


Chapter 3

Navigating the Metaverse: Forecasting Cybercrime in the New Age of Virtual Reality

Akashdeep Bhardwaj

 <https://orcid.org/0000-0001-7361-0465>

University of Petroleum and Energy Studies, India

ABSTRACT

The rise of the metaverse—a virtual world where individuals can interact with each other and digital objects in a fully immersive environment—has led to new challenges in the world of cybersecurity. As more individuals and businesses move towards this new frontier, the potential for cybercrime is also increasing. In this chapter, the authors explore the diverse types of cybercrime that may emerge from virtual theft and fraud to privacy violations and hacking. They also discuss the unique challenges faced by law enforcement and security professionals in detecting and preventing these crimes in a fully virtual environment. To aid in forecasting these crimes, the authors examine current trends and technological developments that may impact the future of the metaverse, including the growth of decentralized technologies, the increasing prevalence of artificial intelligence, and the potential for quantum computing. By understanding the potential risks and challenges of the metaverse, we can better prepare ourselves for a future where virtual and physical crime intersect.

1. INTRODUCTION

As technology continues to evolve and become more integrated into our daily lives, the threat of cybercrime (What is Cyber Crime? Types, Examples, and Prevention, 2023) is becoming increasingly prevalent. The rise of the metaverse, a virtual world that is being created by the convergence of the physical and digital worlds, is presenting new challenges and opportunities for those looking to commit cybercrimes. Forecasting cybercrimes in the age of the metaverse is becoming a critical issue for law enforcement agencies, governments, and businesses. Forecasting cybercrimes in the age of the metaverse is becoming increasingly important as the metaverse continues to grow and evolve. The metaverse is creating new

DOI: 10.4018/979-8-3693-0220-0.ch003

opportunities for cybercriminals to commit crimes and new challenges for law enforcement agencies and businesses to detect and prevent cybercrime. The metaverse (What Does Metaverse Mean and How Does This Virtual World Work?, 2023) is an emerging technology that has the potential to change the way we interact with each other and with the digital world. It is a virtual environment where users can create and explore digital spaces, socialize with other users, and participate in various activities. However, with the emergence of the metaverse comes new challenges and opportunities for cybercriminals.

Cybercrime is a type of criminal activity that is committed using the internet, computers, or other digital devices. Cybercriminals can use a variety of techniques to commit cybercrime, including hacking, phishing, malware, and social engineering. With the metaverse, cybercriminals have a new platform to commit cybercrime, and they are already taking advantage of this opportunity. One of the most significant risks of cybercrime in the metaverse is virtual currency theft. In the metaverse, users can earn virtual currency by participating in various activities, and this virtual currency can be exchanged for real-world goods and services. Cybercriminals (Cybercriminals – Definition, 2023) can steal virtual currency by hacking into user accounts or by using social engineering techniques to trick users into giving them access to their virtual wallets. Another significant risk of cybercrime in the metaverse is virtual identity theft. In the metaverse, users create virtual avatars that represent them in the virtual world. Cybercriminals can steal these avatars and use them to commit virtual crimes or to access the user's personal information. Virtual identity theft can be especially dangerous because it can lead to real-world identity theft and financial fraud. Cybercrime in the metaverse can also take the form of virtual harassment and cyberstalking. In the virtual world, users can communicate with each other using text, voice, or video chat. Cybercriminals can use these communication channels to harass or stalk other users. This type of cybercrime can be particularly challenging to detect and prevent because it takes place in a virtual environment.

To address these and other cybercrime risks in the metaverse, businesses, governments, and law enforcement agencies are taking steps to increase awareness, prevention, and response. They are developing innovative technologies and strategies to detect and prevent cybercrime, such as using artificial intelligence to detect unusual patterns of activity or developing blockchain technology to create a more secure virtual environment. Other companies are creating virtual crime units to investigate and prosecute cybercriminals in the metaverse. Despite these efforts, the risks of cybercrime in the metaverse are likely to persist and evolve. As the metaverse continues to grow and become more integrated into our daily lives, it will become increasingly important to develop effective strategies to prevent and address cybercrime. This will require collaboration between governments, businesses, and individuals to ensure that the benefits of the metaverse are realized without compromising our safety and security.

2. EVOLUTION OF METAVERSE AND CYBERCRIME

The concept of the metaverse has captured the imagination of tech enthusiasts, science fiction writers, and futurists for decades. It envisions a virtual reality space that goes beyond the boundaries of the physical world, offering immersive, interconnected experiences for users. While the idea of the metaverse dates to the early 1990s, its evolution has been a complex journey marked by technological advancements, societal shifts, and economic developments. In this exploration of the metaverse's evolution, we will trace its roots, examine key milestones, and consider future possibilities. The origins of the metaverse can be traced back to science fiction, notably Neal Stephenson's 1992 novel 'Snow Crash' and Vernor Vinge's 1981 novella 'True Names'. Both works depicted immersive virtual worlds where individuals

31 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/navigating-the-metaverse/334494

Related Content

An Adaptive JPEG Steganographic Scheme Based on the Block Entropy of DCT Coefficients

Chang Wang, Jiangqun Ni, Chuntao Wang and Ruiyu Zhang (2012). *International Journal of Digital Crime and Forensics* (pp. 13-27).

www.irma-international.org/article/adaptive-jpeg-steganographic-scheme-based/68407

On the Reliability of Cryptopometry

Thomas Martin, Laurence O'Toole and Andrew Jones (2013). *International Journal of Digital Crime and Forensics* (pp. 27-38).

www.irma-international.org/article/on-the-reliability-of-cryptopometry/79139

Reliable Motion Detection, Location and Audit in Surveillance Video

Amirsaman Poursoltanmohammadi and Matthew Sorell (2009). *International Journal of Digital Crime and Forensics* (pp. 19-31).

www.irma-international.org/article/reliable-motion-detection-location-audit/37422

Recognizing Substitution Steganography of Spatial Domain Based on the Characteristics of Pixels Correlation

Zhe Chen, Jicang Lu, Pengfei Yang and Xiangyang Luo (2017). *International Journal of Digital Crime and Forensics* (pp. 48-61).

www.irma-international.org/article/recognizing-substitution-steganography-of-spatial-domain-based-on-the-characteristics-of-pixels-correlation/188362

A DFT-Based Analysis to Discern Between Camera and Scanned Images

Roberto Caldelli, Irene Amerini and Francesco Picchioni (2010). *International Journal of Digital Crime and Forensics* (pp. 21-29).

www.irma-international.org/article/dft-based-analysis-discern-between/41714