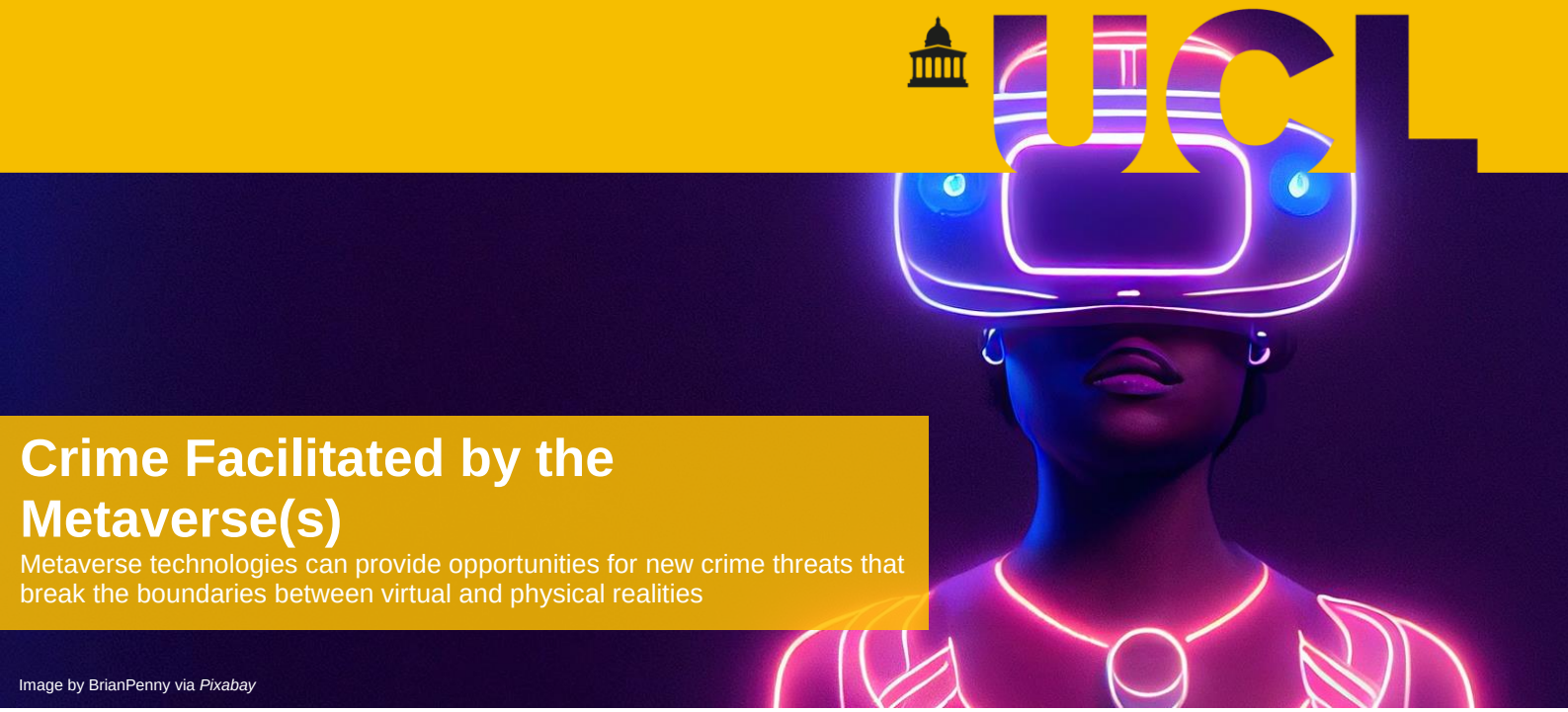

# Crime Facilitated by the Metaverse(s)

Metaverse technologies can provide opportunities for new crime threats that break the boundaries between virtual and physical realities

Image by BrianPenny via *Pixabay*


## Summary

Metaverse technologies – such as virtual reality devices or haptic suits – allow users to experience new realities that integrate both physical and virtual environments. While legitimate uses are both exciting and have enormous potential, these technologies can enable (new) harmful and criminal activities. These can differ from familiar online crimes because of the immersive nature of metaverse interactions and their physical implications. This briefing discusses crime threats that can be facilitated by the metaverse – as identified in the literature and by experts – and discusses the suitability of existing legal frameworks to effectively support their prevention and prosecution.


## Introduction

The metaverse or metaverses are an emerging convergence of technologies that enable users to experience mixed/extended realities (i.e. the merging of physical and virtual environments) for a range of legitimate purposes. There is significant investment in the metaverse(s) and PwC's 2022 Metaverse survey indicates that 82% of executives expect their business plans to include the metaverse(s) in the next three years[1].

Different definitions[2] exist but common aspects of what the metaverse(s) are or will be include:

- **Immersive:** By encapsulating a user's field of view, and through other sensory inputs (e.g. sound, physical interaction), virtual reality can create the perception that the user is physically present in a virtual environment;
- **Spatial:** activity occurs either in simulated spatial environments (virtual reality) or in physical environments enhanced by virtual content (augmented reality);
- **Use of avatars:** users are visually represented as avatars – not necessarily human-like, but these can be photorealistic[3];
- **Multiuser:** multiple users can interact at the same time, even in massive numbers;
- **Multipurpose**: it can be used for retail, work, gaming, social activities etc;
- **Multiplatform:** there will likely be multiple interconnecting platforms;
- **Involving persistent ownership:** of avatars and digital assets (registered using non-fungible tokens – NFTs) such as virtual land and property (e.g. houses, clothes or cars), cryptocurrencies etc.

**Legitimate use cases** of the metaverse include gaming, art and entertainment, hospitality and tourism, work and collaboration, education and training, retail and advertising, and health and wellbeing. For example, organisations have created digital twins of their offices in which users

[1] PWC (2022) *PwC 2022 US Metaverse Survey*. Available at https://www.pwc.com/us/en/tech-effect/emerging-tech/metaverse-survey.html

[2] Forster, A. (2022) *Metaverse NEXT - Antonia Forster - 'How to Build a Metaverse' - Lethbridge College*. Available at https://www.youtube.com/watch?v=ewJEp1aB_08&ab_channel=AntoniaForster

[3] For example, https://research.facebook.com/publications/pixel-codec-avatars/

can meet and interact much like they would in the real locations. High risk, hard to master training scenarios can be simulated and repeatedly practiced in safe (realistic) virtual settings. Immersive virtual concerts can be (and are) held, enabling many more users to attend than would be possible or safe in the real-world. Physical manufacturing systems can be (and are) controlled from virtual environments increasing efficiency. The opportunities for legitimate uses cases are clearly substantial.

## Metaverse technologies

Notions of the metaverse have existed for some time, but it is only recently that the necessary investment and developments of the contributing technologies have made it possible to start realising it at scale.

Key technologies already available to consumers to access and interact in the metaverse include:

- **Virtual and augmented reality devices** that blend physical and virtual environments, enabling users to experience the metaverse (such as exploring purely imagined virtual worlds or digital twins of real ones) in a much more immersive way than would be possible through a tablet or computer;

- **Haptic suits** (wearable devices that simulate physical sensation, including touch and pain) can already be bought from high-street stores and provide a further level of immersion, enabling users to "feel" interactions with others;

- **Teledildonics** (electronic devices to simulate sexual interaction) extend the types of interactions possible and facilitate virtual sexual encounters.

Future developments that would enhance the level of immersion still further include **brain-computer interfaces** (BCIs)[4] which are currently being developed by a number of technology companies (e.g., BrainGate, Neuralink). These will enable direct communication between the brain and an external device.

It is difficult to articulate on paper just how immersive the metaverse can be today. However, it will likely be **still more immersive in the future**. This has implications for online behaviours and interactions which, with a greater level of immersion, may have more significant impacts on people than do similar behaviours on the internet as most people have experienced it to date. While this may be of enormous value to society, it may be particularly problematic for criminal behaviours or those that are illegal in the real world but perhaps currently not so online.

## Crime risks in the metaverse

The scoping study identified **32 crime threats.** These were rated by two expert groups (with representatives from law enforcement, government, industry, academia and the voluntary sector, and with participants from around the world) at workshops conducted in London and Singapore. They were rated in terms of:

- **Harm -** 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.

- **Frequency -** The likely number of times the scenario would occur in a period of time.

- **Achievability -** How easy would it be to commit an offense, accounting for likely readiness of the necessary technology and its availability.

- **Defeat-ability -** How easy would it be to develop/apply measures to prevent, detect or render the offence unrewarding.

To create a ranking of the threats, **an index of risk** was computed by multiplying the harm and frequency ratings together. In this briefing, we describe the top ten high risk crimes (based on the ratings from the London workshop) and show their ratings for risk and defeatability, before providing brief descriptions of the other offences not included in the top-ten.

[4] For a review of BCIs , see: https://www.frontiersin.org/articles/10.3389/fnsys.2021.578875/full; https://theconversation.com/weve-been-connecting-brains-to-computers-longer-than-youd-expect-these-3-companies-are-leading-the-way-197023

| **Top-10 Crime Risks**<br>Rating key: ● Low ●● Medium ●●● High | **Risk** | **Defeat-ability** |
|---|---|---|
| **Child Sexual Abuse Material -** Paid-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. | ●●● | ●● |
| **Child grooming -** Children's avatars could be approached by avatars operated by adults to engage them in sexual activities. | ●●● | ●●● |
| **Investment Scams** - Offenders could exploit metaverse investment hype to commit a range of scams, including giveaway scams, fake metaverses, wearable minting scams, technical support scams, fake land expansions, rug pulls and pump and dump schemes. | ●●● | ●● |
| **Hate Crime** - In virtual settings, a user could be approached by other avatars with the purpose of committing hate crime. | ●●● | ● |
| **Harassment** - In virtual settings, users could be approached by other avatars to harass them; they could even be chased across different metaverse platforms. | ●●● | ●● |
| **Sexual Assault -** An adult user could be approached indecently and forcefully by other avatars operated by malicious actors with the purpose of sexual assault. | ●●● | ●● |
| **Non-consensual sexual image offenses** - Malicious actors could exploit personal, sensitive, and explicit material shared by users for virtual reality non-consensual sex acts. This could also involve the use of deepfakes. | ●●● | ● |
| **Doxing -** Malicious actors could exploit the rich information that will be collected from metaverse users (e.g., bio data and eye tracking) to extort or shame users. | ●●● | ● |
| **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. | ●● | ●● |
| **Radicalisation -** AI designed to be empathetic avatars and multiuser spaces could be used to radicalise vulnerable users (e.g., under-aged individuals). | ●● | ●● |

## Other Offences (Ranked 11+)

### Sexual Offences

#### Virtual trafficking of people for sexual exploitation
Avatars of vulnerable users could be sexually exploited repeatedly in virtual settings without the need to cross borders or disappearing.

#### 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 multiuser spaces could be created so that many users can experience it together.

### Crimes against the person

#### 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).

#### Incitement to self-harm
Several users could come together in a virtual setting to incite vulnerable users to self-harm. AI designed avatars could be made to be more empathetic, and to even incite massive self-harm.

#### 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.

#### Child labour and modern slavery to develop metaverse content
The demand for digital goods, assets and services will create incentives to undercut competitors, perhaps by using child labour and modern slavery.

### Financial crimes

#### Blockchain attacks
Vulnerabilities in blockchain technology could be exploited to steal digital assets (e.g. NFTs) or currency from users.

#### 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.

#### Copyright infringement
Sound, software, pictorial/ 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.

#### Counterfeiting
Malicious actors could create counterfeit digital goods (including NFTs) posing as licit products from brands (e.g., fake digital Gucci bags).

#### 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.

#### Impersonation scam
Criminals could potentially impersonate service providers like doctors and give false medical advice to patients in return for payment.

#### Money laundering
Malicious actors could use metaverse-based assets (e.g., crypto currency and assets, virtual land, wearables) to launder illicit funds.

#### Tax evasion
A company that exists only in the metaverse may lack a logical jurisdiction and, for example, could effectively avoid paying income taxes.

### Property crimes

#### 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 at physical locations.

#### Cyber-physical infrastructure attacks
Digital twins and the connection of infrastructure to the metaverse via internet connected technologies could be exploited by malicious actors to plan and perpetrate attacks against infrastructure.

#### Trespassing in the metaverse
Offenders could trespass virtual properties or virtual events in the metaverse without permission.

#### 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).

### Other offences

#### Impersonating a LEA
Criminals can pretend to be law enforcement authorities in the metaverse for a variety of purposes, including gaining intelligence.

#### Conspiring
Malicious actors could use detailed virtual spaces that resemble real world locations (e.g. digital twins) to plan and train to commit crime in the physical world.

#### 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.

#### 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.

## Policy implications

The identified crime risks pose new policy and legal challenges related to the prevention and prosecution of the crime threats identified. The implications are global, but for brevity we focus on the UK here, noting that the issues discussed will have wider application.

### Prevention

The effective prevention of metaverse-facilitated crime requires a complex strategy including a broad range of interventions, each targeting specific activities, situations, and technologies. In the UK, the Online Safety Act 2023 is a significant contribution towards this, by introducing a comprehensive regulatory online safety regime that is also relevant to metaverse platforms. The Act seeks to make user-to-user and search internet services 'safe by design' by imposing on their providers specific duties of care, including:

- Conducting a suitable and updated **illegal content risk assessment**;
- Taking **safety measures** relating to the **design or operation** of the service to minimise exposure to illegal content and mitigate the risks of criminal exploitation of the service, as well as harms to individuals;
- Including in the service **features to increase adult users' control** over content (so-called 'user empowerment');
- Including in the **terms of service** clear and accessible provisions on risks and control features;
- Implementing systems for users and affected persons to **report** illegal content and content harmful to children;
- Operating easy to use and accessible **complaints procedures**;
- Keeping **record** of risk assessments and safety measures and **regularly reviewing** compliance with the duties of care.

The Act gives OFCOM extensive powers to supervise and enforce these duties and requires it to issue a code of practice – currently in preparation[5] – to specify the measures required to comply with the duties of care.

In its current formulation, the Act already applies to metaverse-related services. Most current metaverse platforms fall within the definition of a 'user-to-user service' under section 3(1) of the Act, as they are internet-based services that enable users to generate, upload, and share content and encounter content generated by other users. Moreover, the use of technology-neutral terminology makes many provisions of the Act applicable to metaverse-related technologies, including future ones. However, some features of the Act might limit the preventive effectiveness of its provisions with regards to metaverse-related crime risks.

The first section of the Act clarifies that the duties of care concern both illegal content and activities.[6] The word 'activities' was introduced during the later stages of the legislative process in response to concerns (including a submission from the Dawes Centre for Future Crime) that emerged in Parliament about the (in)ability of earlier versions of the Online Safety Bill to tackle online behaviours that do not fit the definition of 'content' provided by the Act (ss. 59 and 236). This is precisely the case for many metaverse interactions such as those involving haptic technologies or avatars. However, the provisions regulating the duties of care remain focused mostly on 'illegal content', to the extent that the term 'activities' is not even defined in the Act. This could lead to restrictive interpretations and implementations of the Act excluding illegal metaverse activities from the scope of the risk assessment and the safety measures. **It is essential that OFCOM and any relevant stakeholders take full advantage of the explicit reference to online 'activities' to promote a broad application of the Act**.

Important exceptions to the predominant focus on 'illegal content' are the duty for online service providers to assess the risk of the service being used for the commission or facilitation of any offence defined by the act as 'priority offences'[7] and the corresponding duty to adopt proportionate safety measures to mitigate them.[8] The list of 'priority offences' [9] includes several crimes discussed in his briefing such as child sexual exploitation and abuse, harassment, hate crimes, stalking, the non-consensual disclosure of private sexual images, fraud and money laundering. Nevertheless, some of the illegal or harmful activities identified in this briefing are not on the list. This is the case for offences including

[5] OFCOM (2024) *Consultation: Protecting people from illegal harms online*. Available at https://www.ofcom.org.uk/consultations-and-statements/category-1/protecting-people-from-illegal-content-online
[6] Online Safety Act 2023, s. 1
[7] Ibid., s. 9(5)(c).
[8] Ibid., s. 10(2)(b).
[9] Ibid., s. 53(7) and sch. 5, 6, and 7.

offences against the person such as common assault, battery, assault occasioning bodily harm. malicious wounding, sexual assaults against adults or the more generic (and, therefore, potentially helpful) offence of causing adults to engage in sexual activity without consent. The exclusion of the latter is quite surprising, given that the equivalent offence against children is included amongst the priority offences.[10]

A more general obstacle to the implementation of the Act is its length (currently 241 sections and 17 schedules) and overall complexity, which could make it impenetrable for many and aggravate interpretative difficulties.

OFCOM can play a pivotal role in addressing some of these shortcomings by including metaverse-specific guidance in the code of practice and, more generally, encouraging and supporting online service providers to adequately address metaverse-related crime risks. The success of these activities will depend on OFCOM's continuous monitoring and understanding of emerging crime threats in the metaverse in collaboration with relevant stakeholders. It will also be essential for OFCOM to promote any legislative interventions that might prove necessary later on, such as additions to the list of priority offences.

## Prosecution

A preliminary review of English criminal law suggests that many of the metaverse-facilitated crime threats identified here can already be prosecuted under existing laws, as they fit the legal definitions of existing offences. This is the case for offences that are defined in 'technology-neutral' terms and can be perpetrated through any means, including metaverse technologies. These include:

- offences related to indecent or prohibited photographs or images of minors;[11]
- child sexual exploitation and abuse offences;[12]
- encouraging or assisting serious self-harm;[13]
- fraud and related offences;[14]
- harassment and stalking offences;[15]
- racially and religiously aggravated offences;[16]
- offences related to the incitement of and support of terrorism or hatred;[17]
- money laundering offences;[18]
- tax crimes;[19]
- conspiracy.[20]

Moreover, metaverse-related acts against computer systems or data, which can also be instrumental for real-world crime (e.g. burglary), can be prosecuted under the Computer Misuse Act 1990, which includes the following offences[21]:

- unauthorised access to computer material;
- unauthorised access with intent to commit or facilitate further offences;
- unauthorised acts seeking to impair such systems or data or create serious material damage (i.e., to human welfare, the environment, the economy or national security);
- making, supplying, or obtaining of articles to be used in these offences.

However, some metaverse-related harmful activities do not neatly fit the legal definitions of their equivalent real-life offences and **more creative approaches or legal reform** are required to prosecute these.

In some cases, the wording of existing offences might lend itself to be **interpretatively extended to metaverse-related activities**. For instance, the notion of 'property' under the Theft Act 1968[22] – which is a constitutive element of both theft and robbery – includes also 'intangible property' and could apply to virtual assets. [23] Other offences that require harmful events but do not specify the acts that cause them, such as assaults that involve 'inflicting'[24] or 'occasioning'[25] injury or harm or the offence of 'causing a person to engage in sexual

[10] Ibid., sch. 6.
[11] E.g., Protection of Children Act 1978, s. 1; Criminal Justice Act 1998, s. 160; Sexual Offences Act 2003, s. 8; Coroners and Justice Act 2009, s. 62.
[12] E.g., Sexual Offences Act 2003, ss. 8, 10-15A, 47-50.
[13] Suicide Act 1961, s. 2; Online Safety Act 2023, s. 184.
[14] Fraud Act 2006.
[15] E.g., Protection from Harassment Act 1997, ss. 1-2A; Malicious Communication Act 1988, s. 1; Public Order Act 1986, ss. 4-5.
[16] E.g., Crime and Disorder Act 1998 ss. 31 and 32.
[17] E.g., Terrorism Act 2000, ss. 12, 13, 54, 56, 58-61; Terrorism Act 2006, ss. 1, 2, 5, 6, 11; Public Order Act 1986, ss. 18, 19, 21, 29B, 29C, 29E.
[18] Proceeds of Crime Act 2002, ss. 327-334.
[19] E.g., Taxes Management Act 1970, ss 106A-106D; Value Added Tax Act 1994, ss 59-72; Criminal Finances Act 2017, ss 45-46; Theft Act 1968, s 17.
[20] Criminal Law Act 1977, s. 1.
[21] Computer Misuse Act 1990, ss. 1-3A.
[22] Theft Act 1968, s. 4.
[23] Taylor, A. and Ó Floinn, M. (2021) 'Bitcoin burglaries and the Theft Act 1968.' *Criminal Law Review*, 2021(3), pp. 163-190.
[24] Offences against the Person Act 1861, ss. 18 and 20.
[25] Offences against the Person Act 1861, s. 47.

activity without consent', [26] could apply also to interactions through haptic technologies. However, such interpretations are far from established in practice, and are not yet supported by specific judicial precedents. As such, they are still open to debate and might not be upheld in court.

In other cases, **extensive interpretations might not be feasible**. This is, notably, the case for harmful acts, such as assaults, robberies, or sexual offences, committed by one avatar against another. [27] These acts would fail to satisfy the common requirement that those offences are committed against a 'person'. [28] Interpretations seeking to stretch the letter of the law to cover purely virtual interactions between avatars would be in tension with rule of law principles such as legality and Parliamentary sovereignty. As such, they might attract public criticism and fail to withstand judicial scrutiny. To avoid these pitfalls, prosecutors might attempt to charge alternative offences that, while not exactly mirroring the acts of avatars would still reflect some of the circumstances of the case. For instance, the act of one avatar stealing virtual assets from another could be prosecuted as an unauthorised act with the intent to prevent access to the computer data that comprise the virtual asset under the Computer Misuse Act 1990. [29] This approach might also entail some creative interpretation that might be challenged in court. Most importantly, the alternative offences might not really reflect the nature and seriousness of the harmful behaviour.

**Jurisdiction** can be an additional hurdle to prosecution, given that the metaverse, like cyberspace, does not have any territorial boundaries. The English law extends the extraterritorial jurisdiction of criminal courts to some relevant offences, such as offences against the person,[30] sexual offences against minors, [31] some serious forms of harassment and stalking,[32] theft, fraud and related offences,[33] some terrorism offences,[34] or computer misuse offences.[35] These and similar provisions are helpful but do not cover all possible offences that can be committed in the metaverse (e.g. sexual offences against adults) and their application to metaverse-related activities can pose new interpretative challenges. [36] However, unlike cyberspace, metaverse environments can have clear virtual boundaries often outlined in three-dimensions much like real spaces and buildings. This might provide new opportunities for lawmakers to think more creatively about jurisdiction in the metaverse – for instance, by anchoring jurisdiction to clearly delineated virtual spaces, when possible.

In conclusion, while it is already possible to prosecute some of the harmful activities facilitated by the metaverse under existing English law, any relevant stakeholders – lawmakers, courts, prosecutors, and legal professionals – should initiate a constructive discussion to build a consensus on the applicability of existing offences to metaverse-related crimes and promote appropriate legislative reforms when necessary. In the meantime, comprehensive guidance from relevant agencies such as the Crown Prosecution Service on how to prosecute crime in the metaverse under the existing law could help reducing uncertainty and provide some deterrence.

[26] Sexual Offences Act 2003, s. 4.
[27] Nix, N. (2024) 'Attacks in the metaverse are booming. Police are starting to pay attention.' *The Washington Post* (6 Feb. 2024). Available at https://www.washingtonpost.com/technology/2024/02/04/metaverse-sexual-assault-prosecution/
[28] Cf. Offences against the Person Act 1861, ss. 18, 20 and 47; Theft Act 1968, s. 8(1); Sexual Offences Act 2003, ss. 2 and 3.
[29] Computer Misuse Act 1990, s. 3.
[30] Domestic Abuse Act 2021, s. 72.
[31] Sexual Offences Act 2003, s. 72.
[32] Protection from Harassment Act 1997, s. 4B.
[33] Criminal Justice Act 1993, s. 2.
[34] E.g., Terrorism Act 2000, ss. 59, 62-63; Terrorism Act 2006, s.17.
[35] Computer Misuse Act 1990, ss. 4-9.
[36] Kingsley Napley (2022) *The metaverse: virtual offences, real world penalties?* Available at https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/the-metaverse-virtual-offences-real-world-penalties

## Methods

- **A systematic review** of the academic literature and industry reports was conducted to identify crime threats that might be facilitated by the metaverse. Rather than include all crime currently committed on the Internet, we focused, in particular, on crime threats that would **only be possible in**, or **made worse by**, the metaverse. Across the 39 relevant articles and reports identified, a total of **22 unique crime threats** were identified.
- We subsequently ran **two workshops** with experts comprised of: 1) a mixed European sample (with participants from law enforcement, industry, academia and the voluntary sector), and; 2) an international sample of law enforcement stakeholders (organised with INTERPOL). The expert groups reviewed the 22 crime threats identified in the literature and were then asked to nominate any additional crimes that they could think of. They added **an additional ten crime threats**.
- **A rating exercise** was subsequently conducted with participants asked to rate the threats in terms of the harm that they would cause, their likely frequency in the future, how easy it would be to achieve them (by offenders) and how difficult it would be to address them (e.g. by governments or law enforcement).
- We then conducted a **black letter analysis of relevant criminal legislation and case law in England and Wales** to detect offences that might apply to the threats identified in the project, as well as any legislative gaps and other challenges to prosecution. The analysis was supported by a review of relevant literature and prosecutorial guidance from the Crown Prosecution Service.
- We also conducted a **black letter analysis** of the various drafts of the **Online Safety Bill and the Online Safety Act 2023**, supported by a review of academic literature and media commentaries, transcripts of parliamentary debates (Hansard), and official explanatory notes.


## Funders

This research was funded by Anglia Ruskin University and the Dawes Centre for Future Crime at UCL, and conducted in collaboration with INTERPOL. **The Dawes Centre for Future Crime at UCL was established to identify how technological, social or environmental change might create new opportunities for crime and to conduct research to address them.**

The Dawes Centre is funded by the Dawes Trust and UCL. These funds are limited and so we invite additional funding from the public and private sector. By funding the Centre you will contribute to helping society better prepare for crimes of the future. We are also able to undertake research upon request, contributing to organisational goals and strategic thinking.


## Find out more about the research

A full academic paper that describes what the metaverse is and the crime threats it might facilitate is available at:

https://doi.org/10.1016/j.futures.2024.103338


## Acknowledgements

The authors would like to thank Sadie Lynch (College of Policing) and Arthur Langellier (INTERPOL) for their comments on this briefing note.



## The authors

Juliana Gómez-Quintero, UCL
Professor Shane Johnson, UCL
Dr Lorenzo Pasculli, UCL
Professor Samantha Lundrigan, Anglia Ruskin University
Professor Hervé Borrion, UCL

**Contact:** Mr Vaseem Khan, Strategic Development Manager, UCL Security & Crime Science **vaseem.khan@ucl.ac.uk,** or Professor Shane Johnson, Director, Dawes Centre of Future Crime, **shane.johnson@ucl.ac.uk**.