Chapter 4

Online Crime in the Metaverse:
A Study on Classification, Prediction, and Mitigation Strategies

John Blake

iD https://orcid.org/0000-0002-3150-4995

University of Aizu, Japan

ABSTRACT

With the burgeoning growth of the metaverse and online virtual environments, new security challenges have been introduced that require careful exploration and mitigation. An increasing proportion of human interactions and transactions now take place in these digital spaces, making it essential to protect users and ensure the safety and integrity of virtual worlds. This chapter explores three dimensions of this issue. First, through a study of the types of crimes that occur in these environments, to gain a holistic understanding of the cybercrime technoscape. Second, the authors use a two-pronged approach to increase the safety of the metaverse by targeting both potential perpetrators and victims. This is achievable by identifying indicators that may be used to detect potential perpetrators or victims. Thirdly and finally, strategies and techniques to make these online communities safer are suggested.

1. INTRODUCTION

Online virtual environments, such as the Metaverse, are interconnected, immersive spaces that transcend traditional digital boundaries, linking together multiple three-dimensional virtual worlds. This dynamic technoscape is able to amalgamate augmented reality and virtual reality. The metaverse has experienced exponential growth (Lee, 2022), becoming a nexus for social interaction, entertainment, education, and economic activity (Khalid, 2023). The combination of technological advancements, increased accessibility, and a shift towards remote engagement has fueled this expansion, transforming the metaverse into a complex transactional space where digital assets, services, and experiences are exchanged. In an era marked by digital convergence and globalization, the emergence of the Metaverse underscores a paradigmatic shift in how individuals interact, transact, and perceive both virtuality and reality. As

with real-world transactions of assets, services and experiences, such spaces also attract perpetrators of opportunistic or premeditated crimes. In the physical world a teenager who notices a mobile phone left on a seat, but pockets the device on the spur of the moment. Likewise, a player in a massive online multiplayer game may come across a naïve player who may be convinced to share details of passwords and usernames, that may ultimately result in the loss of the associated digital assets (DaCosta & Seok, 2020).

In the physical world, police forces serve a variety of essential functions aimed at maintaining public order, enforcing laws, and ensuring the safety and well-being of citizens. Through patrolling, community policing, and various crime prevention programs, police work to deter criminal activities before they occur, and maintain a safe and orderly environment for all members of the community. However, the concept of policing in the metaverse raises complex and evolving questions. Traditional policing within virtual environments is a developing and largely uncharted territory (Rosenberg, 2022).

While the ramifications of cybercrimes are well-understood (Aiken et al., 2019), there exists a significant research gap in the development of a comprehensive framework that can not only classify the diverse and evolving nature of these crimes but also predict potential perpetrators and victims, and proactively mitigate occurrences. Existing methods often suffer from fragmentation, relying on disparate tools and techniques that lack cohesion and adaptability to the fast-changing cyber landscape. The absence of a unified approach hampers the ability to understand, analyze, and effectively respond to cybercrimes, leaving communities and individuals at heightened risk. This article seeks to address this research gap by exploring avenues that can be adopted to address the unique challenges of cybercrime.

The following section provides an indicative taxonomy of crimes which may be committed in the Metaverse, some of these cybercrimes can be classed as fully online while others are hybrid, and include both digital-initiated and physical-initiated hybrid crimes. Chanda and Snowe (2022) proposed a multilevel theoretical taxonomy of cybercrimes with a focus on the target of the crime, namely the technological ecosystem or specific victims, e.g. indivdiuals or organisations. Different categories of crimes are next introduced beginning with the crimes most commonly associated with cybercrime, such as cyberstalking and identity theft (Awadallah et al., 2023). However, the multitude of crimes that can be committed or initiated online is much broader. Having established the range of crimes, the focus turns to prediction, specifically the prediction of potential perpetrators and victims. Sociodemographic factors related to perpetrators are first considered. The traits and behaviours of potential victims are next discussed. Statistical models that could be used for risk assessment are described and explained. The final focus is on ways to make online platforms safer though the use of various mitigation strategies, such as moderation, education, detection and regulation.

2. CRIME SPACES

Cybercrimes operate across distinct domains that can be categorized into three specific spaces: virtual, hybrid, and physical. In the virtual space, crimes are committed entirely online; the hybrid realm encompasses crimes transitioning between online and offline worlds; and the physical space refers to tangible geographic locations tied to criminal activities in the Metaverse. Each crime space presents its own challenges and intricacies. The term crime space denotes the environment in which these offenses take place, while geographic regions refer to the tangible locations connected to the crime, which may or may not coincide with the locations of the perpetrators or victims. The complex interplay between these creates a web of jurisdictional challenges, conflicting laws, data privacy concerns, and legal enforcement

Related Content

Blind Detection of Partial-Color-Manipulation Based on Self-PRNU Estimation
Sun Yuting, Guo Jing, Du Lingand Ke Yongzhen (2020). *Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice (pp. 103-116).*
www.irma-international.org/chapter/blind-detection-of-partial-color-manipulation-based-on-self-prnu-estimation/252682

Attack Graph Analysis for Network Anti-Forensics
Rahul Chandranand Wei Q. Yan (2014). *International Journal of Digital Crime and Forensics (pp. 28-50).*
www.irma-international.org/article/attack-graph-analysis-for-network-anti-forensics/110395

Advances in Security and Privacy in Wireless Sensor Networks
Dulal C. Kar, Hung L. Ngo, Clifton J. Mulkeyand Geetha Sanapala (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications (pp. 1654-1681).*
www.irma-international.org/chapter/advances-security-privacy-wireless-sensor/61031

The UID Project: Lessons Learned from the West and Challenges Identified for India
Rajarshi Chakraborthy, Haricharan Rengamani, Ponnurangam Kumaraguruand Raghav Rao (2011). *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives (pp. 1-23).*
www.irma-international.org/chapter/uid-project-lessons-learned-west/50710

Anti-Forensics of Double Compressed MP3 Audio
Biaoli Tao, Rangding Wang, Diqun Yanand Chao Jin (2020). *International Journal of Digital Crime and Forensics (pp. 45-57).*
www.irma-international.org/article/anti-forensics-of-double-compressed-mp3-audio/252867