthcare and education.	Expert consensus

Table 10
Confidence-weighted means for the threats identified, indicators of consensus, and risk ratings (Consensus ratings are shaded where the IQR for the raw values were ≤ 2.5).

	Harm Grp 1	Consensus Grp 1	Consensus Grp 2	Frequency Grp 1	Consensus Grp 1	Consensus Grp 2	Achievability Grp 1	Consensus Grp 1	Consensus Grp 2	Defeatability Grp 1	Consensus Grp 1	Consensus Grp 2	Risk (HxF) Grp 1	Risk (HxF) Grp 2
Child sexual abuse material (S)	9.80			7.02			7.95			4.04			68.77	63.07
Child grooming (S)	9.67			7.09			8.19			6.49			68.52	63.17
Investment scam (F)	8.26			8.20			8.78			4.11			67.75	53.87
Hate crime (P)	7.81			8.58			9.47			3.14			67.00	64.75
Harassment (P)	7.95			8.02			8.33			4.25			63.70	64.78
Sexual assault (S)	8.62			7.23			8.15			5.11			62.38	55.51
Non-consensual image offences (S)	8.80			6.43			7.44			3.48			56.59	57.42
Doxing (S)	7.61			7.16			7.85			3.83			54.49	60.56
Stalking (P)	7.80			6.10			8.04			4.84			47.55	51.61
Radicalisation (P)	7.83			5.99			7.92			4.14			46.94	62.01
Money laundering (F)	6.97			6.58			7.30			5.06			45.87	59.79
Impersonation scam (F)	7.54			5.90			6.53			5.79			44.47	42.84
Broker imposter scam (F)	5.42			8.07			6.83			5.25			43.74	41.86
Identity theft for financial gain (F)	6.55			6.48			6.63			6.58			42.46	53.46
Virtual trafficking for sexual exploitation (S)	8.27			4.64			5.55			4.63			38.40	40.93
Preying on addicted users for extortion, coercion or incitement purposes (P)	7.05			5.33			6.64			4.19			37.62	47.74
Incitement to self-harm (P)	8.50			4.26			7.22			5.17			36.19	41.52
Denial of essential services (O)	7.89			4.49			4.91			6.04			35.42	33.53
Child labour and modern slavery to develop metaverse content (P)	7.22			4.71			6.25			5.36			34.01	33.96
Blockchain attacks (F)	5.76			5.64			6.75			4.90			32.50	35.57
Cyber-physical person attacks (P)	7.46			4.33			4.69			6.65			32.31	29.58
Impersonating a law enforcement officer (O)	7.27			4.41			4.85			6.16			32.06	45.86
Tax evasion (F)	5.39			5.85			7.36			6.29			31.54	35.02
Cyber-physical infrastructure attacks (Pr)	8.42			3.41			5.78			5.50			28.73	35.65
Conspiracy (O)	6.40			4.44			6.63			3.85			28.40	49.94
Trespassing in the metaverse (Pr)	4.76			5.96			5.44			6.28			28.35	24.50
Counterfeiting (F)	3.65			6.80			7.02			4.22			24.78	46.06
Unauthorised adversary (mis)use of training materials (O)	7.16			3.42			5.49			6.02			24.50	33.11
Copyright infringement (F)	3.52			6.80			7.53			4.84			23.95	41.68
Cyber-physical burglary (Pr)	7.15			2.92			4.23			5.31			20.85	41.48

Top Ten Crime Risks

NOTE: S=Sexual offenses, F=Financial crimes, P = crimes against people, Pr=Crimes against property, O=Other

our threshold for consensus. However, it is worth noting that an inspection of participant's ratings indicated that the reason for this was that two participants (who were clear outliers for this question) rated this offence as unachievable (a rating of 1) and one of them[9] reported that they had no confidence in their response for this particular offence (a rating of 1). Excluding this participant (they are not excluded from Table 10), the IQR of 2.5 would indicate a consensus view regarding achievability. In terms of defeat-ability, these offenses were generally perceived to be some of the most difficult to address, although child grooming and sexual assault were seen as relatively easy to deal with by group 1 (group 2 did not agree about child grooming).

In contrast, the property and "other" crimes tended to be rated as being of a (relatively) low future risk, and with only three exceptions, there was no consensus about these offenses for any of the dimensions. In the case of the latter, for both groups, consensus was reached that cyber-physical burglary would be a high harm offense, while group 2 (but not group 1) felt that cyber-physical infrastructure attacks would be a high harm crime. These offenses were not anticipated to be high frequency offenses, easy to achieve or particularly difficult to defeat.

Financial and personal crimes were more varied in terms of anticipated future risk and the extent to which participants reached a consensus across the four dimensions rated. For example, group 1 participants reached a consensus view that investment scams would be (future) high-frequency crimes that would also be easy to achieve, while group 2 agreed that these would be high-harm crimes but did not reach consensus that they would be high frequency or easy to achieve. In contrast, copyright infringement in the metaverse(s) was perceived to likely be a low harm (future) crime threat. Participants views as to how easy these types of offences would be to defeat varied across offence types, with investment scams and counterfeiting being perceived to be the hardest to defeat.

Overall, the results for the two groups were very similar not identical. For example, for the risk variable, the Pearson's correlation coefficient between the confidence-weighted mean values for the two groups was 0.80 ($p < 0.0001$). In terms of differences, perhaps the most notable was money laundering for which only the law enforcement group (group 2) reached a consensus that this would be a future high harm crime that would be highly achievable. Workshop 1 participants did not hold an entirely opposing view about money laundering but were in less agreement about the harm or ease with which this form of offending might happen in the metaverse in the future.

Fig. 2 provides a complimentary visualisation of the data for group 1, by plotting risk against defeatability for each crime threat. Large symbols indicate those crime threats for which group 1 reached a consensus about how defeatable they were (six of the crime threats). Alternative visualisations would include risk plotted against achievability, or defeatability plotted against harm, but Fig. 2 provides a useful mapping of (say) which crime threats participants thought would be the most the difficult to address and would also present the most risk. These threats, of which there were six, appear in the bottom right quadrant of the graph and are perhaps those that require the most attention now. Those in the top left quadrant (12 of the 30) are the crime threats perceived to be the easiest to address and that also present the least risk. As noted above, for child grooming, group 1 did not rate this as particularly difficult to defeat but also did not reach consensus on this issue. Group 2 rated this crime threat as harder to defeat (rating it 4.4) but also failed to reach consensus.

5. Discussion

As discussed in the introduction, there is enormous investment in the development of the metaverse(s) and there are many positive use cases of it. However, as with all new products and services, it has the potential to create new crime opportunities unless adequate attention is given to identifying and preventing them. The existing literature suggests that the metaverse will be more than just an extension of the Internet (e.g., Cheng-Han & Kiat-Boon, 2023). It will be an immersive, 3D environment where individuals are embodied by avatars, content is user-generated and a wealth of new digital property (e.g., NFTs) is traded. These characteristics may facilitate and magnify the harms of many crimes in an environment where regulation is immature. For example, while immersive technologies (e.g., VR headsets and haptic suits) will make experiences more vivid they have the potential to make offences (e.g. harassment, sexual offences, or hate crime) more traumatic. Digital land and other assets will create investment, entertainment and other opportunities but will also increase the scale and variety of investment scams that will be possible.

With this in mind, in this study we used a variation of the nominal group technique to identify future threats and to prioritise them. A systematic scoping review of the existing literature identified a total of 22 crime threat scenarios, to which the experts we consulted added a further eight. While the two groups differed a little in how they rated the crime threats, the overall picture was quite consistent between them. For example, overall, crimes of a sexual nature, such as the use of Child Sexual Abuse Material and non-consensual image offences in the metaverse, were rated as the most harmful, most likely to happen frequently, most achievable, and most difficult to address future threats, whereas property crimes tended to be rated lower for each of these dimensions. This consistency should provide stakeholders with confidence about which offenses they might prioritise in addressing the threats identified here. Fig. 2 provides further insight.

Considering the top ten risks identified in a little more detail, five were sexual in nature. The types of sexual offenses identified are all contemporary problems, some of which – such as child sexual abuse material (e.g., INHOPE, 2021), child grooming (e.g., WeProtect Global Alliance, 2021), non-consensual sexual image offenses (e.g., Harper et al., 2021) – already take place online, whereas rape and sexual assaults, at least as defined in law (e.g., "Sexual Offences Act, 2003), currently only take place in real life. In all cases, attributes of the metaverse(s) have the potential to make these types of offenses worse than their online equivalents. For example, the use of

[9] This participant's confidence varied across responses (i.e., it was not consistently low).

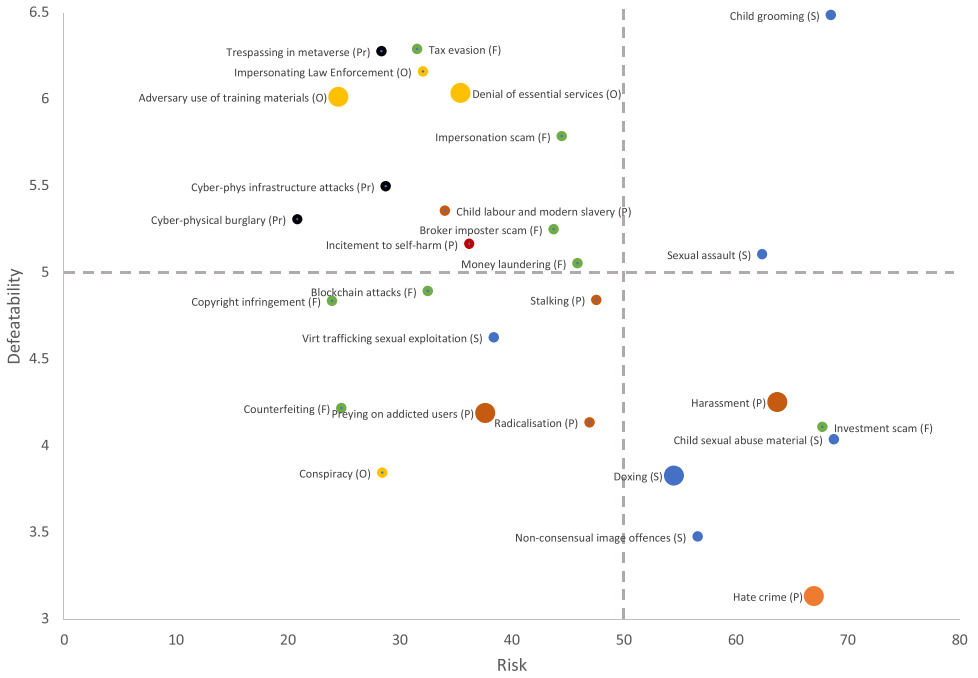

Fig. 2. Risk by defeatability for each crime threat (colour coded by the five general crime categories, see Table 10). *NOTE: Quadrants are defined by the midpoints of each scale; large symbols indicate crime threats for which group 1 reached consensus for the defeatability dimension.

Avatars may create anonymity, which would reduce the risk of offenders being detected. Moreover, the open/user-generated ethos of the metaverse(s) means that users will have the freedom to design avatars or other content in ways that appeal to and mislead victims, which may make these sorts of offenses easier to commit. Decentralisation (i.e., the absence of central controllers) too may make it easier for offenders to escape detection or perceive that they will do so. Relative to similar crimes committed in 2D environments, the level of immersion facilitated by metaverse technologies (e.g., virtual reality, haptic suits and teledildonics) will also likely increase the rewards to offenders, and the harm experienced by victims. In thinking about how to address these offences, there will likely be a tension between privacy and security (Livingstone et al., 2019), since people typically express a desire for privacy but security can require access to personal details (e.g. to verify who someone is). Attention will need to be given to balancing the two to make the metaverse(s) a safe place.

Four of the (top ten) offenses considered were other types of crimes against the person. These already take place in the real world or online, but again, the immersion associated with the metaverse will mean that their effects are amplified for victims. The hyper-spatiality of the metaverse may make offenses such as stalking easier to commit and the use of avatars may help to conceal an offender's activity. Virtual-physical hybridity may also mean that the effects of these offenses (e.g., hate crime, harassment, and stalking) are not constrained to impacting victims in virtual worlds but may also affect them in real world contexts.

While many of the above crimes are expressive ones, the motivation for other forms of offending is clearly financial, and hence it is unsurprising that financial crimes were included in the top ten (they were also the next 4 highest rated offenses). Investment scams are currently rife on the internet, with recent incarnations including cryptocurrency frauds (e.g., Trozze et al., 2022; Vasek & Moore, 2015), such as initial coin offerings (i.e. investment opportunities) for fake currencies. Such scams will be possible in the metaverse, but as there will be other forms of ownership (e.g., virtual goods, virtual land) in the metaverse – which will be recorded on (possibly unregulated) blockchains which lack a central controller to monitor activity – the opportunities for financial crime (including money laundering) will increase substantially and, as the metaverse(s) is expected to be a multi-user environment, this may facilitate offending at a larger scale than we see today.

In terms of the likely scale of the crime harvests that might emerge, participants rated how frequent they anticipated each threat might be. However, what these actual frequencies are likely to be will depend on how ubiquitous the use of the metaverse(s) is, who uses it, and for what purposes. Because of its emerging nature, there is currently uncertainty about this. In their report, Deloitte (2022) outline three scenarios regarding its trajectory which are useful for thinking about this: low orbit, double star, and big bang. In the low orbit scenario, the Metaverse becomes a 'specialty market' that complements existing platforms/technologies – and caters to a particular audience - but does not replace them and is not fully integrated to daily life. In the double star scenario, the metaverse becomes a 'mainstream market' with many applications but one that lacks interoperability which leads to a few major players dominating the metaverse. Lastly, the 'big bang' scenario considers a complete overhaul of how we experience the internet today, with this becoming an immersive world where most businesses and consumers are involved. All three scenarios could facilitate crime harvests, but the scale of the problems generated will depend on which scenario plays out. The big bang scenario would create the greatest crime opportunity and, because there would be the most actors involved, it would also be the most complicated to design

security for, and to monitor place manager's compliance with any guidelines, standards or regulation that are proposed. The situation is, of course, made more complex by the fact that the metaverse(s) is a convergence of technologies, each of which will have their own vulnerabilities and (in some cases) their own standards and regulations (some may have none).

5.1. Regulation and place management

Safeguarding the metaverse(s) will likely require regulation across different fronts including: data protection and privacy, property rights (Cheong, 2022; Goossens et al., 2021), taxation, employment, criminal activity, and financial incentives (Faraboschi et al., 2022; Lau, 2022). Given the possibility for people to create multiple identities in the metaverse, new regulations might need to be created regarding 'honest self-representation' (Morini Bianzino, 2022). Such regulation would need to balance privacy and security, as discussed above. Any grey areas that arise when organisations and individuals operate in a virtual environment will require regulations (Dalton, 2022) to mediate disputes and define taxes (Ernst & Young Global Ltd, 2022). An international law may be required to deal with the lack of jurisdiction of the metaverse (Cheong, 2022). For example, the fact that DAOs operate in the virtual world will require a definition of how they will be treated for legal and tax purposes (Ernst & Young Global Ltd, 2022). Similarly, consideration will need to be given to the fact that individuals will be interacting via avatars in virtual worlds and what the implications of this are (say) if altercations (such as the assault case discussed above) and breaches of the law (including criminal law) occur (Cheong, 2022; Lau, 2022). Special attention will need to be given to computer generated imagery, particularly in the context of (child) sexual abuse material. Generative adversarial networks (Creswell et al., 2018), such as StyleGAN2, can currently generate two dimensional images at scale of people, animals and objects that do not actually exist, and it seems likely that it will be possible to create three-dimensional images soon. In Coutorie's (1995) Delphi study, experts foresaw the problem of computer generated sexual abuse material almost three decades ago but action will need to be taken now to address this problem before it is upon us. Other needs for regulation include contractual issues, consumer and worker protections and the misuses of AI (Woods, 2022).

More generally, there will be a need to identify the roles and responsibilities of stakeholders and individuals. This will include determining who the place mangers will or should be in the metaverse(s), and consideration should be given as to whether existing models of guardianship (to include the part that individuals play) and place management will be sufficient in this new frontier. In their article, Sampson et al. (2010) discuss the role of "super controllers" in crime prevention, defining them as those who can incentivise place managers and guardians (and those who routinely interact with offenders) to act in ways to prevent crime effectively in the places for which they have responsibility. Super controllers include formal actors such as regulators and financial organisations who can (for example) ensure that place managers comply with laws and regulation, or have procedures (e.g., know your customer policies, escrow services) in place to secure payments, respectively. Such actors will need to address the types of issues discussed in the previous paragraph and may need to develop new technical competencies to detect and address the types of crime threats discussed. For example, while techniques have been developed to detect instances of child sexual abuse material (CSAM) on the internet, such as the hashing of known images of CSAM,[10] in the metaverse(s) this will likely be more challenging to do as (for example) "content" goes beyond static images, and can include 3D video, gestures, and physical contact through haptics.

Sampson et al. (2010) also discuss diffuse super controllers which can include markets. This may be particularly important in the metaverse(s) as many providers will seek to monetise their activity. As examples of how markets can affect the actions of place managers, Sampson et al. (2010) discuss certification schemes, which can be used to provide a market advantage to those who achieve – or score highly on – them. Such schemes already exist on the internet today in various forms. For example, *Trustpilot* operates worldwide and enables anyone to post reviews of companies, enabling consumers to see what others think of them. Similarly, online shopping marketplaces often use rating systems to enable consumers to establish whether a particular company is trustworthy or if the products they sell are worth purchasing. Such trust schemes are also used on darknet marketplaces (e.g., Van Hout & Bingham, 2014) illustrating their utility to a diverse range of "consumers". Thought should be given to how to implement such schemes in the Metaverse(s), and who should operate them, but such approaches may provide a less formal mechanism to encouraging responsible place management in the metaverse(s).

Just like the internet today, to keep the metaverse(s) safe will likely require a combination of approaches to include those discussed above, as well as the actions of individuals. The latter will include individuals engaging in acceptable behaviours (perhaps articulated in codes of conduct produced by DAO's or metaverse providers), acting as capable guardians, and reporting consistency to the relevant authorities. Who the latter should be (law enforcement, metaverse providers, regulators) will also require consideration.

5.2. Limitations and future research

As with all research, this study is not without limitations. Chief among these is the composition of the expert groups. Different groups may anticipate different threats, may be more adept at forecasting future trends and may perceive identified risks differently (e.g., Dalal et al., 2011; Tichy, 2004). Here, we elicited opinion from two groups with different expertise, which mitigates this issue to some extent, particularly because the outcomes were largely consistent between the two groups. The crime threats identified were also drawn from the existing literature, which extends the range of expertise drawn upon for this part of the exercise at least. However, the point remains. A second limitation is that we only had one round of the rating exercise. It is possible that a second round would have

[10] For example, see: https://www.iwf.org.uk/our-technology/. Last accessed 16 November 2023.

produced consensus for more of the threats identified, but (unlike some Delphi studies) our goal was not to continue with rounds of the exercise until consensus was achieved.

With respect to the rating exercise, we asked participants to indicate the confidence they had in their judgements and used these ratings to construct confidence-weighted estimates for the four dimensions explored (harm, frequency, achievability, and defeatability). We see value in so doing for a study such as this because participants vary in their expertise for particular threats and for particular technologies and capturing their confidence recognises this fact. However, we acknowledge that previous research (e.g., Rowe et al., 2005) has questioned the association between participant confidence and accuracy in Delphi studies. That said, it is important to note that in their study, Rowe et al. examined participant's mean confidence and accuracy (which we did not), as opposed to examining how confidence and accuracy vary across individual responses per participant (which is what we considered). Moreover, in the current study, to ensure that the use of the confidence ratings did not distort our findings (they did not), we also computed ratings without weighting them by confidence, and the IQR values reported in Table 10 were calculated in this way.

5.3. Conclusion

There is much hype around the metaverse and much investment in it. This study sought to identify the crime threats that it might facilitate in the future and which of these experts perceive to be the most harmful, frequent, easy to commit and most difficult to defeat. Our findings suggest a diverse array of threats, but also clear variation in the anticipated risks and the ease with which they might be prevented. We have discussed the roles and responsibilities of those who might address the identified threats, but more work will be required to understand the ways in which they might do so and to catalyse action.

Funding

This research was funded by the Dawes Trust and Anglia Ruskin University.

CRediT authorship contribution statement

Johnson Shane D.: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Supervision, Visualization, Writing – original draft, Writing – review & editing. **Borrion Herve:** Conceptualization, Investigation, Methodology. **Lundrigan Samantha:** Conceptualization, Funding acquisition, Methodology, Project administration. **Gómez-Quintero Juliana:** Conceptualization, Formal analysis, Methodology, Writing – original draft, Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors would like to thank the INTERPOL Innovation Centre, and in particular Arthur Langellier and Anita Hazenberg for their input to the research including the organisation of the second workshop.

Appendix 1. Included records in Scoping Review

Table A.1
Included records in Scoping Review.

No.	Title	Author (s) and publication year	Publication Type	Data source
1	Security Risks of the Metaverse World	Abdulsattar Jaber (2022)	Peer reviewed journal	Google
2	Safeguarding the metaverse: A guide to existing and future harms in virtual reality (VR) and the metaverse to support UK immersive technology policymaking	Allen and McIntosh (2022)	Report	Backward search
3	Elliptic Metaverse Report 2022 - The Future of Financial Crime in the Metaverse: Fighting Crypto-crime in Web3.0	Annison (2022)	Report	Supplied by expert
4	Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges	Banaeian Far and Imani Rad (2022)	Peer reviewed journal	Academic database
5	The metaverse is coming. Here are the cornerstones for securing it.	Bell (2022)	Blog	Backward search
6	Security and Privacy in the Metaverse: The Threat of the Digital Human	Buck and McDonnell (2022)	Conference paper	Known record

(*continued on next page*)

Table A.1 (*continued*)

No.	Title	Author (s) and publication year	Publication Type	Data source
7	Avatars in the metaverse: potential legal issues and remedies	Cheong (2022)	Peer reviewed journal	Known record
8	Mother, 43, has her avatar groped by three male characters in the online Metaverse	Clayton (2022)	News/magazine article	Backward search
9	Metaverse security: How to learn from Internet 2.0 mistakes and build safe virtual worlds	Combs (2022)	Blog	Google search
10	CITIC Telecom International: (Metaverse Business Opportunities) Changing consumption patterns with Immersive experience; Deconstructing blind spots of blockchain security applications	CITIC Telecom International (2022)	News/magazine article	Academic database
11	Metaverse app allows kids into virtual strip clubs	Crawford and Smith (2022)	News/magazine article	Backward search
12	What security risks could be hidden in the Metaverse? (¿Qué riesgos de seguridad puede esconder el Metaverso?)	Cunha Barbosa (2022)	Blog	Backward search
13	What are the security risks and privacy challenges in Metaverse	Dataquest (2022)	Blog	Academic database
14	Data Privacy in Metaverse is an Evolving Concern	Dey (2022)	Blog	Google search
15	Metaverse: Security and Privacy Issues	Di Pietro and Cresci (2021)	Conference paper	Academic database
16	Protecting Intellectual Property in the Metaverse	Goossens et al. (2021)	Peer reviewed journal	Academic database
17	3 Metaverse Security Issues That You Must Know	Howell (2022)	Blog	Google search
18	Metaverse or metaworse? Cybersecurity Threats Against the Internet of Experiences	Huq et al. (2022)	Report	Supplied by expert
19	Top 10 metaverse risks	Identity Management Institute (2022)	Blog	Google search
20	The Metaverse Fraud Question: What Are the Risks?	Kadar (2022)	Blog	Google search
21	What will it take to stop fraud in the metaverse?	Khitrov (2022)	Blog	Google search
22	How to address digital safety in the metaverse	Li and Lalani (2022)	Blog	Google search
23	Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial	Mackenzie (2022)	Peer reviewed journal	Backward search
24	Metaverse rollout brings new security risks, challenges	Nichols (2022)	Blog	Google search
25	Security risks that lurk deep inside the Metaverse	PCQuest (2022)	News/magazine article	Academic database
26	The metaverse will not be immune to cyber threats	Pinnock (2022)	Blog	Backward search
27	Kids and the Metaverse: What Parents, Policymakers, and Companies Need to Know	Reed and Joseff (2022)	Report	Backward search
28	Inside the Metaverse Are You Safe? Dispatches	Rice (2022)	Documentary	Backward search
29	Evil twins and digital elves: How the metaverse will create new forms of fraud and deception	Rosenberg (2022)	Blog	Google search
30	"Technologies for protecting children on the Internet": Rostelecom identified 10 cyber risks of future	Russia Business News (2022)	News/magazine article	Academic database
31	The.Tinderverse?: Opportunities and Challenges for User Safety in Extended Reality (XR) Dating Apps	Shanker and Zytko (2022)	Preprint	Academic database
32	NFTs and metaverse top tech risks, officials say: Government watchdog warns criminals could steal sensitive user data or access accounts to hijack money as value of cryptocurrency keeps rising	Shen (2022)	News/magazine article	Academic database
33	Metaverse: welcome to the new fraud marketplace	Smaili and de Rancourt-Raymond (2022)	Peer reviewed journal	Google search
34	Metaverse: another cesspool of toxic content	Sum of Us (2022)	Report	Backward search
35	Ala. Securities Commission: Five States File Enforcement Actions to Stop Russian Scammers Perpetrating Metaverse Investment Fraud	Targeted News Service (2022)	News/magazine article	Academic database
36	Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse: A Survey	Vladimirov et al. (2022)	Conference paper	Academic database
37	A Survey on Metaverse: Fundamentals, Security, and Privacy	Wang et al. (2022)	Preprint	Academic database
38	Facebook's Metaverse a dangerous breeding ground for crime and mental health issues, experts say	Williams (2021)	Broadcast	Academic database
39	Metaverse: Security and Privacy Concerns	Zhao et al. (2022)	Preprint	Academic database

Appendix 2. Additional crime threat scenarios identified in workshop 2

In the second workshop an additional two crime threat scenarios were suggested and assessed during the rating exercise. These are shown in Table A.2.

Table A.2
Additional crime threat scenarios generated in workshop 2.

Crime threat	Scenario	Source (s)
AI Generated Child sexual abuse material	Paid-for immersive streaming of **computer-generated** child sexual abuse material could be offered in the Metaverse. Teledildonics and equipment such as haptic suits could be used to make the experience more real. Eventually, encrypted multiusers spaces could be created so that many users can experience it together.	Workshop 2
Virtual Theft	If the Metaverse becomes like Second Life, where virtual items such as clothes and other items can be purchased, these may be stolen in the virtual or physical world (e.g. by force).	Workshop 2

The mean rankings for these crime threats are shown in Table A.3. In terms of consensus, this was achieved for achievability for virtual theft (IQR=2) but not for any of the other indicators.

Table A.3
Confidence-weighted means for the threats identified, indicators of consensus, and risk ratings.

	Harm	Frequency	Achievability	Defeatability	Risk
Harassment (P)	7.85	8.25	8.64	4.04	64.78
Hate crime (P)	7.77	8.34	9.05	3.41	64.75
Child grooming (S)	8.80	7.18	8.66	4.40	63.17
Child Sexual Abuse Material (S)	9.24	6.82	7.43	4.73	63.07
Radicalisation (P)	8.85	7.00	7.65	4.01	62.01
Doxing (S)	7.96	7.61	7.69	4.09	60.56
Money laundering (F)	7.86	7.61	7.71	4.78	59.79
Non-consensual image offences (S)	7.94	7.23	8.34	4.78	57.42
Sexual assault (S)	8.04	6.90	7.56	4.66	55.51
Investment scam (F)	7.54	7.15	7.47	4.71	53.87
Identity theft for financial gain (F)	7.75	6.90	6.41	5.83	53.46
Stalking (P)	7.25	7.12	7.25	4.54	51.61
Conspiracy (O)	7.87	6.35	8.07	5.45	49.94
Preying on addicted users for extortion, coercion or incitement purposes (P)	7.51	6.36	7.11	4.44	47.74
AI-Generated Child Sexual Abuse Material (S)	7.14	6.67	7.80	5.53	47.68
Counterfeiting (F)	6.35	7.25	7.13	5.66	46.06
Impersonating a Law Enforcement Officer (O)	7.94	5.78	6.25	5.93	45.86
Impersonation scam (F)	7.37	5.82	6.34	5.55	42.84
Broker imposter scam (F)	6.42	6.52	7.44	5.34	41.86
Copyright infringement (F)	5.40	7.72	8.23	5.87	41.68
Incitement to self-harm (P)	8.50	4.89	7.32	5.06	41.52
Cyber-physical burglary (Pr)	7.54	5.50	5.32	6.52	41.48
Virtual trafficking for sexual exploitation (S)	7.10	5.76	6.14	5.32	40.93
Virtual theft (Pr)	5.33	7.54	7.15	5.48	40.21
Cyber-physical infrastructure attacks (Pr)	7.99	4.46	4.81	5.24	35.65
Blockchain attacks (F)	6.69	5.32	5.46	5.99	35.57
Tax evasion (F)	5.82	6.02	6.73	5.53	35.02
Child labour and modern slavery to develop metaverse content (P)	7.95	4.27	5.19	5.67	33.96
Denial of Essential Services (O)	7.40	4.53	5.45	6.47	33.53
Unauthorised adversary (mis)use of training materials (O)	7.00	4.73	5.59	6.05	33.11
Cyber-physical person attacks (P)	6.79	4.36	5.45	5.85	29.58
Trespassing in the metaverse (Pr)	4.59	5.34	7.05	5.70	24.50

NOTE: S=Sexual offenses, F=Financial crimes, P = crimes against people, Pr=Crimes against property, O=Other

References

Abdulsattar Jaber, T. (2022). Security risks of the metaverse world. *International Journal of Interactive Mobile Technologies (iJIM), 16*(13), 4–14. https://doi.org/10.3991/ijim.v16i13.33187

Accenture. (2022). *Meet Me in the Metaverse. The continuum of technology and experience, reshaping business (Technology Vision 2022)*. ⟨https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF-5/Accenture-Meet-Me-in-the-Metaverse-Full-Report.pdf⟩. Accessed on 16/06/2022.

Akartuna, E. A., Johnson, S. D., & Thornton, A. E. (2022). The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. *Security Journal*. https://doi.org/10.1057/s41284-022-00356-z

Alkazzi, J.-M., & Rizk, A. (2020). Leveraging NVIDIA's Technology for the Ultimate Industrial Autonomous Transport Robot. GPU Technology Conference,

Allen, C., & McIntosh, V. (2022). *Safeguarding the metaverse: A guide to existing and future harms in virtual reality (VR) and the metaverse to support UK immersive technology policymaking*. ⟨https://www.theiet.org/impact-society/factfiles/information-technology-factfiles/safeguarding-the-metaverse/⟩. Accessed on 12/08/2022.

Annison, T. (2022). *Elliptic Metaverse Report 2022 - The Future of Financial Crime in the Metaverse: Fighting Crypto-crime in Web3.0*. Elliptic. ⟨https://www.elliptic.co/hubfs/Crime%20in%20the%20Metaverse%202022%20final.pdf⟩. Accessed on 12/08/2022.

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology, 8*(1), 19–32. https://doi.org/10.1080/1364557032000119616

Ball, M. (2021, Jun. 29). The Metaverse Primer. *MatthewBall.vc*. ⟨https://www.matthewball.vc/the-metaverse-primer⟩. Accessed on 16/06/2022.

Banaeian Far, S., & Imani Rad, A. (2022). Applying digital twins in metaverse: User interface, security and privacy challenges. *Journal of Metaverse, 2*(1), 8–16.

Beiderbeck, D., Frevel, N., Heiko, A., Schmidt, S. L., & Schweitzer, V. M. (2021). Preparing, conducting, and analyzing Delphi surveys: Cross-disciplinary practices, new directions, and advancements. *MethodsX, 8*, Article 101401.

Bell, C. (2022, Mar. 28). The metaverse is coming. Here are the cornerstones for securing it. *Official Microsoft Blog*. ⟨https://blogs.microsoft.com/blog/2022/03/28/the-metaverse-is-coming-here-are-the-cornerstones-for-securing-it/⟩. Accessed on 12/08/2022.

Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal, 34*(1), 97–125.

Buck, L., & McDonnell, R. (2022). *Security and Privacy in the Metaverse: The Threat of the Digital Human.* ACM CHI Conference on Human Factors in Computing Systems. Session: SSPXR - Novel Challenges of Safety, Security and Privacy in Extended Reality, Online.

Callaghan, N. (n.d.). Simon Harris in conversation with Meta. PwC United Kingdom [Interview]. ⟨https://www.pwc.co.uk/industries/technology-media-and-telecommunications/insights/transcript-simon-harris-in-conversation-with-meta/video-transcript–simon-harris-in-conversation-with-meta.html⟩. Accessed on 16/06/2022.

Chang, L., Zhang, Z., Li, P., Xi, S., Guo, W., Shen, Y., Xiong, Z., Kang, J., Niyato, D., & Qiao, X. (2022). 6G-enabled Edge AI for Metaverse: Challenges, Methods, and Future Research Directions. *arXiv preprint arXiv:2204.06192*.

Chen, D., & Zhang, R. (2022). Exploring research trends of emerging technologies in health metaverse. *A Bibliometric Analysis*. Available *at SSRN 3998068*.

Cheng-Han, T., & Kiat-Boon, D. S. (2023). The Metaverse beyond the internet. *Law Innovation and Technology*, 1–44.

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

Christodoulou, K., Katelaris, L., Themistocleous, M., Christodoulou, P., & Iosif, E. (2022). NFTs and the metaverse revolution: research perspectives and open challenges. *Blockchains and the Token Economy: Theory and Practice*, 139–178.

CITIC Telecom International. (2022, Jul. 5). CITIC telecom international: (metaverse business opportunities) changing consumption patterns with immersive experience & deconstructing blind spots of blockchain security applications https://www.proquest.com/magazines/citic-telecom-international-metaverse-business/docview/2686181145/se-2. Accessed on 12/08/2022.

Clark, P.A. (2021, Nov. 15). The Metaverse Has Already Arrived. Here's What That Actually Means. Time. https://time.com/6116826/what-is-the-metaverse/. Accessed on 16/06/2022.

Clayton, M. (2022, Jan. 30). Mother, 43, has her avatar groped by three male characters in the online Metaverse. *Daily Mail Online*. ⟨https://www.dailymail.co.uk/news/article-10455417/Mother-43-avatar-groped-three-male-characters-online-Metaverse.html⟩. Accessed on 12/08/2022.

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

Combs, V. (2022). Metaverse security: How to learn from Internet 2.0 mistakes and build safe virtual worlds. *Tech Republic*. https://www.techrepublic.com/article/metaverse-security-learn-lessons-from-internet-2-0-mistakes-to-build-safe-virtual-worlds/. Accessed on 30/08/2022.

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology, 25*(4), 933–948.

Coutorie, L. E. (1995). The future of high-technology crime: A parallel Delphi study. *Journal of Criminal Justice, 23*(1), 13–27.

Craig, C. (2018). Risk management in a policy environment: The particular challenges associated with extreme risks. *Futures, 102*, 146–152.

Crawford, A., & Smith, T. (2022, Feb. 23). Metaverse app allows kids into virtual stripclubs. ⟨https://www.bbc.co.uk/news/technology-60415317⟩. Accessed 30/08/2022.

Creswell, A., White, T., Dumoulin, V., Arulkumaran, K., Sengupta, B., & Bharath, A. A. (2018). Generative adversarial networks: An overview. *IEEE Signal Processing Magazine, 35*(1), 53–65.

Cunha Barbosa, D. (2022, Apr. 5). What security risks could be hidden in the Metaverse? (¿Qué riesgos de seguridad puede esconder el Metaverso?). We live security by ESET. https://www.welivesecurity.com/la-es/2022/04/05/riesgos-seguridad-puede-esconder-metaverso/. Accessed on 31/08/2022.

Dalal, S., Khodyakov, D., Srinivasan, R., Straus, S., & Adams, J. (2011). ExpertLens: a system for eliciting opinions from a large pool of non-collocated experts with diverse knowledge. *Technological Forecasting and Social Change, 78*(8), 1426–1444.

Dalton, J. (n.d.). Legal and regulatory challenges in the enterprise application of virtual and augmented reality: What lies ahead. *PwC United Kingdom*. ⟨https://www.pwc.co.uk/issues/intelligent-digital/virtual-reality-vr-augmented-reality-ar/legal-regulatory-challenges-enterprise-application-virtual-augmented-reality.html⟩. Accessed on 16/06/2022.

Dataquest. (2022). What are the security risks and privacy challenges in Metaverse. Dataquest. https://www.proquest.com/trade-journals/what-are-security-risks-privacy-challenges/docview/2639107215/se-2?accountid=14511 https://ucl-new-primo.hosted.exlibrisgroup.com/openurl/UCL/UCL_VU2?url_ver=Z39.88–2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&sid=ProQ:ProQ%3Ahightechjournals&atitle=What+are+the+security+risks+and+privacy+challenges+in+Metaverse&title=Dataquest&issn=0970034X&date=2022–03-15&volume=&issue=&spage=&au=&isbn=&jtitle=Dataquest&btitle=&rft_id=info:eric/&rft_id=info:doi/. Accessed on 12/08/2022.

Deloitte. (2022). A whole new world? Exploring the metaverse and what it could mean for you. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/us-ai-institute-what-is-the-metaverse-new.pdf. Accessed on 16/06/2022.

Deloitte. (n.d.). Ed on the metaverse. Can it bring people closer than ever? https://www2.deloitte.com/uk/en/pages/consulting/articles/what-is-the-metaverse.html?gclid=EAIaIQobChMIp7ul9eyq-AIVxbHtCh3Q2gEzEAAYASAAEgJx6vD_BwE. Accessed on 16/06/2022.

China, Deloitte (2022). The Metaverse Overview: Vision. *Technology, and Tactics*, 2022. https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/metaverse-report.html. Accessed on 28/06.

Dey, V. (2022, Jun. 2). Data Privacy In Metaverse Is An Evolving Concern. Martech Vibe. https://martechvibe.com/martech/data-privacy-in-metaverse-is-an-evolving-concern/. Accessed on 30/08/2022.

Di Pietro, R., & Cresci, S. (2021). Metaverse: Security and Privacy Issues. 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA),

Eck, J. E., & Madensen-Herold, T. D. (2018). Place management, guardianship, and the establishment of order. *Deterrence, choice, and crime* (pp. 269–307). Routledge,.

El Saddik, A. (2018). Digital twins: The convergence of multimedia technologies. *IEEE Multimedia, 25*(2), 87–92.

Elgabry, M., Nesbeth, D., & Johnson, S. (2022). The future of biotechnology crime: A parallel Delphi study with non-traditional experts. *Futures, 141*, Article 102970.

Ernst & Young Global Ltd (2022, Apr. 29). How the metaverse and Web3 are creating novel tax issues. https://www.ey.com/en_uk/tax/how-the-metaverse-and-web3-are-creating-real-tax-issues. Accessed on 16/06/2022.
Faraboschi, P., Frachtenberg, E., Laplante, P., Milojicic, D., & Saracco, R. (2022). Virtual worlds (Metaverse): From skepticism, to fear, to immersive opportunities. *Computer, 55*(10), 100–106.
Flood, S., Rogan, F., Revez, A., McGookin, C., O'Dwyer, B., Harris, C., Dunphy, N., Byrne, E., Gallachóir, B.Ó., & Bolger, P. (2023). Imagining climate resilient futures: A layered Delphi panel approach. *Futures, 147*, Article 103100.
Forster, A. [AntoniaR.Forster]. (2022, Feb. 13). *In my upcoming "no nonsense" metaverse talk, I'm going to try to identify the types of traits/features people mean when they use the M-word. The more traits, the more metaverse-y the experience. Anything you would add to this list? Have I overlooked anything obvious?* ⟨https://twitter.com/AntoniaRForster/status/1493002727433060358⟩. Accessed on 16/06/2022.
Foutty, J., & Bechtel, M. (2022). What's all the buzz about the metaverse? On the board's agenda. Deloitte. https://www2.deloitte.com/us/en/pages/center-for-board-effectiveness/articles/whats-all-the-buzz-about-the-metaverse.html. Accessed on 16/06/2022.
Gonzalez, Y. (2022, Jul. 3). These brands have filed metaverse trademarks–and what it all means; Following Meta's and Nike's lead, several food, entertainment and retail companies have filed trademarks to sell virtual goods. AdAge, 93(4), 0013. https://link-gale-com.libproxy.ucl.ac.uk/apps/doc/A696310881/AONE?u=ucl_ttda&sid=bookmark-AONE&xid=d86d9e0b.
Goossens, S., Morgan, C., Kuru, C., Ji, F., & Cespedes, D. J. (2021). Protecting intellectual property in the metaverse. *Intellectual Property & Technology Law Journal, 33*(9), 11–16.
Gough, D., Oliver, S., & Thomas, J. (2017). *An introduction to systematic reviews*. Sage.
Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information & libraries Journal, 26*(2), 91–108.
Grayscale Investments LLC. (2021). *The Metaverse: Web 3.0 Virtual Cloud Economies*. ⟨https://grayscale.com/learn/the-metaverse/⟩. Accessed on 16/06/2022.
Green, N., & Works, K. (2022). Defining the metaverse through the lens of academic scholarship, news articles, and social media. *Proceedings of the 27th International Conference on 3D Web Technology*.
Gursoy, D., Malodia, S., & Dhir, A. (2022). The metaverse in the hospitality and tourism industry: An overview of current trends and future research directions. *Journal of Hospitality Marketing & Management*, 1–8.
Harper, C. A., Fido, D., & Petronzi, D. (2021). Delineating non-consensual sexual image offending: Towards an empirical approach. *Aggression and Violent Behavior, 58*, Article 101547.
Harris, S. (2022, Feb. 15). The Metaverse – a game-changer for content creators. *PwC United Kingdom*. ⟨https://www.pwc.co.uk/industries/blog/the-metaverse.html⟩. Accessed on 16/06/2022.
Herrman, J., & Browning, K. (2021, Oct. 29). Are We in the Metaverse Yet? *The New York Times*. ⟨https://www.nytimes.com/2021/07/10/style/metaverse-virtual-worlds.html⟩.
Howell, J. (2022, Feb. 23). 3 Metaverse Security Issues that you must know. 101 Blockchains. https://101blockchains.com/metaverse-security-issues/. Accessed on 30/08/2022.
Huq, N., Reyes, R., Lin, P., & Swimmer, M. (2022). Metaverse or metaworse? Cybersecurity Threats Against the Internet of Experiences. Trend Micro Research. https://documents.trendmicro.com/assets/white_papers/wp-metaverse-or-metaworse-cybersecurity-threats-against-the-internet-of-experiences.pdf. Accessed on 31/08/2022.
Identity Management Institute. (2022). Top 10 Metaverse Risks. *Identity Management Institute*. ⟨https://identitymanagementinstitute.org/top-10-metaverse-risks/⟩. Accessed on 30/08/2022.
INHOPE. (2021). *Annual Report, 2020*. ⟨https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839–1620144551/inhope-annual-report-2020⟩. Accessed on 13/03/2023.
Joy, A., Zhu, Y., Peña, C., & Brouard, M. (2022). Digital future of luxury brands: Metaverse, digital fashion, and non-fungible tokens. *Strategic Change, 31*(3), 337–343.
Kadar, T. (2022). The Metaverse Fraud Question: What Are the Risks? SEON. https://seon.io/resources/metaverse-fraud/. Accessed on 30/08/2022.
Kanterman, M., & Naidu, N. (2022). Metaverse may be $800 billion market, next tech platform. *Bloomberg Finance L.P.* ⟨https://www.bloomberg.com/professional/blog/metaverse-may-be-800-billion-market-next-tech-platform/⟩. Accessed on 16/06/2022.
Khitrov, A. (2022, Mar. 29). What will it take to stop fraud in the metaverse? *Information Age*. ⟨https://www.information-age.com/what-will-it-take-to-stop-fraud-in-metaverse-19707/⟩. Accessed on 30/08/2022.
Kim, J. (2021). Advertising in the Metaverse: Research agenda. *Journal of Interactive Advertising, 21*(3), 141–144.
Krotoski, A. (2022, May 12). A beginner's guide to the metaverse: What it is, how you can access it and more. BBC Science Focus Magazine. https://www.sciencefocus.com/future-technology/metaverse/.
Kye, B., Han, N., Kim, E., Park, Y., & Jo, S. (2021). Educational applications of metaverse: possibilities and limitations. *Journal of Educational Evaluation for Health Professions, 18*.
Landeta, J., Barrutia, J., & Lertxundi, A. (2011). Hybrid Delphi: A methodology to facilitate contribution from experts in professional contexts. *Technological Forecasting and Social Change, 78*(9), 1629–1641.
Lau, P.L. (2022, Feb. 1). The metaverse: three legal issues we need to address. The Conversation. https://theconversation.com/the-metaverse-three-legal-issues-we-need-to-address-175891. Accessed on 16/06/2022.
Laycock, G. (2004). The UK car theft index: An example of government leverage. *In Understanding and preventing car theft* (Vol. 17,, 25–44.
Lebowits, M.P. (2022). Gaming. *The Future Of. Netflix, Laps entertainment, Vox Media Studios, The Verge. Retrieved from:* ⟨https://www.netflix.com/gb/title/81123425⟩.
Lee, L.-H., Lin, Z., Hu, R., Gong, Z., Kumar, A., Li, T., Li, S., & Hui, P. (2021). When creators meet the metaverse: A survey on computational arts. *arXiv Preprint arXiv, 2111, 13486*.
Li, C., & Lalani, F. (2022, Jan. 14). How to address digital safety in the metaverse. World Economic Forum. https://www.weforum.org/agenda/2022/01/metaverse-risks-challenges-digital-safety/. Accessed on 30/08/2022.
Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: growing up in a digital age: an evidence review* (LSE Media and Communications Report, Issue. ⟨https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf⟩. Accessed on 13/03/2023.
Lovich, D. (2022, May 11). What Is The Metaverse And Why Should You Care? Forbes. https://www.forbes.com/sites/deborahlovich/2022/05/11/what-is-the-metaverse-and-why-should-you-care/?sh=54db2f8a2704. Accessed on 16/06/2022.
Ma, A. (2022, May 23). What is the metaverse, and what can we do there? The Conversation. https://theconversation.com/what-is-the-metaverse-and-what-can-we-do-there-179200. Accessed on 16/06/2022.
Mackenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. *The British Journal of Criminology*.
Mailley, J., Garcia, R., Whitehead, S., & Farrell, G. (2008). Phone theft index. *Security Journal, 21*, 212–227.
McKinsey & Company (2022). Value creation in the metaverse: The real business of the virtual world. https://www.mckinsey.com/business-functions/growth-marketing-and-sales/our-insights/value-creation-in-the-metaverse. Accessed on 16/06/2022.
McKinsey Technology Council. (2022a, Mar. 29). AT the Edge In The promise and peril of the metaverse https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-promise-and-peril-of-the-metaverse. Accessed on 16/06/2022.
McKinsey Technology Council. (2022b, Mar. 29). At the Edge In What is the metaverse—and what does it mean for business?. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/what-is-the-metaverse-and-what-does-it-mean-for-business. Accessed on 16/06/2022.
Microsoft News Center. (2022, Jan. 18). Microsoft to acquire Activision Blizzard to bring the joy and community of gaming to everyone, across every device. Microsoft.com. https://news.microsoft.com/2022/01/18/microsoft-to-acquire-activision-blizzard-to-bring-the-joy-and-community-of-gaming-to-everyone-across-every-device/. Accessed on 24/06/2022.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Group*, P. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of Internal Medicine, 151*(4), 264–269.
Morini Bianzino, N. (2022, Feb. 14). Metaverse: 5 questions shaping the next frontier of human experience. *Ernst & Young*. ⟨https://www.ey.com/en_uk/digital/metaverse-5-questions-shaping-the-next-frontier-of-human-experience⟩. Accessed on 16/06/2022.
Mystakidis, S. (2022). Metaverse. *Encyclopedia, 2*(1), 486. https://doi.org/10.3390/encyclopedia2010031
Neto, A. C. d A., Eyland, S., Ware, J., Galouzis, J., & Kevin, M. (2013). Internet sexual offending: Overview of potential contributing factors and intervention strategies. *Psychiatry, Psychology and law, 20*(2), 168–181.
Newton, C. (2021, Jul. 22). Mark in the metaverse: Facebook's CEO on why the social network is becoming 'a metaverse company'. The Verge. https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview?scrolla=5eb6d68b7fedc32c19ef33b4. Accessed on 16/06/2022.
Nichols, S. (2022, Feb. 7). Metaverse rollout brings new security risks, challenges. Tech Target. https://www.techtarget.com/searchsecurity/news/252513072/Metaverse-rollout-brings-new-security-risks-challenges. Accessed on 30/08/2022.
Ning, H., Wang, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., Ding, J., & Daneshmand, M. (2021). A Survey on Metaverse: the State-of-the-art, Technologies, Applications, and Challenges. *arXiv Preprint arXiv, 2111, 09673*.
Norman, D. (2013). *The design of everyday things: Revised and expanded edition*. Basic Books.
Ogden, J. A., Petersen, K. J., Carter, J. R., & Monczka, R. M. (2005). Supply management strategies for the future: A Delphi study. *Journal of Supply Chain Management, 41*(3), 29–48.
Parisi, T. (2021, Oct. 22). The Seven Rules of the Metaverse: A framework for the coming immersive reality. Medium. https://medium.com/meta-verses/the-seven-rules-of-the-metaverse-7d4e06fa864c. Accessed on 16/06/2022.
Park, S.-M., & Kim, Y.-G. (2022). A metaverse: Taxonomy, components, applications, and open challenges. *IEEE Access, 10*, 4209–4251.
PCQuest. (2022, Mar. 30). Security risks that lurk deep inside the Metaverse. https://www.proquest.com/magazines/security-risks-that-lurk-deep-inside-metaverse/docview/2645890572/se-2. Accessed on 12/08/2022.
Pease, K. (1997). Crime reduction. In M. Maguire (Ed.), *The Oxford Handbook of Criminology* (2nd ed). Oxford: Clarendon Press.
Peters, M. D., Marnie, C., Tricco, A. C., Pollock, D., Munn, Z., Alexander, L., McInerney, P., Godfrey, C. M., & Khalil, H. (2020). Updated methodological guidance for the conduct of scoping reviews. *JBI Evidence Synthesis, 18*(10), 2119–2126.
Pinnock, B. (2022, Jul. 26). The metaverse will not be immune to cyber threats. *The Mail & Guardian*. ⟨https://mg.co.za/opinion/2022–07-26-the-metaverse-will-not-be-immune-to-cyber-threats/⟩. Accessed on 12/08/2022.
Ravenscraft, E. (2022, Apr. 25). What Is the Metaverse, Exactly? Everything you never wanted to know about the future of talking about the future. Wired. https://www.wired.com/story/what-is-the-metaverse/. Accessed on 16/06/2022.
Reed, N., & Joseff, K. (2022). Kids and the Metaverse: What Parents, Policymakers, and Companies Need to Know. https://www.commonsensemedia.org/sites/default/files/featured-content/files/metaverse-white-paper.pdf. Accessed 12/08/2022.
Rice, K. (2022, Apr. 24). In K. Rice, Inside the Metaverse Are You Safe? Dispatches. Channel 4. https://www.channel4.com/programmes/inside-the-metaverse-are-you-safe-dispatches.
Roach, J. (2021, Nov. 2). Mesh for Microsoft Teams aims to make collaboration in the 'metaverse' personal and fun. Microsoft.com. https://news.microsoft.com/innovation-stories/mesh-for-microsoft-teams/. Accessed on 24/06/022.
Rosenberg, L. (2022, Apr. 25). Evil twins and digital elves: How the metaverse will create new forms of fraud and deception. The Future. https://bigthink.com/the-future/metaverse-fraud-digital-twins/. Accessed on 30/08/2022.
Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: issues and analysis. *International Journal of Forecasting, 15*(4), 353–375.
Rowe, G., Wright, G., & McColl, A. (2005). Judgment change during Delphi-like procedures: The role of majority influence, expertise, and confidence. *Technological Forecasting and Social Change, 72*(4), 377–399.
Russia Business News. (2022, Jun. 16). "Technologies for protecting children on the Internet": Rostelecom identified 10 cyber risks of future. https://www.proquest.com/magazines/technologies-protecting-children-on-internet/docview/2677618257/se-2. Accessed on 12/08/2022.
Sampson, R., Eck, J. E., & Dunham, J. (2010). Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure. *Security Journal, 23*, 37–51.
Sexual Offences Act (2003). https://www.legislation.gov.uk/ukpga/2003/42/contents. Accessed on 13/03/2023.
Shanker, S. S., & Zytko, D. (2022). *The.Tinderverse?: Opportunities and Challenges for User Safety in Extended Reality (XR) Dating Apps*. Cornell University Library, arXiv.org.
Shen, X. (2022, Feb. 15). NFTs and metaverse top tech risks, officials say: Government watchdog warns criminals could steal sensitive user data or access accounts to hijack money as value of cryptocurrency keeps rising. South China Morning Post. https://www.proquest.com/newspapers/nfts-metaverse-top-tech-risks-officials-say/docview/2628333575/se-2. Accessed on 12/08/2022.
Sin, R., & Kanterman, M. (2022, Feb. 22). Metaverse's $80 billion ETF assets by 2024 virtually a reality. Bloomberg Finance L.P. https://www.bloomberg.com/professional/blog/metaverses-80-billion-etf-assets-by-2024-virtually-a-reality/?tactic-page=600488. Accessed on 16/06/2022.
Singh, M. (2022, May 10). Bottom-up look at metaverse landscape. *Bloomberg Finance L.P.* ⟨https://www.bloomberg.com/professional/blog/bottom-up-look-at-metaverse-landscape/?tactic-page=596574⟩. Accessed on 16/06/2023.
Smaili, N., & de Rancourt-Raymond, A. (2022). Metaverse: welcome to the new fraud marketplace. *Journal of financial crime*(ahead-of-print).
Sum of Us. (2022). *Metaverse: another cesspool of toxic content*. ⟨https://www.sumofus.org/images/Metaverse_report_May_2022.pdf⟩. Accessed on 12/08/2022.
Tang, F., Chen, X., Zhao, M., & Kato, N. (2022). The roadmap of communication and networking in 6G for the metaverse. *IEEE Wireless Communications*, 1–15. https://doi.org/10.1109/MWC.019.2100721
Targeted News Service. (2022, May. 12). Ala. Securities Commission: Five States File Enforcement Actions to Stop Russian Scammers Perpetrating Metaverse Investment Fraud. *Targeted News Service*. ⟨https://www.proquest.com/wire-feeds/ala-securities-commission-five-states-file/docview/2662617069/se-2⟩. Accessed on 12/08/2022.
Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology, 8*(1), 1–10.
Thomason, J. (2021). MetaHealth-how will the metaverse change health care? *Journal of Metaverse, 1*(1), 13–16.
Tichy, G. (2004). The over-optimism among experts in assessment and foresight. *Technological Forecasting and Social Change, 71*(4), 341–363.
Tompson, L., & Belur, J. (2016). Information retrieval in systematic reviews: a case study of the crime prevention literature. *Journal of Experimental Criminology, 12*(2), 187–207.
Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D., Horsley, T., & Weeks, L. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. *Annals of Internal Medicine, 169*(7), 467–473.
Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crimean Science, 11*(1), 1–35.
Van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy, 25*(2), 183–189.
Vasek, M., & Moore, T. (2015). There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. Financial Cryptography and Data Security: 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26–30, 2015, Revised Selected Papers 19,
Vladimirov, I., Nenova, M., Nikolova, D., & Terneva, Z. (2022). Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse: A Survey 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST), Ohrid, North Macedoni.
Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *arXiv Preprint arXiv, 2203, 02662*.

WeProtect Global Alliance. (2021). *Global Threat Assessment*. ⟨https://www.weprotect.org/global-threat-assessment-21/#report⟩. Accessed on 13/03/2023.

Williams, C. (2021, Oct. 29). *Facebook's Metaverse a dangerous breeding ground for crime and mental health issues, experts says: Facebook wants us to move away from our phones and into a virtual reality. The scandal-plagued platform has a new - Meta - and will launch a new platform, which will be accessed through a headset and not a phone. Tech experts have raised concerns about how crime will be policed in this new universe. Especially if Facebook can't quite get a hold of the issues it has already* Sydney, Australian Broadcasting Corporation. ⟨https://www.abc.net.au/radio/programs/pm/facebooks-metaverse-a-dangerous-breeding-ground/13609832⟩.

Woods, L. (2022, Feb. 4). Regulating the future: the Online Safety Bill and the metaverse. Carnegie Uk Trust. https://www.carnegieuktrust.org.uk/blog-posts/regulating-the-future-the-online-safety-bill-and-the-metaverse/. Accessed on 16/06/2022.

Zhao, R., Zhang, Y., Zhu, Y., Lan, R., & Hua, Z. (2022). Metaverse: Security and privacy concerns. *arXiv Preprint arXiv, 2203, 03854*.