THE ROLE OF DEEPFAKES IN CYBERATTACKS

[1]SALEH ALRAEESI, [2]EISA ALBLOOSHI, [3]WALEED ALRAEESI, [4]MAHER ALJABER

[1,2,3]Master of Cybersecurity Law, Fujairah University,
[4]Associate Professor of Cybersecurity Law, Faculty of Law. Fujairah University.
E-mail: [1]202510441@fu.ac.ae, [2]202510316@fu.ac.ae, [3]202510332@fu.ac.ae, [4]m.aljaber@fu.ac.ae,
maheraljaber@bau.edu.jo

Abstract: In the digital age, the world is witnessing rapid advancements in artificial intelligence technologies, leading to the emergence of advanced tools capable of producing highly realistic digital content, most notably deepfake technology. Deepfakes have given rise to new types of cyber threats, as they are used in financial fraud, identity theft, and the spread of fake news. They also complicate identity verification processes, particularly given the potential to breach biometric verification systems. The research problem of this study is to examine the role of deepfake technologies in cyberattacks, and a descriptive-analytical approach was adopted to achieve the study's objectives. The study found a significant gap between technological development and the legislation governing it; therefore, it recommends the development of specialized legal frameworks to combat deepfake crimes by raising public awareness of the risks of deepfakes**.**

Keywords - Deepfake, Cyber Crimes, UAE Legislation, Cybersecurity.

I. INTRODUCTION

In the digital age, the world has witnessed rapid advancements in artificial intelligence technologies, leading to the emergence of sophisticated tools capable of producing highly realistic digital content. One of the most prominent of these technologies is so-called deepfake technology, a development that has created unprecedented challenges for cybersecurity systems, which are now required to protect data and systems as well as ensure the authenticity of digital content. Deepfakes are among the most serious of these challenges, given their ability to undermine trust in digital information and their potential use in complex criminal activities.

The UAE legislature has not provided a specific definition of deepfakes; however, existing laws, such as the Law on Combating Rumors and Cybercrimes, address their effects by criminalizing related acts, such as the dissemination of false information or the manipulation of digital content with the intent to harm others. Provisions on forgery and fraud in the Penal Code also apply to certain cases of deepfakes, which provides some legal protection.

Deepfakes essentially involve using artificial intelligence technologies to create fake content that appears real, whether in the form of images, videos, or audio recordings. This type of forgery is used to impersonate people or manipulate digital content in ways that are difficult to detect, raising numerous legal and security issues.

Deepfakes have led to the emergence of new types of cyber threats, as they are used in financial fraud, identity theft, and the spread of fake news, and they also complicate identity verification processes, especially given the potential to breach biometric verification systems. It is also an effective tool in social engineering attacks, where it is used to deceive victims by imitating the voices or faces of trusted figures, such as executives, to carry out fraud or data theft.

1.1. Problem of the Study

The focus of this study is on deepfakes as an emerging technique in cyberattacks, highlighting the importance of defining deepfakes and understanding how they are used to commit cybercrimes, as well as their role in so-called social engineering attacks.

1.2 Methodology

This research is based on the use of several integrated scientific approaches to ensure that the subject is addressed with accuracy and depth, specifically the descriptive-analytical approach. The descriptive-analytical approach was used to present concepts related to deepfakes, alongside the analytical approach, which aims to interpret legal rules and examine their applications in light of technological developments.

1.3 Importance of the Study

The significance of this study stems from the fact that it addresses a contemporary phenomenon with a direct impact on cybersecurity; its importance lies in clarifying its technical and legal dimensions, as well as providing an analysis that assists decision-makers in developing effective strategies to address it. The importance of this study is not limited to the theoretical aspect but extends to the practical aspect, as it can contribute to supporting the work of judges and members of the Public Prosecution Service and improving the performance of competent authorities in dealing with emerging types of cybercrimes. It can also serve as a reference for researchers in the field of cyberlaw, which is currently one of the most rapidly evolving fields.

II. THE NATURE AND IMPORTANCE OF CYBERSECURITY

Cybersecurity is a modern concept that has emerged alongside the rapid development of digital technology; it refers to a set of measures and technologies designed to protect electronic systems, networks, and data from attacks or unauthorized breaches. This includes protecting sensitive information and ensuring its confidentiality, integrity, and availability, thereby ensuring business continuity and the stability of digital systems (Behl & Behl, 2017).

Cybersecurity is also a cornerstone of digital infrastructure protection, as it helps secure sensitive information and ensure business continuity, playing a vital role in critical sectors such as banking, healthcare, education, and telecommunications. Any breach in cybersecurity leads to significant financial losses, as well as a loss of trust in digital systems; it also helps protect privacy and strengthen the digital economy, making it an essential element of sustainable development.

The importance of cybersecurity lies in the fact that it constitutes the first line of defense for protecting the digital infrastructure upon which modern societies rely, as dependence on digital technology has become indispensable in managing various aspects of daily life—whether at the level of individuals, organizations, or governments. Cybersecurity is no longer merely a technical option; it has become a strategic necessity for ensuring economic, social, and political stability (Bernner, 2010).

In the financial and banking sector, cybersecurity plays a pivotal role in protecting electronic transactions from breaches and fraud, especially given the widespread adoption of digital banking services and financial applications. Any breach in this sector could lead to massive financial losses, as well as a loss of customer trust in financial institutions, which directly impacts the national economy.

In the healthcare sector, protecting patients' medical data is a top priority due to its highly sensitive nature; any leakage or tampering with this data could endanger patients' lives, especially given the growing reliance on digital systems for managing medical records and smart medical devices. Furthermore, cyberattacks on hospitals can disrupt vital health services, posing a direct threat to human security.
In the education sector, cybersecurity has become essential for protecting online learning platforms from breaches and ensuring the security of students' and teachers' academic data; it also helps create a safe learning environment, particularly with the shift toward digital education and distance learning.

On the other hand, cybersecurity helps build trust in the digital economy, thereby encouraging the use of digital services and supporting innovation and growth, while also protecting national security from attacks that target infrastructure and undermine stability. Therefore, it is an essential element for achieving sustainable development, as no digital society can thrive without a robust security framework(Behl & Behl, 2017).

For example, numerous real-world examples have emerged over the past five years illustrating the impact of cyberattacks on critical sectors, including the attack on the Colonial Pipeline in the United States in 2022, and at Australian seaports in 2023, specifically affecting DP World Australia, as well as the impact of cyberattacks on the electricity sector in Ukraine in 2015, banking services in South Korea in 2011, and finally the NHS healthcare sector in the UK in 2017(Bernner, 2010).

The methods used to carry out cyberattacks have evolved with the emergence of deepfake technology and various applications such as Deep APP, Zaog, Deep Face Lab, and Face Swap. The volume of deepfake content online increased by 900% between 2019 and 2020. Like other cybercrimes, its most significant characteristic is that it is transnational, as its effects extend beyond the borders of the country where it occurred(Moharam, 2022).

III. THE DEEPFAKES AND STRATEGIES TO ADDRESS THEM

It is defined as "a term referring to visual clips that have been manipulated, or the alteration of a person's image or voice in a video, to make it appear real (Moharam, 2022). The purpose is to create fake content that appears real by manipulating images and videos to produce a new video that is, in fact, fake and untrue. Therefore, artificial intelligence plays a prominent role in deepfake crimes through applications that contribute to the creation of audio or visual content that mimics reality while simultaneously distorting the truth, with the intent to harm the content owner in a manner that violates the law.

Deepfakes pose significant societal, individual, political, and legal risks, as the spread of this technology greatly contributes to the proliferation of false content, flooding the internet with fabricated material and leading to the dissemination of news, images, or videos that are contrary to the truth. It also personally affects the individual depicted in the content, negatively impacting them and leading to the spread of character assassination by portraying them engaging in untrue acts—such as accepting bribes, expressing racist sentiments, making diplomatically

sensitive statements, or committing acts of violence against civilians (Moharam, 2022).

Deepfake and other technologies can also be used in activities that influence the political landscape, such as undermining democracy by spreading fake content intended to mislead voters. For example, during the 2017 French election campaign, Macron's campaign was the victim of cyberattacks attributed to a Russian-backed hacker group, which directly affected the integrity of the elections and posed risks to national security (Alnajar, 2024).

From a legal perspective, deepfakes raise significant legal concerns regarding issues of proof and the admissibility of evidence in legal proceedings. The proliferation of fake content created using deepfake technology may raise legal issues regarding the admissibility of electronic evidence in legal proceedings, as deepfake technology has made it easier to the creation of convincing audiovisual material, which may affect the evidence presented and its admissibility.

Consequently, the importance of combating deepfake crimes has become increasingly evident due to the harm they inflict on individuals, society, and the state. However, a significant legal challenge is that these crimes are considered emerging offenses that traditional legislation has been unable to address or regulate. This has compelled states to address them through cybercrime laws until such time as deepfake crimes are regulated by separate and detailed legislation (Taylor et.al, 2011).

Although this type of crime is relatively new, some jurisdictions have sought to address deepfakes due to the importance of regulating them and the consequences and harm they cause at the individual and societal levels. For example, China was one of the first countries to recognize the importance of enacting detailed legislation on deepfakes, issuing in 2022 a regulation titled "Provisions on the Administration of Deep Synthesis Internet Information Services".

Article 6 of this regulation explicitly states that: "No organization or individual may use deepfake services to produce, reproduce, publish, or transmit information prohibited by laws or administrative regulations, or engage in activities prohibited by such laws and regulations, including those that endanger national security and interests, harm the image of the nation, damage the public interest of society, disrupt the economic or social order, or infringe upon the lawful rights and interests of others".

In the United States, legislation has kept pace with the emergence of deepfakes. Efforts began in 2019 when a federal bill was introduced to regulate the use of fake images and videos intended to harm individuals or society. This was followed by the passage of a law specifically addressing deepfakes, titled:"DEEP FAKES Accountability Act of 2020"
Its goal was to limit the spread of fake content by requiring creators to watermark the content to notify viewers that it is not real, under penalty of legal liability. Virginia and Texas were the first two of the 50 U.S. states to pass legislation criminalizing certain deepfake offenses in 2019.

At the European Union level, the EU has also addressed the threat of deepfakes and their risks by enacting a series of laws addressing artificial intelligence and deepfakes, including the Artificial Intelligence Act and the General Data Protection Regulation 2016 (GDPR).

IV. CONCLUSION

The current study has reached a number of findings, as follows:

1. Deepfake technology has emerged as a modern means through which cybercrimes are committed.
2. This study found that the admissibility of digital evidence has been called into question with the emergence of deep-fake applications.
3. This study also found that numerous legal, technical, and practical challenges have emerged in combatting crimes committed through the use of deepfakes.
4. Finally, this study found that, with the exception of a few countries, legal systems around the world have yet to enact specific legislation regulating the issue of deepfakes.

In light of the findings, and given the accelerating pace of digital transformation, the study has identified a number of recommendations, which we summarize below:

1. The need to enact specialized procedural legislation on deepfakes through a joint international effort under the auspices of the United Nations, with the aim of regulating and criminalizing deepfakes.
2. Efforts should be made to enhance the training of judges and public prosecutors in the field of digital evidence in order to keep pace with the tremendous technical advancements in the field of cybercrime and the methods used to commit it.

REFERENCES

[1] Alnajar, S. 2024. Criminal Response to Crimes Stemming from the Use of Deepfake Technology. Journal of Legal Science. 39 (2). 575-633

[2] Behl, A., & Behl, K. 2017. Cybersecurity and cyberwar: What everyone needs to know. Oxford Academic Journal. 12(2), 55–70.

[3] Bernner, S. 2010. Cybercrime: Criminal Threats from Cyberspace. Praeger Security International

[4] Moharam, A. 2022. Uses of Artificial Intelligence: The Use of Deepfake Technology in Defaming Others as a Model. A Contemporary Comparative Jurisprudential Study. Journal of Jurisprudential and Legal Research, Al-Azhar University, Faculty of Sharia and Law. 48 (1). 2491-2589.

[5] Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. 2011. Forensic investigation of cloud computing systems. Network Security. 2011(3), 4–10.

★★★