INTERPOL

METAVERSE

A LAW ENFORCEMENT PERSPECTIVE

Use Cases, Crime, Forensics, Investigation, and Governance

White Paper

January 2024

TABLE OF CONTENTS

FOREWORD

In every technological advancement, our societies have consistently demonstrated agility in adapting. Whether it is for a better lifestyle or convenience, technology has become an integral part of our modern lives. Among these advancements, disruptive technologies such as the Metaverse could have a significant impact on our societies. This next generation of the Internet is still in its infancy in terms of technology but carries immense potential for change.

While the Metaverse may appear to many as an abstract concept, INTERPOL has already taken a step to be ready for this endeavour. Leveraging its immersive, persistent, and three-dimensional environment, INTERPOL launched the INTERPOL Metaverse in October 2022, allowing registered users to explore a virtual replica of the INTERPOL General Secretariat headquarters in Lyon, France, without any geographical or physical limitations. With more maturity of different technologies consisting of the Metaverse, member countries will be able to interact with fellow officers through their avatars and participate in immersive meetings and training courses on policing capabilities.

In terms of challenges, threats and harms that can arise from the Metaverse, INTERPOL is also set to provide guidance for the global law enforcement community and coordinate an effective response to keep this virtual world safe and secure.

To this end, this White Paper provides an in-depth analysis of various dimensions of the Metaverse from the law enforcement perspective. I cannot emphasize enough the importance of inclusivity and a holistic approach that this effort has taken, and how it was developed in close collaboration with experts from the INTERPOL Metaverse Expert Group.

I would like to extend my sincere gratitude to every member of this Expert Group, whether from law enforcement, governments, the private sector, academia, or other International Organizations, for their invaluable contributions. Their insights were instrumental in identifying what is at stake when we embrace this transformative technology and how law enforcement can approach it. I would also like to thank the Executive Directorate of Technology and Innovation at INTERPOL for pioneering this emerging world.

I trust that this White Paper will serve as an important cornerstone in our efforts to keep our future world safe and secure.

Jürgen Stock
INTERPOL Secretary General

EXECUTIVE SUMMARY

In an ever-evolving world characterized by technological advancements and constant innovation, the agility and resilience of law enforcement are paramount to keep our societies safe and secure. This requires continuous monitoring of new developments and analysis on their impact. To contribute to this effort, the White Paper on the Metaverse was developed based on the inputs from the INTERPOL Metaverse Expert Group to provide valuable insights into the multifaceted aspects of the Metaverse, often described as the long-term vision for the next phase of the Internet.

This paper underscores the Metaverse's potential as an effective tool for law enforcement, especially in immersive training and many other use cases. It presents a typology of Metacrimes and their investigation and forensics, highlighting crucial considerations when accessing and recovering the evidence including endpoints, servers, engines, platforms, and virtual asset analytics. Furthermore, it provides a comprehensive analysis of various dimensions of the Metaverse and its governance from a law enforcement perspective.

The importance of a holistic approach involving multi-stakeholder engagements and cross-border collaboration is highlighted as the Metaverse spans multiple jurisdictions, dimensions, and organizations. INTERPOL is at the forefront of this effort contributing towards a safe fand secure Metaverse.

BACKGROUND AND INTRODUCTION

Bridging the physical and digital worlds, the Metaverse is perceived as the long-term vision for the next phase of the Internet and a powerful tool to transform various aspects of our lives. While there is no internationally agreed-upon definition, one study describes the Metaverse as "a three-dimensional online environment in which users represented by avatars interact with each other in virtual spaces decoupled from the real physical world"[1].

Based on concepts popularized in science fiction and video games, several companies and platforms are focusing on developing various elements of the Metaverse. According to the Gartner, 25% of people will spend at least an hour every day in the Metaverse in 2026[2]. In addition, an estimation was announced in a report that the Metaverse might generate the commercial opportunity as high as 13 trillion $ by 2030[3]. This emerging medium indeed has the potential to reshape how we live, work, play, and interact, much like the Internet does today.

It is important to note, however, that the Metaverse is still in its infancy and there are many technical, social, and ethical challenges that need to be overcome before it can unlock its full potential. The Metaverse is a complex system of various technologies creating synergies to provide an interactive, immersive, persistent, and enhanced user experience. As these technologies continue to advance, the Metaverse will expand and mature, meeting the needs of platform providers, users and other stakeholders.

In the face of rapidly emerging technologies, INTERPOL has been applying a three-dimensional paradigm to analyze each of these innovations as an opportunity, a threat, and a source of evidence from a law enforcement perspective. This paradigm was also used in developing this paper to assess the Metaverse's potential benefits, threats and challenges as well as digital forensics and investigative considerations. This approach enables a balanced perspective to carefully analyze and understand the world of merging technologies.

With the aim to contribute towards a secure-by-design Metaverse, INTERPOL created the INTERPOL Metaverse Expert Group in October 2022. It is a multi-stakeholder group with participation from INTERPOL's member countries, governments, private sector, academia, as well as other International Organizations. The purpose of the Expert Group is to give recommendations and guidance to effectively combat the potential misuse of the Metaverse by criminal actors and to utilize the Metaverse as a tool for law enforcement. This White Paper is the outcome of the extensive and in-depth discussions within the Expert Group and its four subgroups on specific topics around the Metaverse.

1 Ritterbusch, et al., *Defining the Metaverse: A Systematic Literature Review,* 2023, IEEE
2 Gartner, Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026", 2022, https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026
3 Citi Global Perspectives and Solutions, *Metaverse and Money: Decrypting the Future*, 2022, https://www.citifirst.com.hk/home/upload/citi_research/AZRC7.pdf

CHAPTER I
USE CASES OF METAVERSE FOR LAW ENFORCEMENT

The Metaverse, converging physical, augmented, and virtual reality, offers a multifaceted platform for various applications, including those in the field of law enforcement. This section explores concrete use cases of the Metaverse for law enforcement. It assesses the advantages and inherent challenges of its adoption, as well as the future possibilities aimed at enhancing efficiency, safety, and effectiveness.

Law enforcement and digital transformation

Law enforcement agencies have consistently adopted new technologies, from radio systems to body cameras, computing, and every emerging technology to improve public safety and operational efficiency. The digital transformation in policing now looks towards the extended reality and its materialization through the Metaverse as a prospective platform to further these aims. Despite numerous challenges arising from Metaverse, there are opportunities for law enforcement to use it as a tool. These opportunities include building partnerships and networking, convening global conferences, as well as three-dimensional immersive training and digitalizing crime scenes, etc. The use cases of the Metaverse that will have a major impact on policing are outlined below.

Advanced training, education and simulation:

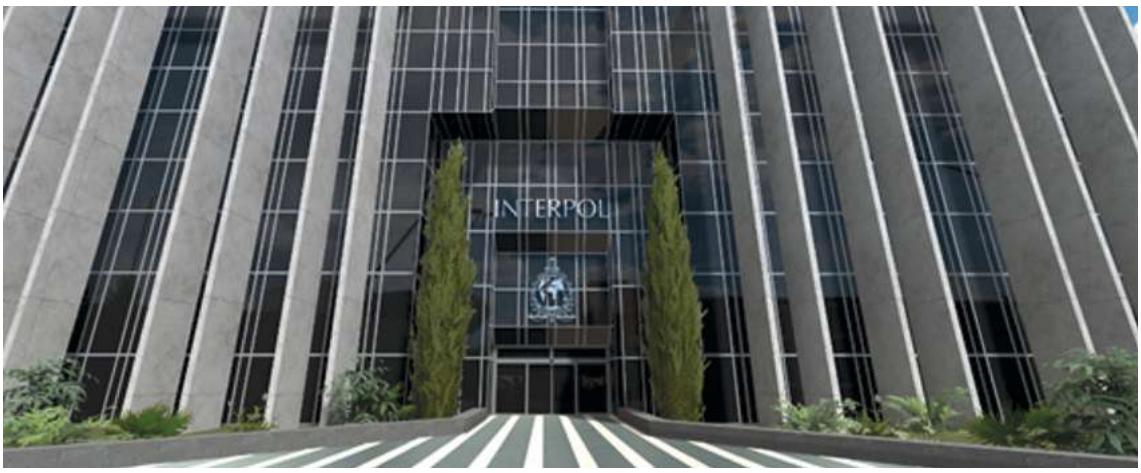
The Metaverse can revolutionize the way law enforcement officers are trained by providing immersive and interactive environments. This medium can facilitate repetitive practice without the associated real-world costs or risks. For instance, virtual reality can be used to replicate high-stress situations such as terrorist attacks, enabling officers to hone their skills in crisis management, negotiation, and use of force.

Virtual meetings

The Metaverse enables virtual meetings that bridge physical and virtual spaces, empowering communication, connection, networking, and information sharing. With the use of avatars, it offers real-time interactions and networking from anywhere globally. Unlike traditional virtual meetings, this immersive experience also allows on-the-side conversations and networking, which contribute majorly towards enhancing communication, collaboration, and productivity.

Operational coordination and support in frontline policing

Frontline policing could greatly benefit from the Metaverse as it will potentially, besides revolutionizing training and skills development, also facilitate real-time collaboration within the Metaverse, enabling police officers to coordinate and respond more effectively to different situations during operations. Recreating crime scenes, information sharing and planning of tactics will boost situational awareness and consequently impact frontline policing competences positively.



Source: INTERPOL Metaverse

Crime scene preservation and analysis

Law enforcement agencies can leverage the Metaverse to create virtual replicas of crime scenes, which can be accessed and analyzed long after the physical sites have been altered. This application not only aids in the preservation of the scene as it was found, but also allows for extensive cross-examination of the evidence, leading to better-prepared personnel in the field. Additionally, juries could virtually visit crime scenes to better understand the context and details of the case, potentially leading to more informed deliberation.

Source: The Times of India

Security of critical infrastructure

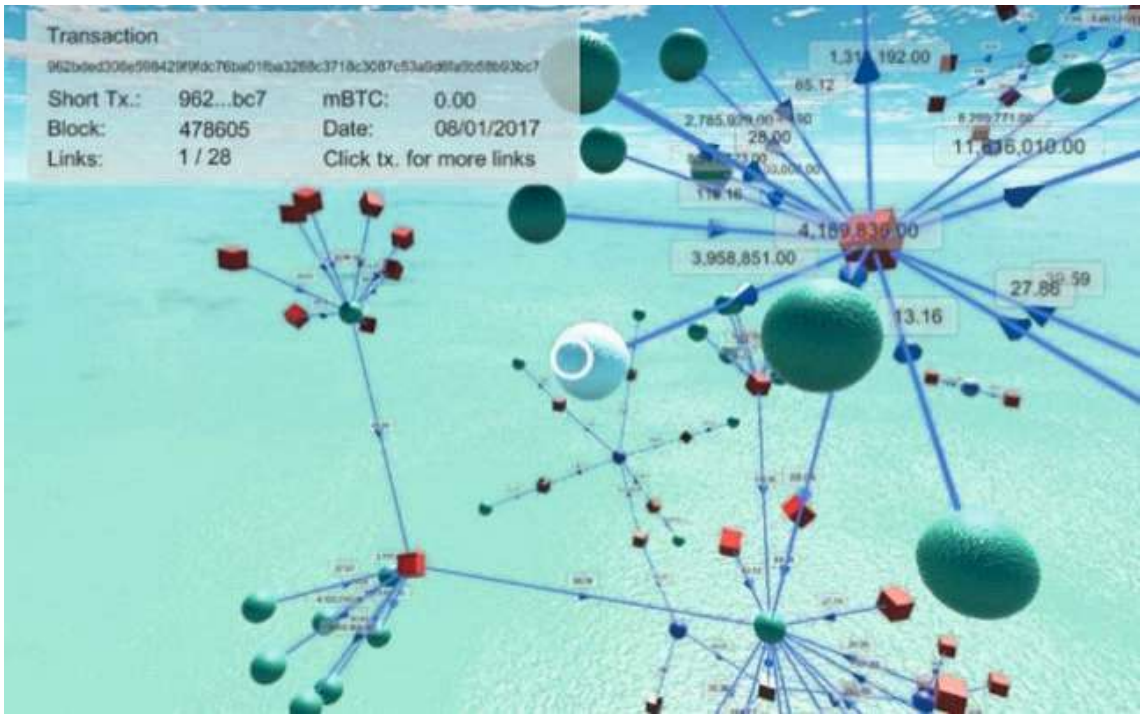
Contingency planning using the Metaverse can help ensure public safety and security, protect critical infrastructure, and facilitate disaster response. It can be used as a platform for simulating large-scale emergency situations, from natural disasters to chemical spills, and conducting rehearsals for responding to terrorist attacks, thereby enabling law enforcement agencies to engage in comprehensive major incident response exercises. Police team rehearsals and simulations can aid in the development of coordinated response plans, allowing multiple agencies to train together and develop interoperability, which is crucial during actual major incident response.

Virtual public services and reporting

Police departments can establish a virtual presence in the Metaverse, offering services such as reporting crimes, filing complaints, or even hosting virtual community meetings. This virtual approach can make police services more accessible, particularly for those who may have mobility issues or for communities located in remote areas. This will also facilitate outreach to sections of society, which are more comfortable in using virtual spaces, especially on the issues requiring awareness generation and advisories for protection of users and their properties. In addition, creation of community spaces in the Metaverse for open communication between law enforcement and the public will foster better interactions and trust.

Next level capabilities

Metaverse technologies are transforming the landscape of law enforcement by introducing innovative Augmented Reality (AR), Virtual Reality (VR) and Extended Reality (XR) tools. These cutting-edge virtual reality solutions leverage spatial perception (#Spacial_Computing) and cognition to establish an immersive workspace for the law enforcement. Through its 3D user interface, these tools tap into our natural spatial reasoning and memory capabilities, offering investigators a unique method for addressing intricate knowledge challenges. This revolutionary approach is poised to reshape how law enforcement agencies navigate complex cases, delivering a fresh perspective and heightened clarity to investigations. In the realm of criminal investigations, XR tools emerge as a game-changing resource.



Source: Bitcoin.com

4 Treeview, "Spatial Computing: A Complete Guide", 2023, https://treeview.studio/blog/spatial-computing-complete-guide/

CASE STUDY

Simulated threats

Recently, in one of the INTERPOL member countries, joint live-simulation police exercises were held focusing on areas such as command and control, crisis response, threat assessment and tactical operations. During the exercise, participants faced simulated threats from an extremist environmental group and worked together to mitigate the threat. The exercise enhanced the operational capabilities to respond to a threat scenario and also allowed the sharing of best practices and experiences in investigation and tactical response. The overall outcomes or benefits of training in the Metaverse include:

- Rapid onboarding and deployment of technology;
- The possibility for maturing technology with flexibility to reproduce any police training scenario;
- Ability to reproduce stress management/ de-escalation training and other dangerous scenarios in a safe and controlled environment (crowd control, firefighting, etc.);
- Ability to train in sensitive locations and to re-use the environments to script various training scenarios in the same location;
- Access to performance data analytics and reports that are visualized on a dashboard to give an insight on the effectiveness of the training;
- The possibility for continuous learning that can be facilitated to refresh and re-train users on scenarios;
- Personnel can be trained remotely from their workplace during working hours or from the comfort of their homes increasing time efficiency;
- Faster learning and better retention of information.

Command and Control using the Metaverse and real-time data from Drones

Drone technology combined with VR headsets can enable police officers to make better decisions in dangerous and urgent situations. By displaying real-time data directly from the drone's flight to the commander's VR sets, operational efficiency can be greatly improved. This technology enables law enforcement officers to see all the relevant information that they needed to identify a specific target task. The data gathered through drones can be reflected as three-dimensional spatial information in the Metaverse, creating a highly detailed and accurate digital landscape. In a nutshell, integrating the Metaverse and drone technology could enable:

- more accurate real-time physical-virtual synchronization;
- situational awareness and rapid response;
- more customized digital drone pilots;
- improved high-resolution images and 3D maps;
- a holistic view of an area with real-time data analysis;
- simulation and training for security personnel;
- collaboration and communication between law enforcement agencies and other stakeholders.

Source: Anarky Labs

Advantages of using the Metaverse for law enforcement

Immersive learning and retention:

Virtual reality in the Metaverse can lead to better retention of training due to its immersive nature, which can engage multiple senses and replicate the stress and unpredictability of real-life situations.

Scalability and adaptability:

The Metaverse can support a virtually unlimited number of participants, allowing agencies to scale their training exercises up or down based on need and availability. It is also highly adaptable, with scenarios and environments being created or modified relatively easily.

Resource efficiency:

Virtual training and investigations can lead to substantial cost savings, as they reduce the need for physical assets and allow for the reuse of virtual environments without incurring additional expenses.

Global collaboration:

The Metaverse allows for global collaboration among law enforcement agencies, breaking down geographical barriers and enabling the sharing of knowledge and best practices on a scale that was previously impossible.

Challenges

Technological and infrastructural requirements:

To effectively leverage the Metaverse, substantial investment in technology and infrastructure is necessary, which includes advanced VR equipment, robust network capabilities, and training for personnel.

Data privacy and ethical concerns:

Protecting personal information and ensuring ethical use of data in the Metaverse is a significant concern, particularly when virtual environments intersect with real-world personal data.

Legal and jurisdictional ambiguity:

The legal framework for actions taken in virtual environments is still unclear. This ambiguity extends to jurisdictional questions.

Cybersecurity threats:

The increased reliance on virtual systems may expose law enforcement agencies to new cybersecurity threats, including data breaches and virtual impersonation.

Future possibilities

Integration with Artificial Intelligence:
The future of the Metaverse in law enforcement includes integrating AI to create more dynamic and responsive training scenarios, and possibly to aid in predictive policing within the virtual realm.

Expanded virtual operations:

Law enforcement operations could expand the scope of their operations within the Metaverse, potentially bringing more diverse use cases.

CHAPTER II
METACRIME

With its increasing use and the number of participants, there is a need to define what constitutes crimes and harms in the Metaverse. Defining crimes and criminalizing harmful actions are essential for ensuring the safety and security of the Metaverse, as effective policing and law enforcement responses depend on clear legislation. A few reports were published in the past year attempting to list the existing and potential criminal activities in the Metaverse. The list included crimes such as NFT frauds, cyber-physical attacks, impersonation by theft of digital identities, theft of 3D properties and virtual assets, grooming of children, stalking and virtual sexual harassment[5].

Adding to these industry perspectives, INTERPOL confirmed that some law enforcement agencies in the member countries have already received reports of crimes featuring the Metaverse, particularly related to financial crime. With its growing popularity, the list of crimes will only expand and challenge the police services to address these emerging criminal activities. Indeed, the Metaverse has opened up opportunities for criminals to commit new types of crime, which can be referred to as "Metacrime". Metacrime is a growing concern and could become a major issue as the immersive world becomes part of our daily life. In this context, it is essential for law enforcement to anticipate the challenges that may arise by listing various potential threats and identifying the gap areas including those in the legal frameworks to criminalize them.

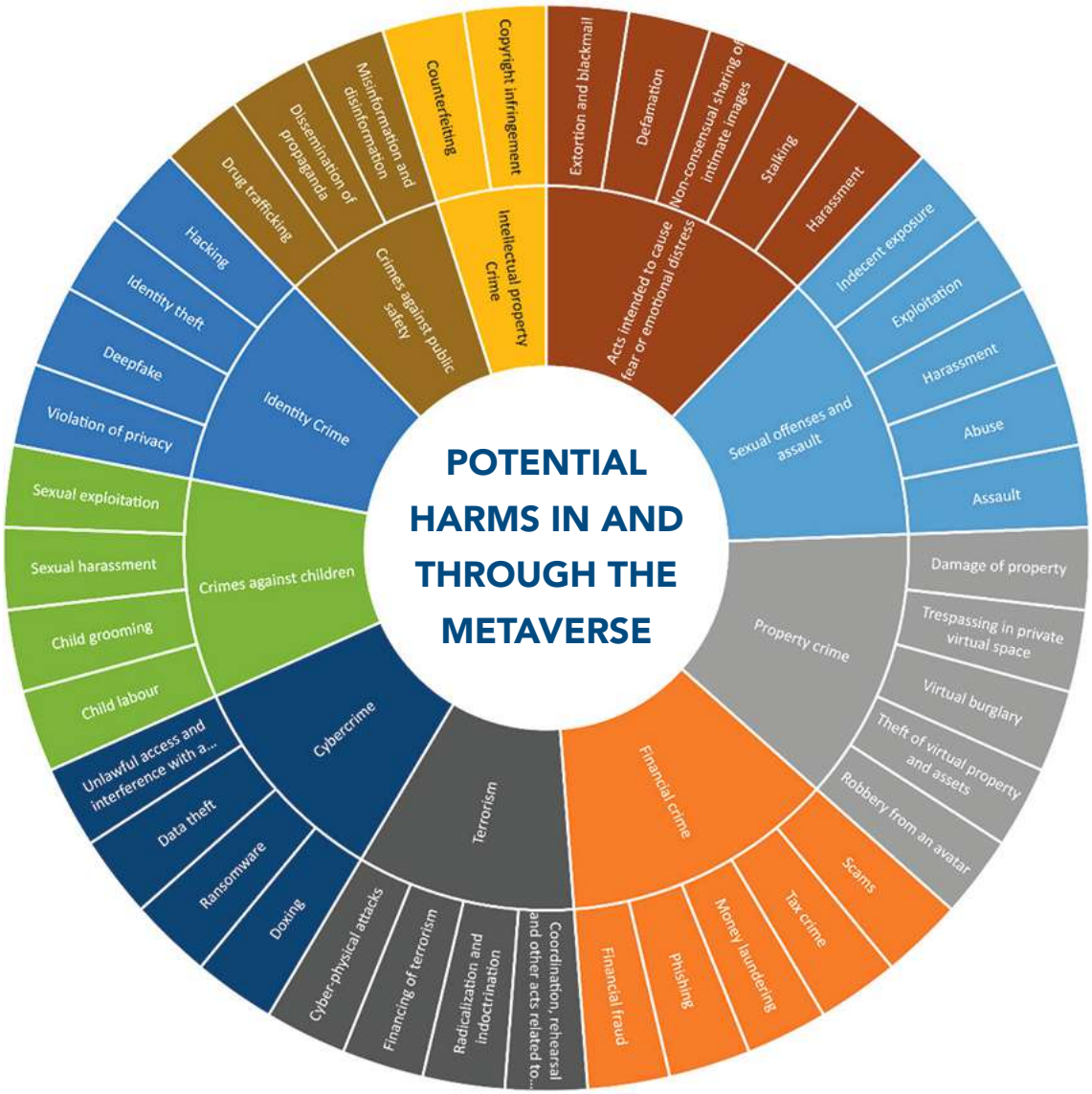
Source: The Sun

5 Trend Micro, "Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences", 2022, https://documents.trendmicro.com/assets/white_papers/wp-metaverse-or-metaworse-cybersecurity-threats-against-the-internet-of-experiences.pdf

Typology of crimes in the Metaverse

In order to update and harmonize existing crime and harm taxonomies, the following diagram illustrates a typology of some of the emerging crimes and potential harms in the Metaverse. Some of these Metacrimes can extend to the real world. The World Economic Forum stressed that the harms in the Metaverse can be local or culture-specific just like in the physical world. At the same time, the Metaverse will add spatial harms such as gestures, postures, digital assets, which will require a dedicated approach.[5]

Crimes in the Metaverse



6 World Economic Forum, "Metaverse Privacy and Safety", 2023, https://www3.weforum.org/docs/WEF_Metaverse_Privacy_and_Safety_2023.pdf

Crime scenarios

In order to gain more insights into the Metacrime, the table below presents specific modus operandi scenarios for these crimes. It is important to recognize that the Metaverse is a complex environment and that these scenarios can evolve rapidly. There exist also numerous other ways in which criminal actors can engage in various forms of crimes within the Metaverse, including existing, emerging and entirely new types.

Type of crime		Scenarios
Identity crime	Hacking	Through hacking or identity theft, criminals can get unauthorized access to user's account and digital assets. They can also steal, reproduce and sell other's identity, including digital fingerprints. Once stolen, fake avatars could be used in committing crimes. In addition, there exist risks associated with token-gating including fraudulent token issuance, theft of token and exploitation of token-gating system for fraud.
	Identity theft	
	Deepfake	Criminals may use deepfake technology to impersonate other users to commit various illicit activities. They could undermine the integrity of information and graphic materials by spreading false data about organizations and individuals, as well as disseminating propaganda and fake news. Threat actors might also generate deepfake sexual exploitation material and spread for defamation.
	Violation of privacy	Criminals may invade user's online privacy by tracking their movement, activities, interests and personal information. These could be used in cyberbullying or harassment.
Financial crime	Financial fraud	Various financial fraud can be committed through hacking, social engineering, virtual identity theft, etc.
	Phishing	Criminals may steal other user's login credentials, personal information or virtual assets through phishing. Vishing and smishing can also occur through unauthorized collection of personal data such as voices and phone numbers.
	Money laundering	Criminals may buy digital assets such as NFTs or virtual currencies with proceeds of crime and sell them for clean assets, restricting the capacity to trace the money's origin source.
	Tax crime	Criminals may establish unclear ownership structures on digital assets to obscure their illegal activities and evade financial trace and taxes.
	Scams	Criminals can trick and inflate the prices of digital assets or create fake virtual marketplaces and defraud other users by selling non-existent products. They may also introduce malware into the Metaverse to steal virtual assets. Some examples include impersonation scam, investment scam, romance scam, tech support scam, fake Metaverse scam, NFT scam, giveaway scam, payment scam, job scam, smart contract scams, etc.

Property crime	**Robbery from an avatar**	Criminals may steal virtual assets or virtual properties anonymously for monetary gain, resulting in significant real-world financial losses. They can also steal cultural properties to replicate, resell or devaluate them.
	Theft of virtual property and assets	
	Virtual burglary	Intrusions into personal space in the Metaverse can lead to cyberstalking, harassment, or even identity theft. Criminals may steal virtual assets linked to in-game transaction or disrupt business operations for monetary profit.
	Trespassing in private virtual space	
	Damage of property	Criminals may disrupt virtual events, target specific users to extort or cause chaos by damaging virtual properties and virtual vandalism. Criminals can also damage cultural assets such as art pieces for personal, political, or ideological motivations.
Intellectual property crime	**Copyright infringement**	Criminals may copy or sell copyrighted NFT work committing pattern and trademark infringement in the virtual marketplace. The copyright of images, videos, written productions and counterfeiting items can be a technique for money laundering and also lead to the disruption of virtual economy.
	Counterfeiting	
Sexual offenses and assault	**Assault**	Criminals may engage in virtual interactions with other users to commit assault or non-consensual and illicit offenses of sexual nature towards their avatars. This can range from instances of harassment to the creation and distribution of explicit sexual content.
	Abuse	
	Harassment	
	Exploitation	
	Indecent exposure	
Crimes against children	**Sexual exploitation**	Criminals may manipulate, threaten,[7] and coerce children into creating explicit sexual content of themselves. The criminal's avatar could also commit sexual harassment and abuse and engage in predatory behavior towards minors, potentially creating an impact on their physical bodies with the use of haptic devices.[8]
	Sexual harassment	
	Child grooming	
	Child labour	Children can be exploited by malicious actors to create games and virtual experiences to generate money. These malicious actors can put pressure on children to work more for more financial gain, which might not be given to them at the end. This can lead to abuse and child labour.
Cybercrime	**Unlawful access and interference with a computer system or data**	Criminals may hack into Metaverse platforms to steal data, threat users, demand virtual assets, manipulate information, or sell third party assets.
	Data theft	
	Ransomware	
	Doxing	

7 The Wall Street Journal, "The social-media company has stepped up enforcement, but its algorithms continue to promote problematic content", 2023, https://www.wsj.com/tech/meta-facebook-instagram-pedophiles-enforcement-struggles-dceb3548?mod=tech_lead_pos1

8 Gomez, et al., *A scoping study of crime facilitated by the metaverse*, 2023, https://osf.io/preprints/socarxiv/x9vbn/

Acts intended to cause fear or emotional distress	**Harassment**	Criminals may threaten users to reveal sensitive information and conduct online bullying. Emerging technologies like haptic feedback could enable new forms of abuse, raising concerns about the physical and psychological safety of users.[9]
	Stalking	Criminals may stalk and closely follow other user's virtual presence, activities, interests and personal information, invading the person's privacy and personal space.
	Non-consensual sharing of intimate images	Criminals may share and spread intimate materials without consent or fake images of an individual's body.
	Defamation	A defamatory statement made against an avatar could impact the individual's identity and reputation in the real world.
	Extortion and blackmail	Criminals may collect specific personal information of users and use it to extort and blackmail. Criminals can also impersonate authoritative figures or governments/law enforcement.
Terrorism	**Cyber-physical attacks**	Using digital twin technology, threat actors can gain unlawful access and control of critical infrastructure's systems for cyber-physical attacks.
	Financing of terrorism	Terrorists could misuse the Metaverse to receive financial support for terrorist purposes,[10] which could lead to the commission of terrorist attacks, the proliferation of weapons or the strengthening of organized crime groups and terrorist networks.
	Radicalization and indoctrination	Terrorists may exploit the Metaverse for online recruitment, radicalization, training and indoctrination of individuals. They could also raise funds anonymously and easily spread disinformation and propaganda reaching a global audience in a short period of time.
	Coordination, rehearsal and other acts related to the activities of a terrorist group	Users engaging in cyberterrorism may lead to real world attacks with improved coordination and execution using digital twin.
Crimes against public safety	**Misinformation and disinformation**	Misinformation and disinformation can be easily spread in the Metaverse, potentially manipulating the public opinion and causing users to take misleading and uninformed decisions with consequences that can range from financial losses to social problems and ideological divisions.
	Dissemination of propaganda	
	Drug trafficking	Malicious actors may sell drugs and narcotics through the Metaverse, reaching a broader spectrum of customers with anonymity. Drug trafficking may lead to addiction issues and harmfully impact communities and public safety.

9 Tseng, et al., *The Dark Side of Perceptual Manipulations in Virtual Reality*. 2022, https://www.researchgate.net/publication/360331738_The_Dark_Side_of_Perceptual_Manipulations_in_Virtual_Reality
10 Financial Action Task Force, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, 2020, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html and *Terrorist Financing Risk Assessment Guidance*, 2019, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Terrorist-financing-risk-assessment-guidance.html

CHAPTER III
METAVERSE FORENSICS AND INVESTIGATION

With its increasing use, the Metaverse will emerge as a very important source of data and evidence for investigators. Therefore, law enforcement should be prepared to:

(1) access data from VR headsets and haptic devices;

(2) recover evidence from the Metaverse infrastructure;

(3) acquire data from the third party Metaverse service providers; and

(4) train first responders, forensic specialists, and the entire criminal justice system.

Technology and devices

The integration or manifestation of the Metaverse into the physical world can be achieved in various ways, primarily through technologies like Augmented Reality (AR) and the Internet of Things (IoT). Information or virtual objects could be overlaid on our physical surroundings. For example, AR glasses or lenses could provide navigational directions, information about physical objects, or enable virtual interactions with real-world locations. People might interact physically with the Metaverse via AR, for example, by using hand gestures to manipulate virtual objects or employing spatial audio and haptic feedback to experience virtual events in a tactile manner.

IoT devices, embedded in physical spaces, could be synchronized with virtual spaces in the Metaverse, ensuring real-time data flow between both worlds and potentially enabling control of physical environments via virtual interactions. Wearables might transmit real-time biometric data into the Metaverse, affecting the avatar's appearance, behavior, or capabilities based on the user's physical state. Wearables could also provide haptic feedback to mimic physical sensations experienced by the avatar in the Metaverse, providing a tangible link between virtual and physical experiences. Designs or objects created within the Metaverse could be brought into the physical world through 3D printing technologies.

Investigating crimes in the Metaverse, using conventional forensic capture methods, poses several challenges for law enforcement agencies due to emerging technologies being adopted in Metaverse such as the adoption of distributed ledgers, blockchain technology, cryptocurrency and decentralization.

Endpoint forensics

In most criminal investigations and digital forensics examinations, the examination of a device that was involved in the crime, either to facilitate the crime or the victim of the crime, needs to be validated and verified once the crime has been reported. A majority of modern criminal investigations have a digital element to them due to the use of technology such as smartphones, other smart devices and the internet in everyday life. Digital forensics is a powerful tool that can be used to aid investigations across a wide range of fields. By providing accurate and reliable evidence, digital forensics can help investigators to identify and prosecute perpetrators, recover stolen or lost data, and deter future crimes. Digital forensics follows the following steps including **collection of data, recovery of deleted or hidden data, analysis of data, reconstruction of events, Identification of the attacker, and remediation and prevention.**

Since most data will be stored on the platforms, endpoint forensics is limited in the Metaverse. Endpoint forensics can be useful in investigating incidents that occur within a single device or system, but it has several limitations when it comes to investigating incidents that occur in the Metaverse. Endpoint devices that may be useful for investigators and digital forensic examiners when investigating a Metacrime could include:

- VR Headsets and other wearables
- Computer/Laptop
- Mobile Phone
- Routers
- Smart Devices

Challenges of endpoint forensics

- **Lack of standardization:** The Metaverse is a complex and rapidly evolving digital environment that lacks standardized protocols and structures. This makes it difficult to conduct endpoint forensics in a consistent and reliable manner, as different Metaverse platforms may have different logging and data collection mechanisms.
- **Distributed nature:** Incidents in the Metaverse often involve multiple devices and systems, which are distributed across a wide range of networks and platforms. Endpoint forensics may not be sufficient to investigate such incidents, as it focuses on a single endpoint device and may not provide a complete picture of the incident. Data may be stored temporarily on the device and ultimately transferred to a centralized cloud server for long-term safekeeping.
- **Difficulties in extracting data:** Investigations in the Metaverse may involve collecting and analyzing large amounts of personal data, which can raise concerns about privacy and data protection. Endpoint forensics may not be able to provide a complete picture of the incident while respecting the privacy and data protection rights of individuals involved in the investigation. In this context, it may be necessary to acquire appropriate privileges in order to retrieve additional information from the VR headset for investigation.
- **Lack of physical evidence:** In the Metaverse, incidents often involve virtual assets and digital interactions, which may not leave physical evidence that can be collected and analyzed using endpoint forensics. This makes it difficult to determine the sequence of events that led to the incident and to identify the parties involved.
- **Technical challenges:** The Metaverse is a technically complex environment, and investigations may require specialized knowledge and tools that are not readily available to most investigators.
- **Anti-forensic Metaverse:** Utilizing platforms designed for temporary data storage and dynamic environments could make evidence vanish quickly or appear altered.
- **Multi-Jurisdictional aspects:** Due to decentralization and cloud servers being located in different jurisdictions, laws where the server is applicable may affect investigations involving the Metaverse and the collection and use of forensic evidence obtained. Different legal systems, legislation and understanding of person involved all have an impact on the successful investigation and prosecution of crimes committed in the Metaverse.

In summary, endpoint forensics has several limitations when it comes to investigating Metacrimes, due to the lack of standardization, distributed nature, privacy and data protection concerns, lack of physical evidence, and technical challenges involved. As such, investigators may need to use a combination of techniques, including network forensics, social engineering, and specialized tools and techniques, to effectively investigate incidents in the Metaverse.

Server investigations and forensics

Server forensics is the process of investigating a server to determine whether it has been compromised, or to determine the cause of a Metacrime, or to recover specific evidence around a particular user or interaction. The primary goal of server forensics is to collect and analyze digital evidence to identify the root cause of the incident and to help prevent future incidents or to acquire specific data around a user or identify associates of a particular individual.

During server forensics, investigators typically follow a structured process that includes identifying and preserving digital evidence, analyzing the evidence to determine what happened, and presenting their findings in a clear and concise manner. Server forensics can be used to investigate a wide range of incidents, including unauthorized access, data breaches, malware infections, and system failures.

Overall, server forensics is a critical tool for investigating security incidents and helping organizations protect their digital assets. Most, if not all, of this server evidence will need to be subpoenaed from a third-party company as part of litigation or a law enforcement action. These third-party servers are in the cloud, secured in massive data centers by the Metaverse host, where forensic examiners are not typically permitted to enter. Consideration should be given to:

- SSD technology to recover deleted data from hosted servers, data centers and cloud.
- Seizure of electronic assets and hard copy assets (mobile devices, electronic ledgers such as Nano Ledger, e-Wallets, seed phrases, mobile device interrogation, backups, encrypted backups, security mechanisms such as MFA/2FA/Email Verification).

- The approach taken by law enforcement to interview suspects and taking witness statements. Whilst the Metaverse is still developing, care must be taken to adopt the existing robust techniques by digital investigators to support specialist digital and forensic crime units to ensure defensibility.

Metaverse platforms

Digital platform forensics is a branch of digital forensics that involves the investigation of digital platforms such as social media sites, messaging apps, and cloud-based services. The goal of digital platform forensics is to collect and analyze digital evidence to determine the cause of a Metacrime, identify the parties involved, and provide evidence that can be used in legal proceedings.

One of the challenges of digital platform forensics is that digital platforms are constantly evolving, with new features and functionalities being added on a regular basis. This means that investigators need to stay up to date on the latest tools and techniques in order to effectively investigate incidents on these platforms.

Overall, digital platform forensics is a critical tool for investigating Metacrime incidents on digital platforms and can help organizations and law enforcement agencies identify perpetrators, collect evidence, and prosecute cybercriminals.

As an example, some social media platforms allow users to download their profile, interactions, friends list, chat messages, photos, videos, and other data types, which can be used by law enforcement if a standard operating procedure has been established for this purpose. This approach reduces inconvenience to users as well as limits the amount of information that law enforcement requests from service providers and platforms.

Blockchain forensics

Blockchain forensics is a branch of digital forensics that focuses on the investigation of blockchain-based transactions and activities. Blockchain is a decentralized ledger technology that provides a tamper-evident record of all transactions and activities that occur on the network. As such, blockchain forensics involves the collection and analysis of digital evidence from blockchain networks to investigate fraudulent or criminal activities.

Some of the key applications of blockchain forensics include the investigation of Metacrimes where cryptocurrency is involved such as money laundering, fraud, and extortion. Investigators may use a variety of techniques to collect and analyze digital evidence from blockchain networks, including analyzing transaction records, examining wallet addresses, and tracking the flow of funds between different addresses.

One of the key challenges of blockchain forensics is the decentralized and pseudonymous nature of blockchain transactions. Unlike traditional financial transactions, blockchain transactions do not require users to provide personal information, which can make it difficult to identify the parties involved in a transaction. In addition, blockchain networks are designed to be transparent, which means that anyone can view the contents of the blockchain ledger, but this also makes it difficult to maintain the confidentiality of sensitive information.

Overall, blockchain forensics is a rapidly growing field that is becoming increasingly important as blockchain technology continues to gain mainstream adoption. By providing the tools and techniques necessary to investigate and prosecute blockchain-related crimes, blockchain forensics can help to protect the integrity of blockchain networks and prevent abuse of the technology.

Cryptocurrency analytics

Cryptocurrency analytics is a field that involves the investigation and analysis of cryptocurrency transactions[11] to identify individuals involved in illicit activities such as money laundering, fraud, and extortion. Cryptocurrencies are digital or virtual currencies that use encryption techniques to regulate the generation of units of currency and verify the transfer of funds.

The investigation of cryptocurrency transactions requires a deep understanding of the underlying blockchain technology and the various cryptocurrency protocols. Investigators use specialized tools and techniques to analyze blockchain transaction records, wallet addresses, and other digital artifacts in order to identify patterns and anomalies that may indicate illicit activity.

Some common applications of cryptocurrency analytics include the investigation of ransomware attacks, dark web marketplaces, and other forms of cybercrime that involve the use of cryptocurrencies. Cryptocurrency forensics can also be used to investigate

11 Basel Institute on Governance, *Quick Guide 1: Cryptocurrencies and money laundering investigations*, 2023, https://baselgovernance.org/publications/quick-guide-1-cryptocurrencies-and-money-laundering-investigations

cases of fraud or embezzlement in which cryptocurrencies have been used to transfer funds.

One of the key challenges of cryptocurrency analytics is the anonymous nature of cryptocurrency transactions. Cryptocurrencies such as Bitcoin and Ethereum are designed to be pseudonymous, which means that users can create wallet addresses without providing identifying information. This can make it difficult to identify the parties involved in a transaction, although investigators can use various techniques to link wallet addresses to specific individuals.

As the use of cryptocurrency becomes mainstream and more accessible, the current methodology for cryptocurrency investigation may have to adapt to the innovative landscape that cryptocurrency technology attracts.

Non-Fungible Tokens (NFT) Forensics

NFT forensics is a branch of digital forensics that deals with the investigation and analysis of non-fungible tokens (NFTs). NFTs are unique digital assets that are stored on a blockchain and are becoming increasingly popular in the art world and other creative industries. Recently, in line with its widespread adoption, a Purple Notice[12] was issued on NFT related crimes from a member country in December 2023.

Some software architects consider NFTs to be a core component of Metaverses to allow for the portability of assets between platforms. Some examples of portable NFT assets might include:

- **Virtual real estate:** In virtual worlds or Metaverses, NFTs can represent ownership of virtual land. These virtual plots can be bought, sold, and developed just like physical real estate.
- **Digital art and collectibles:** NFTs have already made a huge impact in the digital art world by allowing artists to monetize their work in new ways. In the Metaverse, these pieces of art could be displayed in virtual galleries or homes.
- **Virtual goods:** NFTs can represent virtual goods like clothing, furniture, vehicles, etc. Users can buy these items to use within the Metaverse.
- **Identity and reputation:** NFTs could potentially be used to create a unique digital identity. This could include proof of accomplishments, skills, or experiences that can be showcased in the Metaverse.
- **Experiences and access:** NFTs can be used as tickets to virtual concerts, lectures, meet-ups, or other experiences in the Metaverse. They could also grant access to exclusive areas or clubs within the Metaverse.
- **Gaming assets:** In video games within the Metaverse, NFTs can represent in-game assets. This could include anything from weapons and armor to characters and pets.
- **Intellectual Property:** NFTs can also be used to manage and transfer intellectual property rights within the Metaverse, such as the rights to a piece of music, a movie, or a brand.

NFT forensics involves the collection and analysis of digital evidence related to NFT transactions and activities. This may include analyzing blockchain transaction records, examining the metadata of NFTs, and tracking the flow of NFTs between different addresses.

One of the key applications of NFT forensics is to investigate cases of NFT fraud, such as the creation and sale of counterfeit NFTs. Investigators may also use NFT forensics to investigate cases of copyright infringement and intellectual property theft involving NFTs.

One of the challenges of NFT forensics is the complex and decentralized nature of blockchain networks, which can make it hard to identify the parties involved in an NFT transaction. Additionally, it is difficult to identify the original creator of an NFT or to determine the authenticity of an NFT as it often contains a wide range of digital content, including images, videos, and other multimedia files.

NFT forensics is a rapidly growing field that is becoming increasingly important as the use of NFTs continues to grow. NFT forensics can help protect the integrity of NFT marketplaces and stop people from abusing the technology by giving police the tools and knowledge they need to investigate and prosecute crimes involving NFTs.

12 INTERPOL Purple Notice: To seek or provide information on modus operandi, objects, devices and concealment methods used by criminals.

Metaverse service and platform providers

As law enforcement, requesting data from service and platform providers is a common practice to aid investigations. To request data from service and platform providers, law enforcement agencies typically need to submit a legal request, such as a subpoena, warrant, production order or court order, to the provider. The specific process and requirements for making such requests may vary depending on the jurisdiction and the type of information being requested.

It is important for law enforcement agencies to follow the proper legal procedures when requesting data from service and platform providers to avoid any legal challenges or other issues. In addition, it is important to balance the need for access to information with the rights of individuals to privacy and due process.

One of the major challenges law enforcement faces in requesting data from Metaverse providers is understanding what data can be requested, as most of the time they are not aware of what data is stored by the host platform, or where that storage may be.

It is important that law enforcement engage with the platform after it has been identified to ensure that the requested data can be obtained. In addition, each request will be subject to a specific process and limitations. As an example, some social media platform providers may only retain specific data for a limited amount of time. Therefore, after an account has been identified, a preservation request must be made as soon as possible to ensure that the account remains in its current state to limit the deletion of data and activity information. The Metaverse will present several challenges to law enforcement on determining two elements: **jurisdiction and attribution.** These challenges are similar to any traditional cybercrime, but the Metaverse will add another layer of complexity.

There will be numerous legal challenges that will be litigated in the coming years regarding Metaverse-related matters. Ensuring that the Law Enforcement and Legal communities are aware of the technology and have the expertise in-house will be essential.

Large Language Models and other Generative AI technologies

Building the Metaverse with generative AI technologies and large language models presents an enticing vision of vast virtual environments, dynamic narratives, and diverse non-player characters (NPCs). However, it's crucial to be aware of potential criminal risks and the unpredictable nature of these AI technologies, often regarded as "black boxes."

- **World generation:** AI could generate diverse virtual environments, ranging from entire cities to individual pieces of furniture. However, there's a risk that AI might create environments conducive to illicit activities. If not properly managed, these environments might inadvertently facilitate or encourage criminal behavior, from virtual theft to more serious crimes.
- **Non-Player Characters (NPCs):** While AI like GPT-3 can generate unique personalities and behaviors for NPCs, there's a risk that these characters might be manipulated for criminal purposes. NPCs could be exploited to perform harmful actions, distribute illicit materials, or deceive other users.
- **Dynamic storylines:** AI could create personalized storylines based on user interactions. But, this could potentially be used to target individuals with harmful content, or to manipulate users into revealing personal information or engaging in illegal activities.
- **Content moderation:** AI can help monitor and moderate content, but it's not infallible. Malicious users could find ways around these systems to propagate harmful content or engage in criminal behavior.

The "black box" nature of many AI models exacerbates these risks. While we can observe the inputs and outputs of these models, their internal workings are opaque and complex. This can result in unexpected and potentially harmful outcomes. For example, an AI might generate an environment or NPC behavior that facilitates criminal activity, without human designers realizing it.

Furthermore, AI models can reflect and propagate biases present in their training data. If not carefully curated, this data could include harmful or illegal content, leading the AI to generate similar content within the Metaverse.

The "black box" nature of Large Language Models (LLMs) and AI technologies could pose challenges for criminal investigations in several ways:

- **Traceability:** Since the decision-making processes of AI models are not easily interpretable, tracing the origins of a particular output or action could be challenging. This might make it difficult to determine whether an illicit act in the Metaverse was facilitated or performed by an AI, or by a human exploiting the AI.
- **Predictability:** The unpredictability of AI behaviors means that illegal activities might not be anticipated and prevented in advance. For example, if an AI generates an environment that unintentionally facilitates criminal activity, this might only become apparent after the fact.
- **Liability:** If a crime is committed with the assistance of an AI (for example, if an NPC is manipulated to carry out harmful actions), it may be difficult to establish who is legally responsible. The key question is who is responsible or accountable in the context of AI in the Metaverse (i.e. designers of the AI, the operators of the Metaverse, the individual user who manipulated the AI, or some combination of these).
- **Data privacy:** Investigations often rely on the collection and analysis of data. However, AI technologies might generate or process data in ways that infringe on privacy rights. For instance, if an AI is used to monitor user behavior in the Metaverse to prevent crime, this could lead to concerns about surveillance and data misuse.
- **Bias and discrimination:** If AI technologies reflect and propagate biases present in their training data, this could impact criminal investigations. For example, certain users or activities might be unfairly targeted or overlooked due to biased AI behavior.
- **International and jurisdictional issues:** Given the global nature of the Metaverse, crimes committed within it may involve participants from multiple countries. This could complicate criminal investigations, especially if AI technologies are involved, due to differences in international laws and regulations regarding AI and cybercrime.

As the integration into applications, platforms and devices that are used to access the Metaverse the investigator and forensic examiner will need to keep updated on the use of LLM and AI within the Metaverse and associated platforms and applications. They would need to have an understanding of how LLM and AI functions to ensure that they can interpret the use of these technologies within a crime or investigation.

Training of 1st Responders, Digital Forensics Specialists and Judicial System

It is essential that first responders, digital forensics specialists, and the judicial system understand the Metaverse, virtual environments and associated technology to ensure the safety and security of virtual environments, as well as to protect the rights of individuals who use them. In order to investigate and analyze digital evidence pertaining to virtual environments, law enforcement officers need to be trained in digital forensics. To support virtual environments, specialized training may be required in virtual and augmented reality technologies, as well as the underlying blockchain and other distributed ledger technologies.

It is also necessary for the judicial system to be trained on how to evaluate and adjudicate cases involving virtual environments. It may be necessary to develop new legal frameworks and standards for virtual environments, as well as to train judges, attorneys, and other legal professionals in the challenges and issues that arise in virtual environments.

CHAPTER IV
METAVERSE GOVERNANCE

The emergence of the Metaverse can present a wide range of governance and policy issues given its potential significant impact on our societies. Understanding these issues and reflecting the necessary changes in the regulatory framework would be crucial for this emerging technology to thrive. As each policy option may have a different impact on various stakeholders, a multi-stakeholder approach is required to identify necessary changes in the regulatory framework. Providing a basis for this important discussion, a few key policy issues are outlined in this section, especially that are relevant to law enforcement. It is also important to note that there are various models of the Metaverse based on how it is governed. This section discusses the present and future aspects of the Metaverse considering both centralized and decentralized models.

Key governance issues

Identity construct in the Metaverse

- In many criminal activities in the Metaverse, avatars can provide anonymity that can be exploited by criminals. They can be used as proxies for real-world individuals and use virtual currencies to purchase stolen goods. Threat actors can also use avatars to create fake identities and lure people into engaging in illegal activities.
- When creating an account and avatars in the Metaverse, the requirements and processes of identity validation can vary. Some Metaverse platforms might require only a crypto wallet, while others might request for email addresses or national identity number. With lower level of standards or requirements in place for verifying the identities, law enforcement can face challenges in tracing the individuals behind their avatars who engage in criminal activities.
- Another consideration includes distinguishing between the information that platforms collect regarding user identity (user-to-service) and the information that users share with other users about their identity (user-to-user). It is also possible that users may prefer different modes of identification depending on the contexts and use cases within the Metaverse.

What is an avatar?

The international community continues to engage in discussions aimed at defining the concept of avatar. One of the definitions developed within the ITU's Focus Group on Metaverse includes "a digital entity that can be used as a (visual) representation of the user inside the virtual environments." In addition, from INTERPOL's perspective, the legal personas of the avatar could be considered as either:

- Extension of human; or
- Symbolic representation of human; or
- Property of human; or
- Autonomous legal persona.

The way we perceive and acknowledge avatars can lead to different implications of harms and criminal activities involving them. To hold an avatar responsible for its action would mean attributing a legal persona to the avatar, recognizing avatars within a legal system and allowing them to be subject to legal actions such as suing or being sued.[13]

The legal consequences and potential outcomes of prosecution can differ depending on the definitions and legal personalities of avatars. It would also be important to develop standards and criteria for distinguishing between a legal avatar and the user controlling that avatar.[14] In this context, a continued dialogue among various stakeholders is essential to develop a common understanding and definition of avatar, and to reduce the legal gaps between member countries given the transnational nature of this medium.

13 Visa AJ Kurki, *A Theory of Legal Personhood*, 2019, Oxford University Press.
14 Cheong, B.C. *Avatars in the metaverse: potential legal issues and remedies*. Int. Cybersecur. Law Rev. 3, 467–494, 2022, https://doi.org/10.1365/s43439-022-00056-9

Data management

When using the Metaverse, there is a massive amount of data which gets generated, collected, stored and processed. This data includes biometric data, as well as data on the emotional and physiological responses of users using VR headsets. However, there is a lag between the rapid adoption and expansion of biometric and facial recognition technologies and the development of universally accepted standards and regulations for them.[15] This delay could lead to various challenges, including privacy concerns and gaps in different industries and regions. At the same time, numerous entities involved in the Metaverse also creates a complex network of relationships, leading to ambiguity in responsibilities and liabilities in terms of data management. Defining the responsibility and liability of data controller and data processor, for instance, will be important to safeguard user data and ensure compliance with the existing data and privacy related laws and regulations.

Laws and regulations

- In the Metaverse, different jurisdictional laws and regulations could be applied. To understand the differences, there is a need to assess how the current jurisdictional contractual law, property law, criminal law, tax law and other relevant laws are applicable within the Metaverse. At the same time, ensuring the application of Universal Declaration of Human Rights and other existing international laws in the Metaverse would be fundamental.
- With a better understanding of the jurisdictional context, it would be more feasible to address legislative and regulatory gaps among member countries in criminalizing acts that cause harm in or through the Metaverse, considering the transnational nature of this three-dimensional world.

Establishing threshold for intervention to address harms in the Metaverse

- Similar to the physical world, this three-dimensional world requires a threshold for response to harms committed in the Metaverse, depending on their severity. Whether it is physical, psychological or hybrid harms, it is important to understand and recognize the level of harm to effectively mitigate and address them.[16]
- In general, individuals are expected to first self-regulate, taking responsibility of their behaviors and actions. With intensifying interactions, hosting platforms are setting boundaries and implementing rules for safety and security in the Metaverse.[17] A potential legal challenge in Metaverse investigations is the quasi-judicial systems on platforms. Platforms may require individuals and agencies to present their case to a group of "international experts" that have been chosen by the platform if there is a dispute on whether data should be released or whether enforcement be conducted on the platform.
- Beyond platform intervention, there are scenarios where some actions might cause severe harm, financial loss, or have real-world consequences, which require reports to law enforcement. It is therefore important to devise this threshold-based system to address harms caused in or through the Metaverse. Along with establishing a threshold for response to harms, a robust reporting mechanism will be necessary.

International law enforcement cooperation

In the face of global threats and harms arising from the Metaverse, international law enforcement cooperation is at the core of efforts in addressing these emerging challenges. It is therefore important to reflect the perspectives of global law enforcement when building a secure-by-design (inclusive of the aspects like safety-by-design[18] and privacy-by-design) Metaverse. For instance, it would be useful to allow timely access to the relevant data for investigations of Metacrime while ensuring privacy and other fundamental rights. Harmonizing different laws and regulations would also be helpful, as often crimes in the Metaverse are committed across multiple virtual environments and multiple jurisdictions. These efforts will enable effective law enforcement response and cross-border collaboration to keep the virtual world safe and secure.[19]

15 Ericsson, ¨Privacy Standards in the Metaverse¨, 2023, https://www.ericsson.com/en/blog/2023/2/privacy-standards-in-the-metaverse
16 eSafety, "What you can report to eSafety", https://www.esafety.gov.au/report/what-you-can-report-to-esafety; "Basic Online Safety Expectations", https://www.esafety.gov.au/industry/basic-online-safety-expectations; "Industry codes and standards", https://www.esafety.gov.au/industry/codes
17 Tang and Kong, "Online safety in the dawn of immersive technologies and the metaverse", 2023, https://www.herbertsmithfreehills.com/insights/2023-08/online-safety-in-the-dawn-of-immersive-technologies-and-the-metaverse
18 eSafety, "Safety by Design", https://www.esafety.gov.au/industry/safety-by-design
19 Responsible Metaverse Alliance, "Policing in the Metaverse: Prevention, Disruption, and Enforcement Challenges", Discussion Paper, 2023, https://responsiblemetaverse.org/wp-content/uploads/2023/07/RMA-Discussion-Paper_-Policing-in-the-Metaverse-7-June-2023.pdf

Legal status and liability of avatars

Adding a layer of complexity to the issue, AI-based avatars can be used in crimes in the Metaverse with the aim to increase the sophistication, quantity, and speed of criminal activities. As mentioned in the previous section on the identity construct, an autonomous legal persona is relevant in this case. The key question would be who or which entity is controlling the AI-based avatar. This could draw lessons from a recent legal case in which a man was sentenced to two and a half years in jail for using AI to generate child sexual exploitation materials[20]. This ruling confirmed that materials involving virtual humans, realistic enough to resemble real children or minor, are illegal. Regulatory frameworks should be up-to-date and ready to be able to address these issues of liability related to crimes committed or facilitated by AI-based avatars.

Interoperability

- Interoperability is a pivotal yet complex issue that can unlock the full potential of the Metaverse. According to the World Economic Forum, it encompasses a wide range of technical, usage and jurisdictional aspects[21] to unify economics, avatars, and systems across multiple virtual worlds. Once achieved, it can provide seamless and frictionless experience, resulting in network effects[22] for mass adoption.
- To ensure an interoperable network of different three-dimensional virtual worlds, the ecosystem would need to address various issues relating to asset ownership, identity, data privacy, intellectual property, demographic inclusivity, data management and jurisdictional challenges. It is also essential for legal or regulatory interoperability to reflect the technical interoperability in the Metaverse.
- Having a unique digital identity per person across multiple Metaverses could also be considered. As all these issues have implications for the global law enforcement community, close monitoring of developments is essential to keep abreast of the progress for effective law enforcement response.

Security and safety

- The Metaverse can be vulnerable to various cyberattacks. For instance, it can be exploited for spreading harmful content including misinformation and disinformation. This can be particularly damaging due to its three-dimensional, immersive, persistent, and borderless nature, amplifying the effects of such content. This can lead to serious violations of privacy and safety that can have direct consequences in the physical world. Therefore, robust cybersecurity measures need to be implemented to address these concerns. To better protect children in the Metaverse who could be vulnerable to crimes outlined in Chapter II on Metacrime, platforms and service providers should consider implementing safeguards such as child safety locks and filters. Other safety related issues could include health issues such as VR hangover.
- In addition, it is important to establish robust and adaptable data protection measures and frameworks in order to protect user privacy effectively. As highlighted during the Metaverse Safety Week 2023[23], the privacy risks might be elevated especially in the AI-powered Metaverse given its significant data collection and processing. An agile data protection framework would be therefore crucial to protect users against potential misuse of AI-processed data in the Metaverse. This can also assist and reinforce regulatory efforts and initiatives with diverse privacy and security controls.
- Another aspect to consider is how experiences and their sources can be identified and attributed. The process of identifying sources in the Metaverse is still unclear as the methods of referring to a source of information in the current Internet or social media (e.g., URL) might not work in the Metaverse. Given that multiple instances of a particular experience are also possible, this multiplicity could pose challenges in determining which specific instance served as the source.

20 Bae, CNN, "South Korea has jailed a man for using AI to create sexual images of children in a first for country's courts", 2023, https://edition.cnn.com/2023/09/27/asia/south-korea-child-abuse-ai-sentenced-intl-hnk/index.html
21 World Economic Forum, *Interoperability in the Metaverse*, 2023, https://www3.weforum.org/docs/WEF_Interoperability_in_the_Metaverse.pdf
22 Stobierski , "What are Network Effects", Harvard Business Review, 2020, https://online.hbs.edu/blog/post/what-are-network-effects
23 XRSI, *Cybersecurity and Data Protection - Navigating the cyber frontier in the AI-powered metaverse*, The Roundtable Report, 2023, https://metaversesafetyweek.org/wp-content/uploads/2024/01/Cybersecurity-Data-Protection-MSW2023-Post-Roundtable-Report.pdf

Governance in action

Criminalization

Criminalizing malicious behaviors and illicit activities in the Metaverse requires established laws and the recognition of such acts as criminal behaviors. This entails the establishment of clear definitions, as not all future crimes in the Metaverse fit the definitions of traditional offenses. For instance, offenses involving hybrid (physical-virtual) interactions might require new or revised definitions. However, it is important to avoid unclear and broad definitions of crime, as greater ambiguity in the definition can lead to more contradictions and unpredictability in legal outcomes. Therefore, there is a need to establish clear definitions that can enable the penalization of criminal behaviors accordingly. Moreover, it would be important for law enforcement to be able to assess the mens rea and actus rea in the Metaverse environment, as well as apply the relevant age of criminal responsibility.

Future-thinking in policy

It is crucial that any policy or legal framework adopted to regulate the Metaverse is future-proof. Metaverse platforms and technologies will continue to evolve and might change in unimaginable ways. Future-proofing policies and laws requires a comprehensive strategy. Law or policy design techniques can help, such as the use of technology-neutral terminology that can easily apply to unknown future technologies. Systematic and regular reviews of policies and laws can help assess their effectiveness and keep them up to date. These reviews can be supported by legal requirements for relevant public bodies (e.g., regulators, law enforcement agencies) and other stakeholders (e.g., private sector and civil society) to produce periodic reports on the evolution of Metaverse technologies and related criminal trends.

CONCLUSION

In a rapidly evolving world marked by technological advancements and constant innovation, it is vital for law enforcement to remain agile and resilient. This requires continuous monitoring of new developments and analyzing the impact of these changes. As part of this effort, this White Paper provides important insights into the multifaceted aspects of the Metaverse.

With the aim to contribute towards a secure-by-design Metaverse, this paper presents a comprehensive analysis of various dimensions of the Metaverse from a law enforcement perspective, based on the inputs from the INTERPOL Metaverse Expert Group. It raises awareness of the Metaverse's role as an effective tool for law enforcement, particularly in the areas of immersive training and other use cases. It also presents a typology of various types of Metacrime.

In terms of forensics and investigations within the Metaverse, it outlines several key elements to consider when accessing and recovering the evidence, including endpoints, servers, engines and platforms as well as virtual asset analytics. To address complex governance issues, assessing the application of existing national and international laws, conducting regular policy reviews to reduce the gaps, and devising future-proof policies are recommended.

Recognizing that the Metaverse spans multiple jurisdictions, dimensions, and organizations, a holistic approach involving multi-stakeholder engagements and cross-border collaboration is pivotal for an effective law enforcement response to Metacrime. INTERPOL stands ready to continue this dialogue with various stakeholders worldwide to help build a secure and safe Metaverse. In support of the global law enforcement community, INTERPOL will remain at the forefront of efforts to safeguard our future world.

INTERPOL

www.interpol.int INTERPOL @INTERPOL_HQ INTERPOL_HQ INTERPOL HQ INTERPOL