8-2023

The Future of Deep Fakes: Analyzing the Potential Future Consequences of the Widespread Use of Deepfakes on the Policing Sector

Maryam Salem Alshamsi
msa5605@rit.edu

The Future of Deep Fakes:

Analyzing the Potential Future Consequences of the Widespread Use of Deepfakes on the Policing Sector

by

Maryam Salem Alshamsi

A Thesis Submitted in Partial Fulfilment of the Requirements for the Degree of Master of Science in Professional Studies: Future Foresight and Planning

Department of Graduate Programs & Research

Rochester Institute of Technology
RIT Dubai
August 2023

RIT

Master of Science in Professional Studies:

Future Foresight and Planning

Graduate Thesis Approval

Student Name**:** Maryam Salem Alshamsi

Graduate Capstone Title**:** The Future of Deep Fakes

Graduate Thesis Committee:

Name: Dr. Sanjay Modak Date:24/8/2023

Chair of committee

Name: Dr. Khalil Al Hussaeni, Date: 24/8/2023

Member of committee

Acknowledgments

I would like to begin by expressing my gratitude to my workplace for their generous support, in sponsoring my education. I also want to thank my manager, Dr. Ibrahim bin Seba Almarri, who believed in my potential and encouraged me to pursue studies. I am grateful to my colleagues for the support and understanding throughout this process. Thank you to Dr. Sanjay Moudak, chair of committee as well as my mentor, Prof. Khalil Al Hussaeni, who has been providing guidance, patience and feedback on this project. Lastly, thank you to my friends and family for your unconditional support.

Abstract

In today's world there is a growing uncertainty in terms of the truthfulness of what we see and hear. People digest a great amount of information throughout the day using their devices, yet the quality and credibility of content is in question. People question if we are experiencing and perceiving the same reality at this point. This issue is not novel, however, it has progressed and developed to a level of realism that deceives people and affect their comprehension of information. Rapid technological advancement has raised the concern of what is referred to as "Deepfakes", a machine learning technique that allows the manipulation of media content, including, videos, photographs and voice. In present time, deepfakes is considered as an issue that affects public trust and law enforcement, history has revealed that it developed and progressed with time, however we are unsure of what the future of deepfakes holds, it has a high uncertainty and impact on public trust and law enforcement.

The policing sector common goal is to provide safety and security for citizens, therefore, proactive and reactive measures that are future oriented are important since the progression of crimes in the realm of artificial intelligence are accelerating. This paper aims to illustrate the future outlook for deepfakes and analyze its results' using future foresight methods, including; the futures wheel, a swot analysis and scenario planning. The study will also examine the complex ethical, legal, and social issues surrounding the use of deepfakes on the policing sector through an interdisciplinary method that draws on theories of technology, criminology, and future foresight. The paper will conclude by providing recommendations for mitigating the risks of deepfakes, while highlighting the potential opportunities for leveraging this technology to enhance public safety and trust.

Key Words: Crimes of the future, Deepfakes, police challenges, future foresight

Table of Contents

List of Figures

List of Tables

Chapter 1

1.1 Introduction

According to Korshunov and Marcel deepfake is a technique used to manipulate or tamper with media content allowing users to replace the face of an individual, for instance; a famous actor or celebrity with someone else (2018). This involves creating videos, audio or images that appear and sound genuine. `in which, the process involves building a model based on datasets that contains collection of recordings, videos or photos of the targeted person. Deepfake technology utilizes techniques from the field of artificial intelligence which aims to understand human thought processes and behavior, as well as machine learning since it enables systems to learn from data. Deepfake has gained popularity since it has the ability to produce highly realistic results using data such as photos and videos; secondly its accessibility for general users due to its widespread availability. As Matern et al. (2019) stated it is possible to create deepfake images or videos without extensive knowledge of machine learning and programming. Stover (2018) also mentioned that deepfakes are being used to generate fabricated videos of politicians, which can contribute to the dissemination of news (Albahar & Almalki, 2019).

1.2 Statement of the Problem

Law enforcement is facing serious challenges due to the development of deepfakes. These sophisticated techniques have the ability to produce fabricated videos and images that are incredibly realistic making it extremely challenging to distinguish them from genuine ones. In which, has implications to the legal system as deepfakes can be exploited to manipulate evidence or challenge the authentication of evidence and potentially result in wrongful convictions. Moreover, deepfakes can be used for purposes, such as; manipulating electronic evidence, perpetrating scams and frauds, creating fake online identity distributing pornography, facilitating online child exploitation and even disrupting financial markets (Europol, 2022). The ramifications extend further as they could also be deployed to disseminate misleading information about law enforcement activities or individuals. Given these threats posed by deepfake technology in relation to law enforcement it is crucial for stakeholders to acknowledge these risks proactively and take measures to mitigate them effectively and be prepared for its future possibilities.

1.3 Objectives and Deliverables

This study aims to navigate the future of deepfakes; by defining the uncertainties and exploring factors that might impact law enforcement. For the police, it is very important to have resiliency to the challenges that hinders safety and security. Being prepared to tackle crimes before they happen is a key concept in achieving excellence in policing, by which achieving the goal of maintain safety and security is a top priority. The goal of this research is to highlight the possible future outcomes and to analyze the challenges and opportunities to mitigate risks associated with deepfakes. Additionally, this paper provides mitigation strategies recommendation based on the results and analysis of the used future foresight methods.

1.4 Limitations of the Study

The study had some limitations that needs to addressed to fully understand and interpret its findings. The main challenge is its general scope, as the extensive nature of the research might have affected the specificity and relevance of the information and resulting outcomes. Additionally law enforcement, due, to the nature of their work and the importance of their tasks tend to be cautious when it comes to sharing data. Therefore, the data provided for this study may not offer a representation of the situation as the absence of specific data could unintentionally favor hypotheses or conclusions potentially leading to misconstrued interpretations or general assumptions.

Chapter 2 - Literature Review

2.1 Literature Review

Photographs and videos are often used as evidence in police investigations and are submitted to courtrooms to resolve legal cases since they are considered reliable sources. However, increasingly sophisticated technology has led to the development of new video and photo editing techniques that have potentially made these pieces of evidence unreliable (Koopman, et al, 2018). The increase of technological advancements has enabled the effortless manipulation of photographic and video materials. In case this trend persists, it will be critical to detect photographic and video evidence before providing it in a court of law (Chesney & Citron, 2018).

The term 'Deepfake' originated in 2017 on a Reddit forum by a user named 'deepfakes'. The user boasted about the advancements in technology that enabled the swapping of faces in adult videos using open-source machine learning tools, specifically with the faces of celebrities (Cole, 2017). The term "Deepfake" was initially coined in scholarly publications as a combination of "deep learning AI" and "faked imagery." (Wagner & Blewer, 2019, p.33). According to Öhman's (2020) definition, deepfakes refer to videos that exhibit a high degree of realism, achieved through the use of Deep Learning algorithms to analyze a person's face and subsequently superimpose it onto the face of an actor in a video. According to Afchar et al., (2018), the prevalence of video and photo manipulation and fabrication is increasing, largely due to technological advancements, particularly in the fields of machine and deep learning.

Korshunov & Marcel (2018) has described "Fake News" as deliberate misinformation that is caused by the creation and dissemination of high-quality manipulated video content has been facilitated by recent advancements in automated video and audio editing tools, generative adversarial networks (GANs), and social media. Moreover, Yang et al. (2018) defined it as the process of generating Deep Fakes requires the utilization of deep neural networks to synthesize faces, which are subsequently inserted into original images or videos. Güera & Delp, (2018), terms Deepfake as the employment of deep learning algorithms to make fake photos by switching a person's face from a source image into a target image, creating a hard-to-detect fake image. Moreover, Maras, & Alexandrou (2019) states that Deepfake videos are the product of artificial intelligence or machine-learning applications that merge, combine, replace and superimpose images and video clips onto a video, creating a fake video that appears authentic.

Nguyen et al., (2021) provide a more comprehensive characterization of deepfakes in their research article, wherein they describe these falsified media as being generated through the utilization of artificial intelligence and classified into three distinct categories: face-swaps, lip-sync, and puppet-masters. According to Nguyen et al. (2021), the process of face-swapping entails overlaying the images of a target individual onto the source. On the other hand, lip-syncing involves modifying the lip movements in a video to synchronize with an audio clip. Additionally, puppet-masters utilize videos of a target person on a "puppet," and the facial expressions, head, and eye movements of another individual, or the "master," to animate the video of the "puppet."

An important aspect to consider is the expansion of the construct beyond facial manipulation, as Zhao et al. (2021) have incorporated the term in cartographic research to address manipulation in geospatial imagery.

Author	Year	Findings of Deepfakes Definition
Korshunov & Marcel	2018	Deliberate misinformation that is caused by the creation and dissemination of high-quality manipulated video content has been facilitated by recent advancements in automated video and audio editing tools, generative adversarial networks (GANs), and social media.
Yang et al.	2018	The process of generating Deep Fakes requires the utilization of deep neural networks to synthesize faces, which are subsequently inserted into original images or videos.
Güera & Delp	2018	Deepfake as the employment of deep learning algorithms to make fake photos by switching a person's face from a source image into a target image, creating a hard-to-detect fake image.
Maras, & Alexandrou	2019	Deepfake videos are the product of artificial intelligence or machine-learning applications that merge, combine, replace and superimpose images and video clips onto a video, creating a fake video that appears authentic.
Wagner & Blewer	2019	A combination of "deep learning AI" and "faked imagery”.
Öhman	2020	Videos that exhibit a high degree of realism, achieved through the use of Deep Learning algorithms to analyze a person's face and subsequently superimpose it onto the face of an actor in a video.
Nguyen et al	2021	Falsified media as being generated through the utilization of artificial intelligence and classified into three distinct categories: face-swaps, lip-sync, and puppet-masters.

Table 1: Progression of Deepfakes Definitions

Table 1 illustrates the progression of deepfakes definition, in which in its early stages was more of a general description, but in recent papers there has been more focus at different angles and categorization of the issue.

The evolution of deepfakes dates back to 1865 when an early case of face-switching is a portrait of American President Abraham Lincoln from around 1865. Lincoln's head has been superimposed on a print of John Calhoun from 1852 (Chawla, 2019). Late in 2017, a person going by the name "deepfakes" posted explicit videos to the well-known website Reddit while pretending they belonged to famous actresses. On February 7, 2018, almost all of the online forums and subreddits associated with this widely known "deepfaking" technique were either deleted or banned. The software engineer who created the deepfake approach, according to Gardiner (2019), provided a development kit that was effective enough to enable consumers to produce their own modified videos. The tools and features are made available as open source by popular software providers like NVidia and Google (Chawla, 2019). This indicates that, even if technical expertise and an awareness of computational parameters are necessary for the development of a technique like this, most of the necessary software is already accessible to the general public for use. Once the U.S. Department of Defense's Defense Advanced Research Project Agency (DARPA) learned that anyone with basic knowledge might interfere with any visual material, the threat took on significant dimensions (Siekierski, 2019). A researcher at the University of Washington produced a fake video of former U.S. President Barack Obama in July 2017, the general public was alerted to the possible disruptive intervention of deep fake technology. Following that, a poor quality deep fake video of President Donald Trump advising Belgians to leave the Paris Climate Change Agreement was posted to social media in May 2018.

Deepfake videos can be classified into several distinct categories; face-swapping, lip-synching, puppet-mastering, face synthesis, attribute manipulation, and audio deepfakes. Face-swap deepfakes involve the substitution of the face of the source individual with that of the target individual, resulting in the creation of a fabricated video featuring the target individual engaging in actions that were actually performed by the source individual. Deepfakes that focus on face-swapping are commonly created with the intention of exploiting the fame or reputation of well-known individuals by placing them in situations they have never been involved in (Boylan, 2018). These deepfakes are also employed to damage the public image of individuals, such as in cases of non-consensual pornography (Harwell, 2018). Lip-synching-based deepfakes involve the manipulation of the lip movements of a target individual to align them with a predetermined audio recording. The act of lip-syncing is employed with the intention of portraying an individual speaking in a manner that the perpetrator manipulates the victim to mimic. Deepfakes are generated using a puppet-master technique that involves replicating the target individual's facial expressions, eye movements, and head motions. The objective of puppet-master deepfakes is to manipulate the facial expressions or entire body of the source individual in a video, with the intention of animating them in accordance with the impersonator's preferences (Chan et al., 2019). The procedures involved in face synthesis and attribute modification incorporate the generation of facial images that show a high degree of realism, as well as the capacity to alter certain facial characteristics. The present manipulation is designed with the purpose of disseminating disinformation across social media platforms through the utilization of fabricated user profiles. Lastly, audio deepfakes primarily center around the utilization of deep learning methodologies to generate the voice of a specific individual, thereby simulating the speaker uttering content that they have not actually articulated.

The categorization of deep fake detection methods can be classified as either manual or automated, as stated by the European Union Agency for Law Enforcement (2022). The process of manual detection entails a labor-intensive task, which is practical only for a limited number of files, and necessitates adequate training to develop familiarity with all relevant indicators. Additionally, the complexity of this process increases by the associated human tendency to trust audio-visual material and operate from a default assumption of truth. Levine presents the notion of potential errors in the process of selecting files for inspection and conducting the inspection itself (2014). The deepfake generation models have the capability to produce visually convincing images, yet upon meticulous examination, these images may still exhibit imperfections. Several examples can be observed, as discussed by Venema and Geradt (2020). These include the idea of blurring around the edges of the face, the absence of blinking, the presence of light reflection in the eyes, inconsistencies in the hair, visible vein patterns, visible scars, and inconsistencies in the background, both in terms of subject and focus and depth.

While Automated detection refers to a system designed to scan digital content and provide automatic assessments regarding its authenticity. It is unlikely that such a system will attain perfection; however, as deepfake technology becomes more advanced, the system's ability to provide a high level of certainty may outweigh the need for manual inspection. Previous attempts to develop software capable of detecting manipulation have been made by various organizations, including Facebook (Michigan State University, 2022) and security firm McAfee (2020). The primary objective of these detection technologies is to uncover different signs of manipulation and provide an AI report that aids reviewers to assess the validity of the information. Deepfake detection models are typically trained using databases of deepfake images, as the creation tools for deepfakes require training data to accurately understand the appearance of a genuine individual. The understanding of manipulation indicators mostly relies on existing deepfake data, which has difficulties in accurately evaluating the effectiveness of identifying deepfakes created by either new or updated models. Furthermore, it is possible to enhance a deepfake Generative Adversarial Network (GAN) by incorporating updates that consider the indications identified by established detection models. This method seeks to modify the outputs in a way that prevents the development of these signs, allowing to be undetected.

The dissemination of modified content associated with events such as actions on social media platforms has the potential to incite unnecessary or misplaced police intervention. Law enforcement agencies involved in criminal investigations may incorrectly pursue an incorrect individual as a suspect in a crime due to the spread of a deepfake representation of said suspect fleeing the scene of the incident, which subsequently gains significant popularity on various social media platforms. Deepfakes may be used by people to distort visual media in an effort to portray police officers as participating in misconduct when they are not, undermining the authority of the law or inciting violence against policemen. Audio-visual evidence is widely recognized in court proceedings as a reliable and accurate representation of the events under investigation. The use of deepfakes has the potential for individuals to manipulate visual media with the intention of falsely depicting police officers engaging in misconduct, thereby aiming to undermine the credibility of law enforcement or instigate acts of violence against officers. The escalating skepticism towards authoritative figures, the employment of deepfakes and manipulated visual content has the potential to exert harmful influence on public sentiment. audio-visual evidence is commonly regarded as a reliable and accurate depiction of the events in question during legal proceedings. The authenticity of the depicted scene is typically not called into question, regardless of whether the file is obtained from the suspect's phone, acquired from social media, or obtained from the CCTV system of a nearby shop in proximity to the crime scene. The significance of cross-checking footage will be further heightened. According to the European Parliamentary Research Service (2022), the utilization of more small neural network architectures, coupled with advancements in hardware technology, will lead to a substantial reduction in both training and generation time. It is anticipated that in a few years, deepfake software will possess the capability to produce comprehensive deepfakes of entire bodies, execute real-time impersonations, and seamlessly eliminate elements within video footage. Lastly. recent advancements in algorithms have shown a notable capacity to achieve ever higher degrees of realism while maintaining a shorter delay. (Europol, 2022).

2.2 Main Takeaways

- Genuine content like; video, photos and audio can be manipulated and superimposed onto other individuals, leading to deliberate false content.
- Deepfakes can be produced by automated video and audio editing tools, generative adversarial networks (GANs), and social media.
- Deepfakes are very realistic and are hard to distinguish from genuine content, leading to major issue of trust and authenticity.
- Deepfakes can be generated by unskilled individuals are easy to create due to the availability of resources at an increasing rate.
- Detection methods for deep fakes are necessary to validate evidence for police investigations.
- Deepfakes detection can either be manual or automated, yet there are technical challenges in detecting deepfakes related to machine learning algorithms.
- Deepfakes poses many challenges to law enforcement and legal proceed

Chapter 3 - Research Methodology

Popper's (2008) Foresight Diamond presents a theoretical framework that categorizes methods according to their primary source of knowledge, which is derived from creativity, expertise, interaction, or evidence, as shown in figure 1. These domains exhibit interdependence and are not completely separate from each other. The study will employ qualitative methodologies to investigate its research question on the future of deepfakes. The methods include; a SWOT analysis, Future Wheels and the scenario planning method to investigate the four plausible futures of deepfakes.

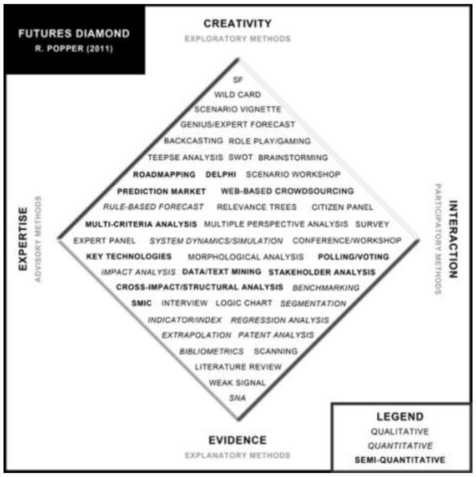

FUTURES DIAMOND
R. POPPER (2011)
CREATIVITY
EXPLORATORY METHODS
SF
WILD CARD
SCENARIO VIGNETTE
GENIUS/EXPERT FORECAST
BACKCASTING ROLE PLAY/GAMING
TEEPSE ANALYSIS SWOT BRAINSTORMING
ROADMAPPING DELPHI SCENARIO WORKSHOP
PREDICTION MARKET WEB-BASED CROWDSOURCING
RULE-BASED FORECAST RELEVANCE TREES CITIZEN PANEL
MULTI-CRITERIA ANALYSIS MULTIPLE PERSPECTIVE ANALYSIS SURVEY
EXPERT PANEL SYSTEM DYNAMICS/SIMULATION CONFERENCE/WORKSHOP
KEY TECHNOLOGIES MORPHOLOGICAL ANALYSIS POLLING/VOTING
IMPACT ANALYSIS DATA/TEXT MINING STAKEHOLDER ANALYSIS
CROSS-IMPACT/STRUCTURAL ANALYSIS BENCHMARKING
SMIC INTERVIEW LOGIC CHART SEGMENTATION
INDICATOR/INDEX REGRESSION ANALYSIS
EXTRAPOLATION PATENT ANALYSIS
BIBLIOMETRICS SCANNING
LITERATURE REVIEW
WEAK SIGNAL
SNA
EXPERTISE
ADVISORY METHODS
INTERACTION
PARTICIPATORY METHODS
EVIDENCE
EXPLANATORY METHODS
LEGEND
QUALITATIVE
QUANTITATIVE
SEMI-QUANTITATIVE

Figure 1: Foresight Methods by Popper, 2011

3.1 Futures Wheel

The Futures Wheel is a tool used to systematically organize and structure thoughts related to future trends and developments, as demonstrated in figure 2. The use of interconnected lines allows the visualization of interdependencies between causal variables and consequent factors. This method facilitates the generation of diverse ideas concerning potential future advancements.

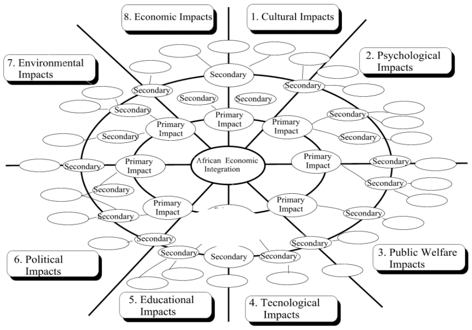


Figure 2: Futures Wheel by Glenn, 202

3.2 SWOT Analysis

SWOT, which stands for internal strengths and weaknesses for the subject, while opportunities, and threats are external, as shown in the figure 3. This method allows the examination of different variables. As well as assess subjects in a nonconventional manner to see them from multiple perspective.

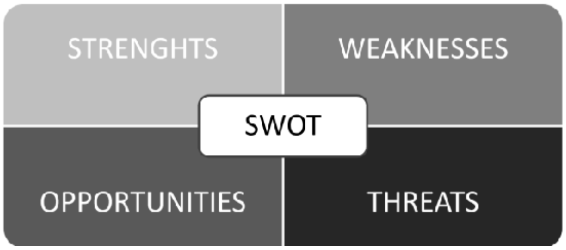


Figure 3: Diagram of classical SWOT analysis by Dean, 2019

3.3 Scenario Planning

This paper defines the driving forces that could have an impact on the future of deepfakes technology using the PESTLE Analysis method, in which two critical uncertainties are selected; based on high impact and high probability to a 2x2 axis to portray two extreme contraries, as demonstrated in figure 4. Four quadrants will result in different landscapes that could affect the police force with a description for each scenario key characteristics. The outcomes of this method conveys possible opportunities and challenges for each scenario to depict the future of deepfakes on the policing sector.

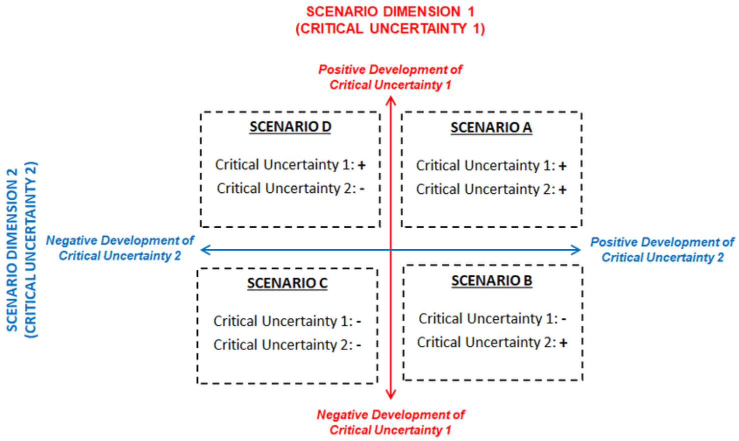


Figure 4: 2x2 Scenario Matrix by Dean, 2019

Chapter 4 - Analysis and Results

4.1 Futures Wheels

First order consequences are direct implications of of deepfakes on law enforcement in which encompass a range of factors including the potential increase in criminal activities involving deepfakes, as shown in figure 5. The strategic utilization of this technology to enhance investigation methods and training as well as the ethical and legal concerns arising from its use. As we delve deeper into the matter we encounter second order consequences that naturally follow from the initial impacts observed at the first level. The proliferation of deepfake technology affects different domains, including; rising pressure on systems due to an increase in deepfake related crimes that requires specialized skills for effective law enforcement against such offenses. Furthermore there is an advancement in crime solving capabilities through investigative tools and techniques. However there is also a looming risk of misuse and public mistrust stemming from concerns. Moving forward to third order consequences we witness societal implications that gradually emerge as a result of the previous levels interconnected outcomes. These implications encompass areas such as legal matters the implementation of new protocols for managing evidence partnerships with the technology sector discussions within society prompting legislative modifications and a potential over reliance on technology, within law enforcement. As well as establishing protocols for dealing with crimes related to deepfakes and adapt policies to ensure fair resource allocation and create ethical guidelines that govern the use of deepfake technology in law enforcement.

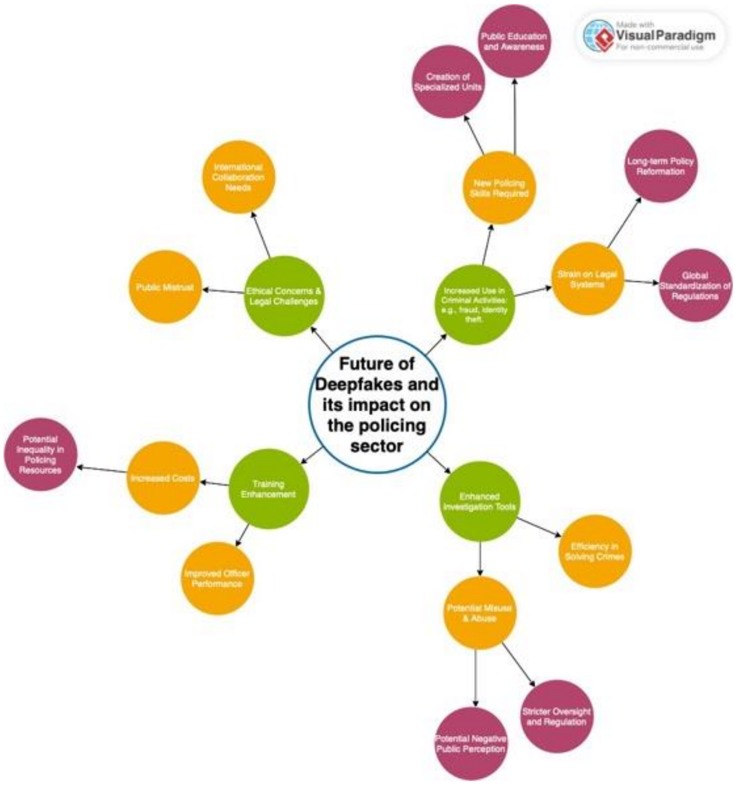

Public Education and Awareness
Made with Visual Paradigm For non-commercial use
Creation of Specialized Units
International Collaboration Needs
New Policing Skills Required
Long-term Policy Reformation
Public Mistrust
Ethical Concerns & Legal Challenges
Increased Use in Criminal Activities: e.g., fraud, identity theft.
Strain on Legal Systems
Global Standardization of Regulations
Future of Deepfakes and its impact on the policing sector
Potential Inequality in Policing Resources
Increased Costs
Training Enhancement
Enhanced Investigation Tools
Efficiency in Solving Crimes
Improved Officer Performance
Potential Misuse & Abuse
Stricter Oversight and Regulation
Potential Negative Public Perception

Figure 5: Future Wheel of Deepfakes and its impact on the policing sector

4.2 SWOT Analysis

Figure 6 highlights the main outcomes of the SWOT analysis method; the sections below will discuss the internal strengths and weaknesses as well as the external opportunities and threats of deepfakes impact on the policing sector.

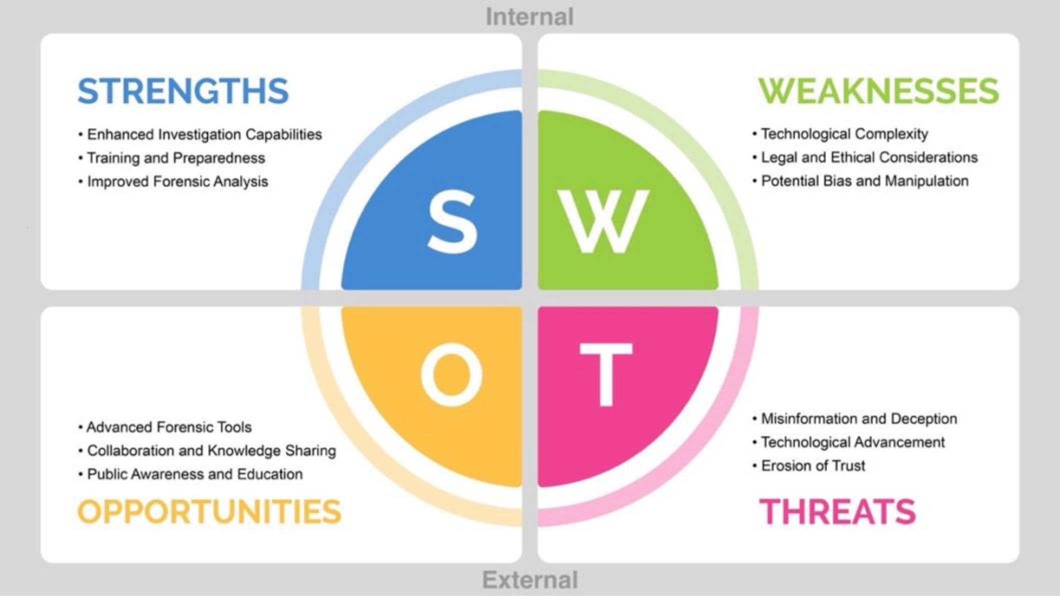

Internal
STRENGTHS
• Enhanced Investigation Capabilities
• Training and Preparedness
• Improved Forensic Analysis
WEAKNESSES
• Technological Complexity
• Legal and Ethical Considerations
• Potential Bias and Manipulation
S
W
O
T
• Advanced Forensic Tools
• Collaboration and Knowledge Sharing
• Public Awareness and Education
OPPORTUNITIES
• Misinformation and Deception
• Technological Advancement
• Erosion of Trust
THREATS
External

Figure 6: SWOT Analysis of Deepfakes and its impact on the policing sector

4.2.1 Internal:

Strengths

According to the European Network of Law Enforcement Agencies (ENLETS) Deepfakes can have the potential to be utilized in a beneficial manner. including; deploying this technology as chatbots for customer and employee's communication. Moreover, object identifications using police’s artificial intelligence systems, within various types of media, such as; photographs, videos, and audio recordings can much more effective with the large datasets used for AI training. It can also help in delivering information to the general public through selecting the language to to individuals' preference by officers who have synthesized the information. Deepfakes allows strategic use of synthetic media in the context of criminal investigations and the methodical gathering of information with regards to ethical considerations. Moreover, there are emerging prospects in enhancing the safety of witnesses and under covering police colleagues through various means such as training, simulated scenarios, debriefing sessions, and trauma processing (Synthetic Reality & Deep Fakes Impact On Police Work, 2021, P. 14).

Weaknesses:

The technology of deepfakes is complex and is facing rapid advancements. Law enforcement may face difficulties in staying aware of the most recent advancements that requires continuous training and investment in specialized technologies to efficiently identify and respond deepfakes. Concerns about ethical and legal matters are raised by the usage of deepfakes in the policing industry. Therefore, ensure that the use of deepfakes is in accordance with privacy legislation to protect individual rights and adhere to ethical principles. However, failing to adhere to this can affect public's trust and potentially result in legal issues. The use of deepfakes can potentially have bias and manipulation into investigation processes. If not subjected to diligent monitoring and strict control measures, the potential misuse of deepfakes has the capacity to exert influence on public perceptions, obstruct the administration of justice, and disseminate false information. Hence, this could result in unjust compromised investigative processes and consequences.

4.2.2 External

Opportunities

Law enforcement has several opportunities with the development of advanced deepfake detection and verification tools. In which it could enhance the capacity of individuals or organizations through efficient allocation of resources towards research and technology to detect, evaluate, and verify manipulated media, thus strengthening investigation proficiencies. The issue of deepfakes can foster the sharing of knowledge, expertise, and resources through collaboration with academic institutions, and technology companies. Moreover, collaborating with external stakeholders can have the allow collective devising and refining best practices, methodologies, and further echnological advancements. Deepfakes can also raise public awareness regarding the threats and consequences of manipulated media. The public can be equipped with necessary skills to evaluate digital content through public education initiatives to make them more resilient to combat disinformation and the erosion of trust.

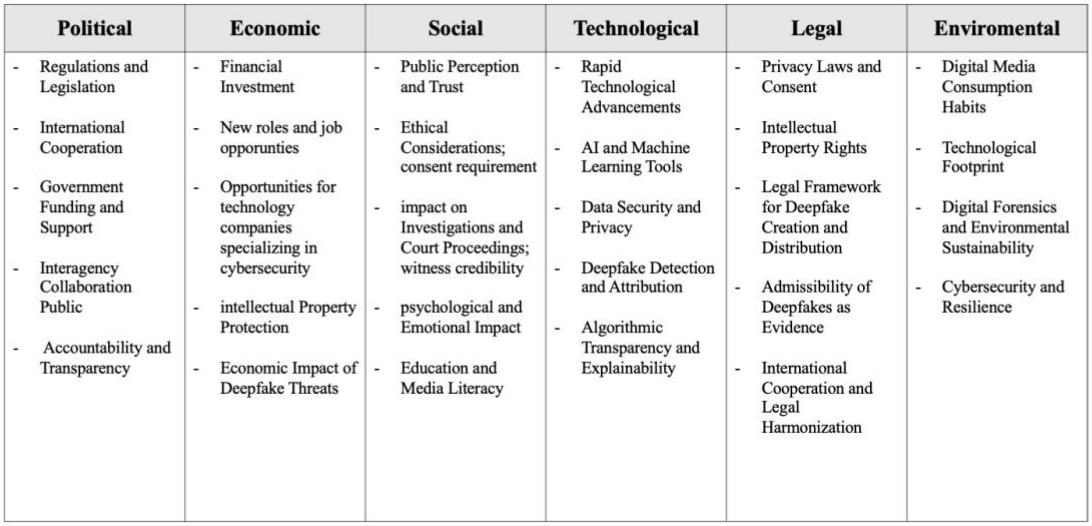
Threats

Individuals' perceptions of authority and the media environment is highly influenced by the the increasing accessibility of disinformation and deepfakes and poses many threats. Authority's trust may be hindered due to the lack of people's trust. Also, people can have societal confusion regarding the credibility of information sources, it is when individuals stop from having a collective understanding of reality with different information. This scenario is occasionally labeled as an 'information apocalypse' or 'reality apathy'. Individuals need to have an understanding of this manipulation and be adequately equipped to address this issue, in order to identify between the safe and harmful application of this technology. The increased use of deepfake technology has the potential to enable a range of criminal activities, such as; online harassment and humiliation of individuals, fraud and schemes, t document forgery, the creation of false online identities, non-consensual pornography, the exploitation of children the falsification or manipulation of electronic evidence in criminal justice inquiries, the disruption of financial markets, the dissemination of disinformation and manipulation of public sentiment, the reinforcement of extremist or terrorist group narratives, and an escalation of social unrest and political polarization (Europol, 2022).

4.3 Scenario Planning

4.3.1 Pestle Analysis

The PESTLE analysis in table 2 sheds light on the impact of deepfakes, on law enforcement and the factors that contribute to this issue. When it comes to politics, strict regulations, international cooperation and investment in cutting edge technologies all play a role in maintaining privacy and upholding standards to effectively overcome global deepfake related crimes. From economic standpoint resources need to be allocated towards research, training and the development of forensic tools. Leading to the emergence of professional roles like deepfake analysts but also opens up growth opportunities for cybersecurity and artificial intelligence industries. Social factors include the distortion of public perception and undermining trust in the authenticity of evidence. In which, holding initiatives that promote media literacy enhances transparency and provide support for those affected by this issue. Technological factors involve staying updated with the advancements is crucial along with advocating for the use of intelligence solutions for detection purposes while prioritizing transparency. Legal factors are also vital to ensure compliance with privacy laws, consent standards, intellectual property rights restrictions and international legislative harmonization efforts. Lastly environmental factors include substantiality considerations such, as energy usage and the incorporation of eco technology that emerge from studying and developing deepfake technologies. Additionally giving importance to prioritizing cybersecurity measures and implementing resilience methods can help reduce the risks associated with cyberattacks.

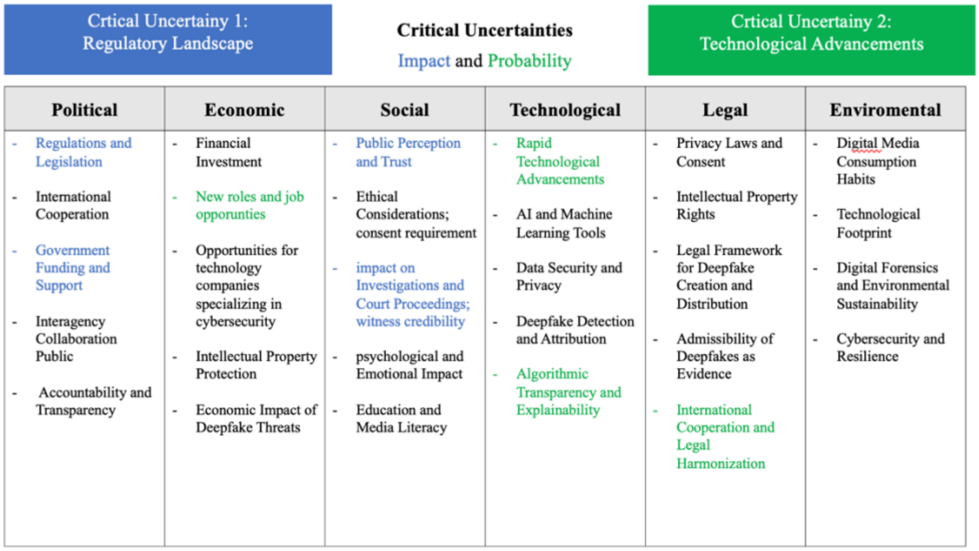


Political	Economic	Social	Technological	Legal	Enviromental
- Regulations and Legislation - International Cooperation - Government Funding and Support - Interagency Collaboration Public - Accountability and Transparency	- Financial Investment - New roles and job opporunties - Opportunities for technology companies specializing in cybersecurity - intellectual Property Protection - Economic Impact of Deepfake Threats	- Public Perception and Trust - Ethical Considerations; consent requirement - impact on Investigations and Court Proceedings; witness credibility - psychological and Emotional Impact - Education and Media Literacy	- Rapid Technological Advancements - AI and Machine Learning Tools - Data Security and Privacy - Deepfake Detection and Attribution - Algorithmic Transparency and Explainability	- Privacy Laws and Consent - Intellectual Property Rights - Legal Framework for Deepfake Creation and Distribution - Admissibility of Deepfakes as Evidence - International Cooperation and Legal Harmonization	- Digital Media Consumption Habits - Technological Footprint - Digital Forensics and Environmental Sustainability - Cybersecurity and Resilience

Table 2: PESTLE Analysis of Deepfakes

4.3.2 Critical Uncertainties

The Driving forces that could possibly impact the deepfakes on the policing sector has been selected using the PESTLE Analysis method, as shown in table 3. The critical uncertainties were chosen based on two factors; their level of impact and uncertainty. Several elements in the analysis are interdependent and are leading to a multi-faceted uncertainty, leading to a cluster of different domains that results in either a high impact or a high uncertain factor. The following section will discuss each uncertainty thoroughly.



Crtical Uncertainy 1:
Regulatory Landscape

Critical Uncertainties
Impact and Probability

Crtical Uncertainy 2:
Technological Advancements

Political	Economic	Social	Technological	Legal	Enviromental
- Regulations and Legislation - International Cooperation - Government Funding and Support - Interagency Collaboration Public - Accountability and Transparency	- Financial Investment - New roles and job opporunties - Opportunities for technology companies specializing in cybersecurity - Intellectual Property Protection - Economic Impact of Deepfake Threats	- Public Perception and Trust - Ethical Considerations; consent requirement - impact on Investigations and Court Proceedings; witness credibility - psychological and Emotional Impact - Education and Media Literacy	- Rapid Technological Advancements - AI and Machine Learning Tools - Data Security and Privacy - Deepfake Detection and Attribution - Algorithmic Transparency and Explainability	- Privacy Laws and Consent - Intellectual Property Rights - Legal Framework for Deepfake Creation and Distribution - Admissibility of Deepfakes as Evidence - International Cooperation and Legal Harmonization	- Digital Media Consumption Habits - Technological Footprint - Digital Forensics and Environmental Sustainability - Cybersecurity and Resilience

Table 3: Critical Uncertainties of Deepfakes

4.3.2.1 Critical uncertainty 1: Regulatory Landscape (Stability vs Chaos)

The effectiveness of regulations in dealing with deepfake related challenges remains uncertain. This uncertainty gives rise to a scenario where we can consider "Stability vs Chaos" in terms of regulations and legislation. In a scenario robust regulations and legislation are put in place ensuring control and mitigation of deepfake risks within the policing sector. However, in a scenario the absence of regulations and inadequate legal frameworks may lead to challenges allowing deepfakes to spread and impede law enforcement efforts.

Factors influencing this uncertainty include establishing frameworks specific to deepfakes that comprehensively address their potential harms. Moreover, factors such, as the speed at which laws are enacted the coordination between jurisdictions and the ability to adapt existing laws to technological challenges all have an impact on how effective regulatory responses are. Stakeholder cooperation also play an important role in influencing the stability of regulations. In order to develop and implement regulations for governments, law enforcement agencies, technology companies and civil society organizations will need collaborate effectively. The strength of the landscape depends on their ability to bring together perspectives, align interests and foster collaboration. International cooperation is also vital since deepfake threats can exceed borders. The effectiveness of addressing these challenges depends on factors like countries willingness to collaborate establishing mechanisms for sharing information and harmonizing frameworks across jurisdictions. Policymakers and regulators awareness and knowledge regarding deepfake technology and will require a good understanding of the subject. Furthermore, public awareness and perception play a role in shaping the need to regulate deepfakes. Becoming aware of the risks associated with deepfakes and their potential impact on society could influences decision makers motivation to address challenges. Various factors, including the extent of media coverage educational efforts and campaigns to engage the public contribute to shaping awareness and perception. These factors in turn have an impact, on how regulations are made and implemented.

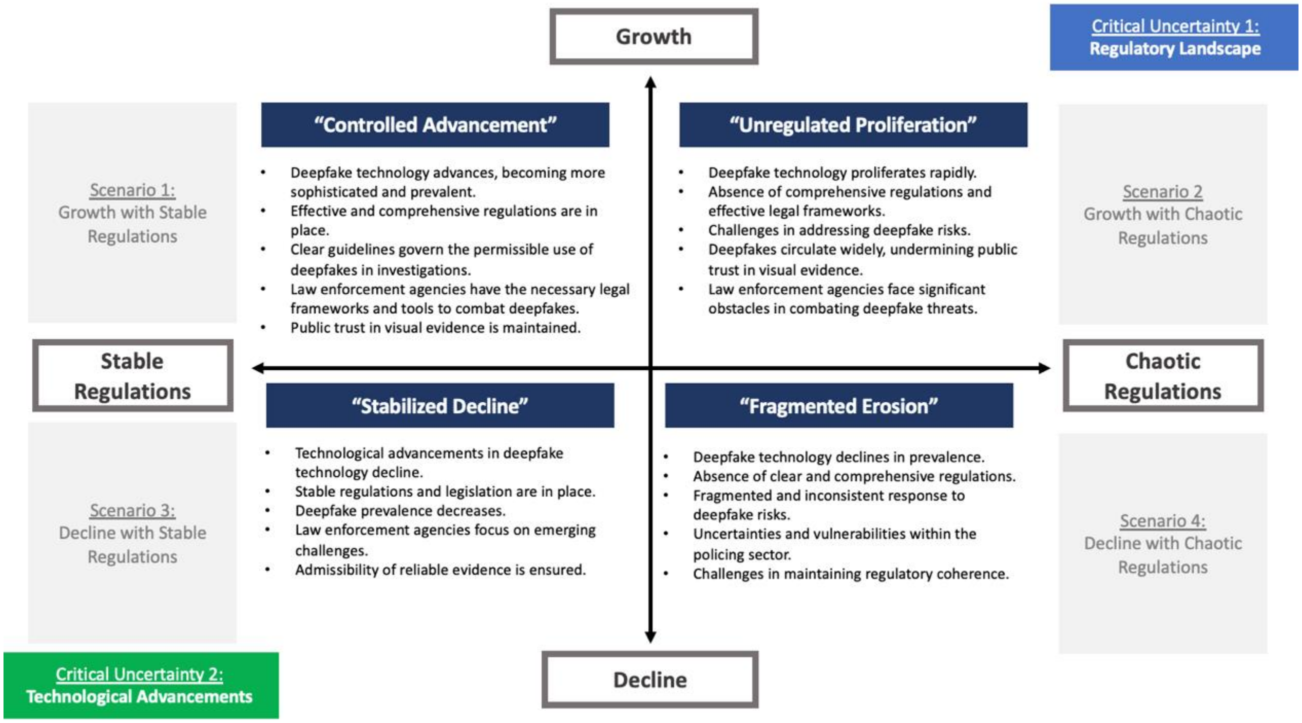
4.3.2.2 Critical uncertainty 2: Technological Advancements (Growth vs Decline)

The speed and direction of advancements in deepfake technology is all also a critical uncertainty. It can be represented by a scenario matrix called "Growth vs Decline " which reflects the sophistication and prevalence of deepfakes. In one scenario we may witness growth and advancement in technology that makes it more accessible while becoming harder to detect. This will have an increased challenges for law enforcement. In another scenario significant advancements in detection and prevention techniques could lead to a decline in the effectiveness and prevalence of deepfakes in the future.

Factors that influence the speed and direction of advancements in deepfake technology, are; The level of investment and focus dedicated to deepfake research and development by academia, industry and technology companies has an impact on the speed and sophistication of progress. Factors like funding availability, talent procurement and collaboration play roles, in shaping the advancement of deepfake technology. Deepfake technology creators continuously try to outsmart developers working on detection methods. This competition drives innovation as counter innovation influencing how rapidly deepfake technology evolves. These factors include the resources and expertise, on both sides the effectiveness of detection methods and the adaptability of creation techniques. The accessibility of tools and techniques for creating deepfakes also has an impact on it progression and advancements. The availability of user tools, algorithms and techniques can greatly influence how widespread and sophisticated deepfake content becomes. Moreover, factors like open source deepfake tools, online tutorials and easy to use creation software all play a role in determining accessibility. Technological breakthroughs also have an effect on deepfake capabilities, as advancements in intelligence machine learning, computer vision and related fields can enhance the realism of deepfakes while making them harder to detect. In addition, breakthrough research findings, technological collaborations and advancements in related fields all contribute to these developments. Researchers, technology companies, law enforcement agencies and policymakers' action's, against the challenges presented by deepfakes can shape the trajectory of advancements in this area. The development and adoption of methods to detect and counter deepfakes, along with attribution techniques have the potential to slow down the growth and use of deepfakes. On the hand if there is a lack of strong response it could allow deepfake technology to advance without constraints. The response and countermeasures against deepfakes are influenced by factors such as research investment, collaboration among stakeholders, regulatory frameworks and public awareness initiatives.

4.3.3 Scenario Matrix

Figure 7 illustrates the four different scenarios using the selected critical uncertainties, the sections below will discuss each scenario's key characteristics, opportunities and challenges, as well as the recommended strategic response, it will finally give each scenario a name to help differentiate them and highlight the outcomes from each quadrant.



"Controlled Advancement"

- Deepfake technology advances, becoming more sophisticated and prevalent.
- Effective and comprehensive regulations are in place.
- Clear guidelines govern the permissible use of deepfakes in investigations.
- Law enforcement agencies have the necessary legal frameworks and tools to combat deepfakes.
- Public trust in visual evidence is maintained.

"Unregulated Proliferation"

- Deepfake technology proliferates rapidly.
- Absence of comprehensive regulations and effective legal frameworks.
- Challenges in addressing deepfake risks.
- Deepfakes circulate widely, undermining public trust in visual evidence.
- Law enforcement agencies face significant obstacles in combating deepfake threats.

"Stabilized Decline"

- Technological advancements in deepfake technology decline.
- Stable regulations and legislation are in place.
- Deepfake prevalence decreases.
- Law enforcement agencies focus on emerging challenges.
- Admissibility of reliable evidence is ensured.

"Fragmented Erosion"

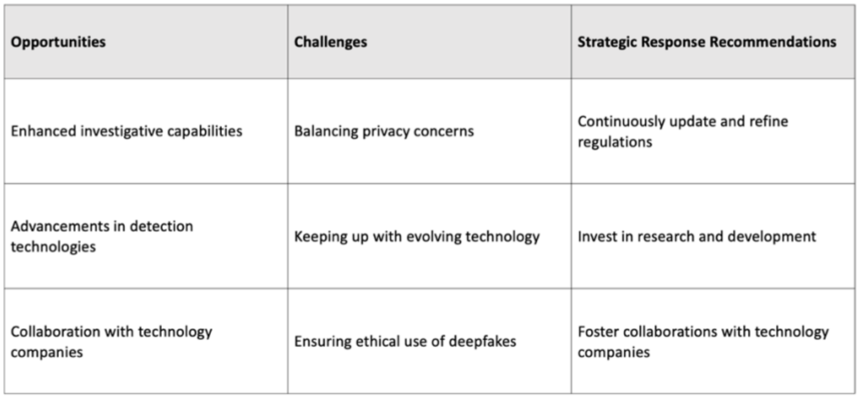
- Deepfake technology declines in prevalence.
- Absence of clear and comprehensive regulations.
- Fragmented and inconsistent response to deepfake risks.
- Uncertainties and vulnerabilities within the policing sector.
- Challenges in maintaining regulatory coherence.

Figure 7: Future of Deepfakes Scenario

4.3.3.1 Scenario 1: Controlled Advancement (Growth with Stable Regulations)

Key Characteristics

In this scenario the continuous development and evolution of deepfake technology indicate its increasing level of detail and usage. However, the implementations of laws and regulations to effectively address the challenges that arise from this evolving deepfake landscape. Clear guidelines are in place to regulate the use of deepfakes in practices ensuring compliance with privacy laws and ethical standards. Detecting, analyzing, and combating deepfakes properly is made possible by law enforcement agencies' access to the necessary frameworks and tools. A stable regulatory environment offers the strength and resources to effectively manage risks, maintain public confidence, and protect the integrity of investigations and legal procedures. Table 4 summarize and highlights the main points discussed in the opportunities and challenges section, as well as the recommended strategic response.



Opportunities	Challenges	Strategic Response Recommendations
Enhanced investigative capabilities	Balancing privacy concerns	Continuously update and refine regulations
Advancements in detection technologies	Keeping up with evolving technology	Invest in research and development
Collaboration with technology companies	Ensuring ethical use of deepfakes	Foster collaborations with technology companies

Table 4: Opportunities, challenges and strategic recommendation of Scenario One

Opportunities

The opportunities in this scenario are; having the capacity to support investigations by improving the processes and gathering evidence through the appropriate use of deepfakes. Moreover, capabilities for identifying and attributing deepfakes have been improved with the significant technological advancements. Other opportunities include ongoing progress in identifying and tracking manipulated media through sophisticated detection algorithms that provides law enforcement authorities to successfully trace back information to its origin. Additionally, collaboration between technology companies and law enforcement organizations holds promise for both parties by facilitating efforts, in creating and employing tools and techniques to combat deepfakes across different institutions.

Challenges

The challenges in this scenario are; finding the balance between addressing privacy concerns and effectively employing this technology. Tackling this issue requires the establishment of guidelines and legal frameworks that enable the use of deepfakes while protecting individuals' privacy rights. Also, there is a challenge of keep using with the evolving field of deepfake technology and possibility the allocation resources for research and development.

Strategic Recommendations

In this scenario it is recommended to review and revise rules according to the advancements in deepfake technology to ensure effectiveness in dealing with emerging challenges. Additionally investing resources into research and development initiatives focused on improving detection methods, attribution approaches and preventive technologies is. Collaborating with businesses can be beneficial as their specialized knowledge and abundant resources can contribute to creating technologies, for identifying deepfakes. Furthermore, establishing and enforcing processes that encourage transparency and accountability in using deepfakes for purposes. This may involve implementing reporting obligations or setting up inspection committees.

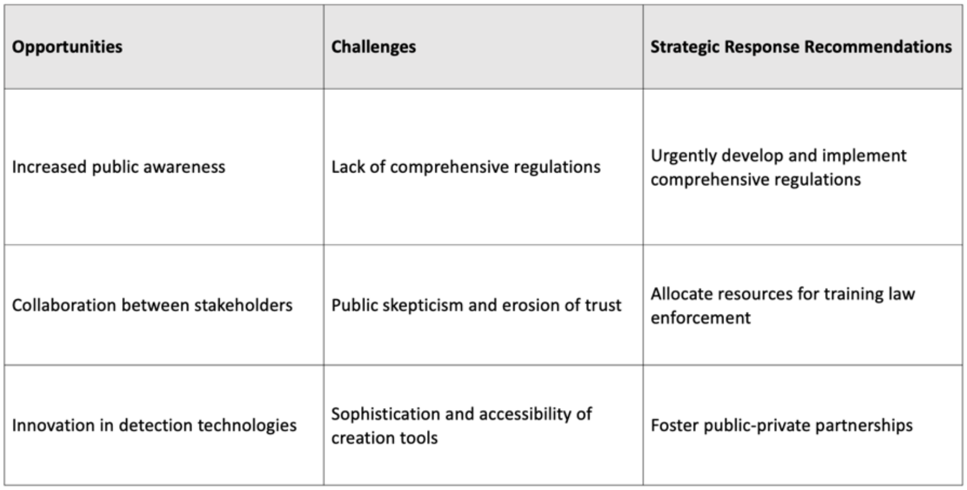
Scenario Name

This scenario is called "Controlled Advancement" as it depicts an advancement in deepfake technology while still adhering to regulations and despite the growth of deepfakes the police have established a framework that guarantees control and accountability.

4.3.3.2 Scenario Two: Unregulated Proliferation (Growth with Chaotic Regulations)

Key Characteristics

In this scenario the rapid proliferation of deepfake technology surpasses the pace of efforts. The chaotic landscape created by the lack of regulations and effective legal frameworks presents challenges to law enforcement agencies when dealing with deepfakes. The absence of guidelines hinders their ability to address the risks associated with deepfakes resulting in increased vulnerabilities and obstacles. With control measures in place deepfakes circulate widely eroding trust in visual evidence and undermining the integrity of the justice system. Law enforcement agencies encounter hurdles in their tackling deepfake threats due to this regulatory environment. Table 5 summarize and highlights the main points discussed in the opportunities and challenges section, as well as the recommended strategic response.



Opportunities	Challenges	Strategic Response Recommendations
Increased public awareness	Lack of comprehensive regulations	Urgently develop and implement comprehensive regulations
Collaboration between stakeholders	Public skepticism and erosion of trust	Allocate resources for training law enforcement
Innovation in detection technologies	Sophistication and accessibility of creation tools	Foster public-private partnerships

Table 5: Opportunities, challenges and strategic recommendation of Scenario Two

Opportunities

The opportunities in this scenario are; increasing awareness among the public about the risks of deepfakes can help foster an understanding of why regulation and countermeasures are necessary. Also, to create regulations, innovative detection technologies, and efficient response methods, law enforcement agencies, legislators, and technological professionals must work collaboratively. The growing threat presented by deepfakes can drive innovation in detection and prevention technologies leading to reliable tools.

Challenges

The challenges in this scenario are; the lack of regulations that hinders law enforcement efforts to effectively tackle deepfake threats and hold offenders accountable. Further challenges include, doubt and erosion of trust in evidence. The widespread circulation of deepfakes affects public trust in visual evidence and credibility of investigations and court proceedings. The increasing accessibility and sophistication of creation tools empower individuals to produce more deepfakes.

Strategic Recommendations

In this scenario it is recommended to develop and implement regulations through establishing regulations and legal frameworks to address the creation, distribution and misuse of deepfakes to ensure control and mitigation. Also, allocating resources for training officers to equip them with the knowledge and skills to detect, analyze and investigate deepfakes effectively. Moreover, fostering partnerships is essential, encouraging collaboration, between law enforcement and technology companies will enable the development of advanced deepfake detection technologies. Additionally educating the public is important, launching public awareness campaigns will help individuals recognize information empowering them to differentiate between content and manipulated deepfakes.

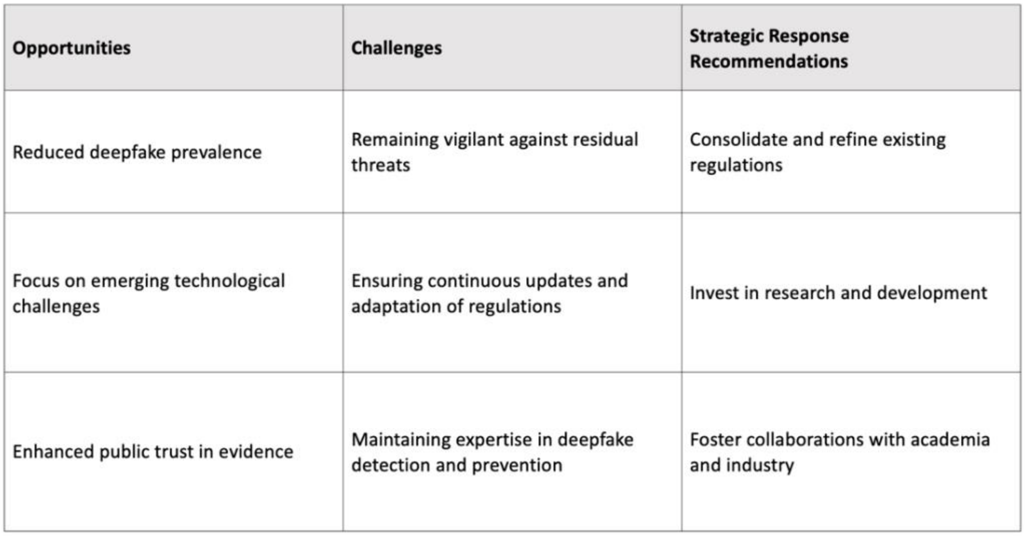
Scenario Name

This scenario is called "Unregulated Proliferation" since it portrays a situation where deepfake technology rapidly spreads without oversight. In which, deepfakes are being widely circulated and creating difficulties for law enforcement because there are no clear guidelines or comprehensive regulations in place.

4.3.3.3. Scenario 3: Stabilized Decline (Decline with Stable Regulations)

Key Characteristics

In this scenario, advancements in deepfake technology have decreased, resulting in a reduction in the frequency and complexity of deepfakes. Due to regulations and effective legislation the risks associated with deepfakes are being controlled and mitigated within the policing sector. Law enforcement agencies can now shift their focus from dealing with deepfakes to addressing emerging challenges. The regulatory framework ensures that reliable evidence remains admissible thereby upholding the integrity of investigations and court proceedings. As incidents related to deepfakes become common public trust in visual evidence is gradually being restored. Table 6 summarize and highlights the main points discussed in the opportunities and challenges section, as well as the recommended strategic response.



Opportunities	Challenges	Strategic Response Recommendations
Reduced deepfake prevalence	Remaining vigilant against residual threats	Consolidate and refine existing regulations
Focus on emerging technological challenges	Ensuring continuous updates and adaptation of regulations	Invest in research and development
Enhanced public trust in evidence	Maintaining expertise in deepfake detection and prevention	Foster collaborations with academia and industry

Table 6: Opportunities, challenges and strategic recommendation of Scenario Three

Opportunities

The opportunities in this scenario are; allocating resources towards tackling emerging technological threats due to the decline in deepfake challenges. Also, opportunities to redirect resources towards emerging challenges, as the risks associated with deepfakes decrease law enforcement agencies can prioritize addressing other emerging challenges in different domains. In addition, restored trust in visual evidence due to reduced prevalence of deepfakes, as the occurrence of deepfakes becomes less frequent public confidence, in evidence can gradually be rebuilt. This contributes significantly to maintaining the integrity of investigations and court proceedings.

Challenges

The challenges in this scenario are; remaining vigilant against any lingering deepfake threats, despite a decrease in the dominance of deepfakes. As well as updating and adapting regulatory frameworks to keep up with the ever-evolving technological landscape and effectively tackle emerging challenges. Law enforcement could also challenges in maintaining their expertise and knowledge in detecting and preventing deepfakes during periods of decreased prevalence to be prepared for potential resurgences or new types of threats.

Strategic Response

In this scenario it is recommended to consolidate and refine existing regulations and legal frameworks to ensure their relevance and adaptability. Additionally investing in research and development efforts to stay of potential resurgences or new forms of deepfake threats. Collaboration with institutions and industry partners can help develop advanced methods for detecting deepfakes by leveraging their expertise and resources. Sustaining public awareness campaigns remains vital to educate the public about the risks associated with deepfakes and strategies, for mitigating them even when prevalence declines.

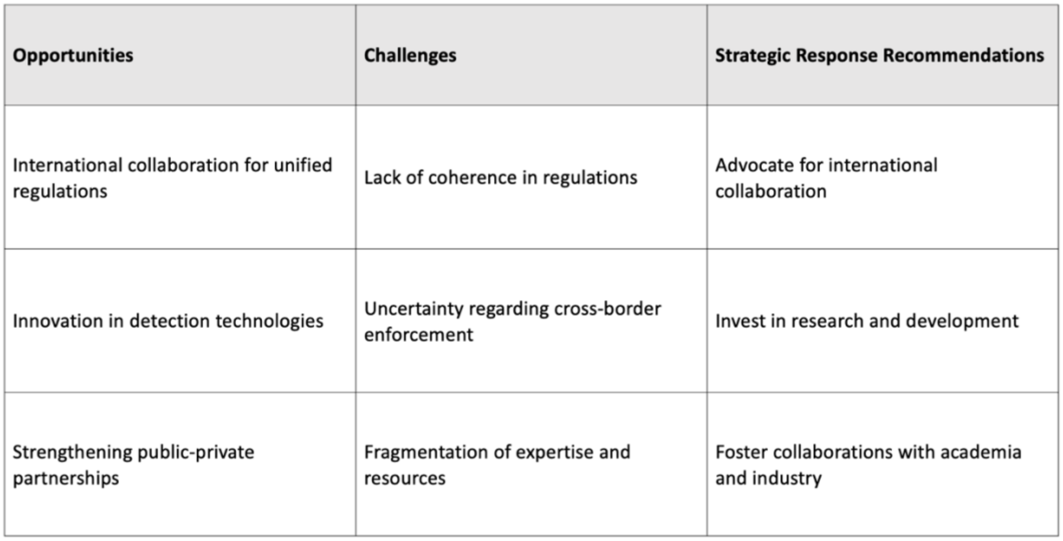
Scenario Name

This scenario is called "Stabilized Decline" as it represents a scenario where the use of deepfake technology decreases and regulations are firmly established. The name reflects the idea that the deepfake landscape has become more stable due to regulations resulting in a decline.

4.3.3.4 Scenario Four: Fragmented Erosion (Decline with Chaotic Regulations)

Key Characteristics

In this scenario the prevalence of deepfake technology decreases. The lack of comprehensive regulations poses challenges, for law enforcement agencies. Without frameworks in place addressing deepfake risks becomes difficult and inconsistent. The absence of guidelines on creating, distributing and using deepfakes as evidence leads to uncertainties and potential vulnerabilities within the policing sector. While the occurrence of deepfakes diminishes, the lack of coherence hinders control and mitigation of the associated challenges. Law enforcement agencies encounter difficulties in navigating through these regulations, which could potentially affect the integrity and reliability of investigations. Table 7 summarize and highlights the main points discussed in the opportunities and challenges section, as well as the recommended strategic response.



Opportunities	Challenges	Strategic Response Recommendations
International collaboration for unified regulations	Lack of coherence in regulations	Advocate for international collaboration
Innovation in detection technologies	Uncertainty regarding cross-border enforcement	Invest in research and development
Strengthening public-private partnerships	Fragmentation of expertise and resources	Foster collaborations with academia and industry

Table 7: Opportunities, challenges and strategic recommendation of Scenario Four

Opportunities

The opportunities in the scenario are; promote collaboration to establish regulatory frameworks, foster collaborative efforts with stakeholders to develop regulatory frameworks that can effectively address deepfake challenges across borders and ensure consistent enforcement. Encourage advancements in deepfake detection and attribution technologies to tackle challenges, foster innovation in technologies that can detect and attribute deepfakes. Other opportunities include; enhancing partnerships and strengthening collaborations between public and private entities to collectively combat risks associated with deepfakes by leveraging their respective expertise and resources for more effective response strategies.

Challenges

The challenges in this scenario are; lack of coherence and consistency in regulations that hinders control and mitigation. The absence of consistent regulations, across jurisdictions can create obstacles in effectively controlling and mitigating risks arising from deepfakes resulting in an inconsistent response. The lack of coordination in frameworks can create challenges for enforcing laws across borders and affects the sharing of crucial information concerning deepfake threats.

Strategic Response

In this scenario it is recommended to encourage collaboration and cooperation to establish frameworks that harmonize legal standards to facilitate cross border enforcement efforts and to promote the sharing of information. Additionally allocating resources towards research and development initiatives focused deepfake detection and attribution technologies will help combat a range of deepfake threats. Moreover, strengthening partnerships between entities, private organizations and academia through leveraging their combined expertise.

Scenario Name

This scenario is called "Fragmented Erosion" since it highlights the response to deepfake risks which could potentially affect control measures aimed at mitigating their impact. The absence of a framework creates uncertainties within the policing sector leading to vulnerabilities.

Chapter 5 - Conclusion

5.1 Conclusion

This paper has delved into the future of deepfakes and its possible implications on the policing sector and law enforcement. It also provided a comprehensive overview of the existing literature and the academic efforts to address this issue, it highlighted the definition of deepfakes, history, its formation, detection methods and its impact on the policing sector. Furthermore, this research utilized future foresight methods to illustrate the future outlook of deepfakes, the first tool was the futures wheel in which helped with mapping the direct and indirect consequences of the issue and presenting connections that can aid with decision making. Second tool was a SWOT analysis that studied the internal strengths and weakness, and the external opportunities and threats, this method allows it user to think in a counter intuitive manner that broadens one perspective and eventually reveal an unexpected outcome that can be considered into strategies. The third tool was the scenario planning, this method consisted of employing the PESTLE analysis and selecting two critical uncertainties that has the highest impact and uncertainty, that led to two possible contrasting outcomes with four possible futures of deepfakes, each scenario was analyzed in terms of highlighting its key characteristics, opportunities, challenges, strategic recommendation as well as giving each scenario a name. overall, this paper provided insight and perspective on the possible future outcomes of deepfakes and it recognizes its potential as threat and opportunity for the safety and security of citizens.

5.2 Recommendations

The study has previously discussed possible mitigation and preventive measure to tackle deepfakes, this section will highlight the recommendations drawn from the analysis of the methodologies used in this paper.   Firstly, it recommends the regular update of rules and law to regulate the use of deepfakes, as it has progressed and developed rapidly. In addition, it stresses on the allocation of resources and funding of research and development to further investigate the evolving nature of the issue. Funding can also play a role in providing training officers to detect deepfakes. Second, strengthening collaborations with external technological partners can aid in the development of innovative solutions and sharing of knowledge, the paper also recommends collaborations with other nations for possible global deepfakes misuse to unify a legal framework that can used a manual for dealing with this issue. Lastly, raising the public’s awareness of deepfakes can help them in its detection and the risk associated with it use, this could in turn maintain the trust and confidence in the police.

References

Albahar, M.A., & Almalki, J. (2019). DEEPFAKES: THREATS AND COUNTERMEASURES SYSTEMATIC REVIEW.

Afchar, D., Nozick, V., Yamagishi, J., & Echizen, I. (2018). MesoNet: A Compact Facial Video Forgery Detection Network. *2018 IEEE International Workshop on Information Forensics and Security (WIFS)*, 1–7.

Boylan, J. F. (2018, October 17). Opinion | Will Deep-Fake Technology Destroy Democracy? *The New York Times*. https://www.nytimes.com/2018/10/17/opinion/deep-fake-technology-democracy.html

B. J. Siekierski. (2019) , Deep Fakes: What Can be Done About Synthetic Audio and Video. Library of Parliament.https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/InBriefs/PDF/2019-11-e.pdf

Cole, S. (2017, December 12). AI-Assisted Fake Porn Is Here and We're All Fucked. Retrieved November 5, 2021, from Vice website: https://www.vice.com/en/article/gydydm/gal-gadot-fake-ai-porn

Chan, C., Ginosar, S., Zhou, T., & Efros, A. (2019). Everybody Dance Now. *2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, 5932–5941. https://doi.org/10.1109/ICCV.2019.00603

Chesney, Robert, and Danielle Keats Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *SSRN Electronic Journal*, 2018. https://doi.org/10.2139/ssrn.3213954.

Chawla, R. (2019). Deepfakes : How a pervert shook the world. *International Journal for Advance Research and Development, 4*, 4-8.

Dean, Marco. (2019). Scenario Planning: A Literature Review. 10.13140/RG.2.2.12629.24802.

Drew. (2018). *Scarlett Johansson on fake AI-generated sex videos: 'Nothing can stop someone from cutting and pasting my image.'* The Washington Post. https://www.washingtonpost.com/technology/2018/12/31/scarlett-johansson-fake-ai-generated-sex-videos-nothing-can-stop-someone-cutting-pasting-my-image/

D. Güera and E. J. Delp, "Deepfake Video Detection Using Recurrent Neural Networks," 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, New Zealand, 2018, pp. 1-6, doi: 10.1109/AVSS.2018.8639163.

Europol (2022), Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg.

Gardiner, N. (2019). Facial re-enactment, speech synthesis and the rise of the Deepfake.

Glenn, J. C. (2021). *The Futures Wheel*.

Güera, D., & Delp, E. J. (2018). Deepfake Video Detection Using Recurrent Neural Networks. *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, 1–6.

Inayatullah, Sohail. (2019). Causal Layered Analysis A Four-Level Approach to Alternative Futures RELEVANCE AND USE IN FORESIGHT. Futuribles.

Khalil, Hady A., and Shady A. Maged. "Deepfakes Creation and Detection Using Deep Learning."

In *2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC)*, 1–4, 2021. https://doi.org/10.1109/MIUCC52538.2021.9447642.

Koopman, Marissa & Macarulla Rodriguez, Andrea & Geradts, Zeno. (2018). Detection of Deepfake Video Manipulation.

Korshunov, Pavel, and S. Marcel. "DeepFakes: A New Threat to Face Recognition? Assessment and Detection." *ArXiv*, December 20, 2018. https://www.semanticscholar.org/paper/6eb0b0ddc1f87df9c74259feef5c6ccafc334a8f.

Levine, T.R., 'Truth-Default Theory (TDT): A Theory of Human Deception and Deception Detection' Journal of Language and Social Psychology, 2014, pp. 378-392., https://www. researchgate.net/publication/273593306_Truth-Default_Theory_TDT_A_Theory_of_ Human_Deception_and_Deception_Detection.

Maras, Marie-Helen, and Alex Alexandrou. "Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos." *The International Journal of Evidence & Proof* 23, no. 3 (July 1, 2019): 255–62. https://doi.org/10.1177/1365712718807226.

Malik, K.M., Malik, H., & Baumann, R. (2019). Towards Vulnerability Analysis of Voice-Driven Interfaces and Countermeasures for Replay Attacks. *2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, 523-528.

Malik, K.M., Javed, A., Malik, H., & Irtaza, A. (2020). A Light-Weight Replay Detection Framework For Voice Controlled IoT Devices. *IEEE Journal of Selected Topics in Signal Processing, 14*, 982-996.

Matern, F., Riess, C., & Stamminger, M. (2019). Exploiting Visual Artifacts to Expose Deepfakes and Face Manipulations. *2019 IEEE Winter Applications of Computer Vision Workshops (WACVW)*, 83-92.

McAfee, 'The Deepfakes Lab: Detecting & Defending Against Deepfakes with Advanced AI', 2020, accessed on 10 March 2022, https://www.mcafee.com/blogs/enterprise/securityoperations/the-deepfakes-lab-detecting-defending-against-deepfakes-with-advanced-ai.

Michigan State University, MSU, ‘Facebook develop research model to fight deepfakes’, 2021, accessed on 10 March 2022, https://msutoday.msu.edu/news/2021/deepfake-detection.

Nazarko, Joanicjusz & Ejdys, Joanna & Halicka, Katarzyna & Magruk, Andrzej & Nazarko, Łukasz & Skorek, Adam. (2017). Application of Enhanced SWOT Analysis in the Future-oriented Public Management of Technology. Procedia Engineering. 182. 482-490. 10.1016/j.proeng.2017.03.140.

Nguyen, T. T., Nguyen, Q. V. H., Nguyen, C. M., Nguyen, D., Nguyen, D. T., & Nahavandi, S. (2021). Deep Learning for Deepfakes Creation and Detection: A Survey. *ArXiv:1909.11573 [Cs, Eess]*. Retrieved from http://arxiv.org/abs/1909.11573

Łukasz & Skorek, Adam. (2017). Application of Enhanced SWOT Analysis in the Future-oriented Public Management of Technology. Procedia Engineering. 182. 482-490. 10.1016/j.proeng.2017.03.140.

Öhman, Carl. “Introducing the Pervert’s Dilemma: A Contribution to the Critique of Deepfake Pornography.” *Ethics and Information Technology* 22, no. 2 (June 2020): 133–40. https://doi.org/10.1007/s10676-019-09522-1.

Popper, R. (2011). The Diamond. Future Diamond. Retrieved April 23, 2023, from http://www.futuresdiamond.com/en/the-diamond

Stover, D. (2018). Garlin Gilchrist: Fighting fake news and the information apocalypse. *Bulletin of the Atomic Scientists*, *74*, 283 - 288.

Tammekänd, J., Thomas, J., & Peterson, K. (2020). *Deepfakes 2020: The tipping point*.

UCL. (2020, August 4). ‘Deepfakes’ ranked as most serious AI crime threat. Retrieved November 17, 2021, from UCL News website: https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat

Venema, A. E., & Geradts, Z. J., ‘Digital Forensics Deepfakes and the Legal Process,’ 2020, TheSciTechLawyer, 16(4), pp. 14-23.

Wagner, Travis L., and Ashley Blewer. “‘The Word Real Is No Longer Real’: Deepfakes, Gender, and the Challenges of AI-Altered Video.” *Open Information Science* 3, no. 1 (January 1, 2019): 32–46. https://doi.org/10.1515/opis-2019-0003.

Yang, Xin, Yuezun Li, and Siwei Lyu. “Exposing Deep Fakes Using Inconsistent Head Poses.” arXiv, November 13, 2018. http://arxiv.org/abs/1811.00661.

Zhao, Bo, Shaozeng Zhang, Chunxue Xu, Yifan Sun, and Chengbin Deng. “Deep Fake Geography? When Geospatial Data Encounter Artificial Intelligence.” *Cartography and Geographic Information Science* 48, no. 4 (July 4, 2021): 338–52. https://doi.org/10.1080/15230406.2021.1910075.