Chapter 6
Societal Risks of Using Cyber Metaverse Technology

Amar Yasser El-Bably
Police Academy, Egypt

ABSTRACT

AI's widespread use poses challenges, especially accountability and legal readiness for metaverse's unique traits. This study addresses AI's current hurdles, focusing on regulating AI-related crimes, including metaverse. It aims to define responsibilities and penalties. Metaverse's societal, reputational, and security implications, along with tech firms' oversight, can escalate cybercrime. Complex evolving cybercrime patterns hinder guilt proof. Criminalizing tech use in terrorism planning and financing is crucial. Social media users face risks like deepfakes, fostering doubt and inciting terrorism. Tech-security agency partnership is vital. Growing digital interconnectedness heightens cybersecurity issues. Metaverse's growth and internet use call for strengthened anti-terrorism and IT crime laws.

INTRODUCTION

Today we are faced with the phenomenon of social media and Internet applications, which are phenomena that science fiction books have always dealt with in the past. Now, we see these technologies becoming an integral part of our lives, with three billion people interacting on the Facebook platform and two billion using Instagram every day. Estimates predict that the size of the Internet market will reach $1.6 trillion by 2030, and the value of electronic commerce is currently $50 billion (Fahd, 2022).

And with the advent of the concept of metaverse, we find that it will open the doors to new jobs such as virtual architects. Already, Mark Zuckerberg announced his future for Metaverse and pointed to the potential for jobs and investments in the European Union worth hundreds of billions.

The importance of technology management in this context cannot be denied. As we can witness how the Twitter platform has evolved from simply publishing short messages to a basic source for displaying our daily news. Social media has played a major role in promoting new media, and this is evident in how people rely on it to follow up on events and news, a development that may be an alternative to traditional news agencies and technology based on continuous management.

DOI: 10.4018/979-8-3693-0220-0.ch006

And with this technological advance, new challenges and potential risks emerge. Including the use of websites by terrorist groups for their purposes, It requires the development of coping mechanisms and the need for a proactive step by both legislators and those in charge of law enforcement to confront this danger by enacting legislation and making amendments to national laws and the need to adhere to the use of electronic signature to tighten control over commercial transactions that take place through Metaverse, and activate international agreements that combat Cybercrimes, setting legal requirements and rules for companies operating in the metaverse field to obtain licenses to carry out their work with criminal liability in case of violating these conditions and rules, and developing plans to protect metaverse users and activating the Information Technology Crime Law No. 175 of 2018.

This research deals The crime of propaganda and promotion of terrorism where Penalties are directed at those who use metaverse technology to spread and promote terrorist content or to recruit volunteers to participate in terrorist acts Those who use metaverse technology to plan or carry out terrorist attacks are punished, whether by directing actual attacks or providing training and mentoring to militants. And Criminalize the financing of terrorism using technology: Those who use metaverse technology in terrorist financing operations or exchange money to support terrorist activities will be held accountable.

THE STUDY PROBLEM

Importance the Study

I became The terrorism industry in light of the rapid technical progress is a very important topic In light of preserving societies from extremism and terrorism, Andin order to put lines of defense to confront the causes of terrorism through the cyber environment Preserving the cyber violations and penetrations of terrorist militias must be criminalized Use Information technologies such as metaverse in communication, tango, training, and setting scenarios for hostile and terrorist acts in light of the rise in Internet users and social communication, And must Inaugurating a strong partnership between technology companies and security and intelligence agencies To combat hostilities committed via advanced technologies and The crime of propaganda and promotion of terrorism: Penalties are imposed on those who use metaverse technology to spread and promote terrorist content or to recruit volunteers to participate in terrorist acts.

Objectives of the Study

- Identify the most important properties of Metaverse technology and its security and societal risks considering the digital development.

- Recognition The dangers of deep falsification technology through social networking sites and platforms and the risks of artificial intelligence related to deepfakes, Internet bots, spreading rumors, and how dangerous it is the dangers of the dark web Dark Web) in spreading rumors.

- Identify dangers of “metaverse” augmented reality associated with social networking sites and platforms in training and education on weapons and the danger of chatting in planning terrorist operations.

- Finding out about the latest UAE and Egyptian legislation regarding combating information technology crimes related to financing and training terrorist elements on modern technologies and using them to harm national and public security.