The news media coverage of organisational deepfake risks

A qualitative thematic analysis of the Financial Times

Student Name: Selena Yip Hui Li

Student Number: 520217

Supervisor: Dr. Charlotte Bruns

Master Media Studies - Media & Business

Erasmus School of History, Culture and Communication

Erasmus University Rotterdam

Master's Thesis

June 2023

THE NEWS MEDIA COVERAGE OF ORGANISATIONAL DEEPFAKE RISKS: A QUALITATIVE THEMATIC ANALYSIS OF THE FINANCIAL TIMES

ABSTRACT

In recent times, extensive advancements in artificial intelligence have brought about influential developments. One of these developments includes deepfakes, a by-product of artificial intelligence applications that manipulate images and videos to develop authentic-looking fake videos. While deepfake do offer benefits, concerns about their consequences have gained significant attention within the mainstream news media. Existing academic literature analysing deepfake coverage within the news media predominantly discusses the individual and societal level while neglecting the organisational level. This leaves a significant research gap that this study seeks to investigate. Given the threats that deepfakes pose on the organisational level, it is crucial to examine the deepfake threat for organisations. However, existing studies found that when analysing deepfakes, it is essential to investigate the phenomena on the individual, organisational, and societal risks level. Hence despite this study's focus on the organisational level, it will also explore the individual and societal levels to provide a comprehensive understanding of the topic. As such, this study will examine the following research question: How does the *Financial Times* address the risks of deepfakes for companies? To answer the research question, a qualitative approach was employed, using thematic analysis as a method of data analysis. The data collection process collected and analysed 55 articles from the *Financial Times*. From the analysis, a total of three main themes were derived. Firstly, the manipulation themes explore the *Financial Times's* discussion on how deepfakes are used to exploit people and information. The second theme, security risks, discusses the possible risks and vulnerabilities deepfake poses to organisations, individuals, and society. The last theme is the regulation theme which provides insights into the actions and policy measures discussed within the *Financial Times* articles that could mitigate the risks associated with deepfakes. These themes indicate discrepancies in the reporting of the *Financial Times's* coverage of the deepfake risk levels. While the coverage addresses all levels to an extent, the societal level receives more coverage than the individual and organisational levels. When discussing the organisational level, the coverage predominantly focuses on financial and reputational risks. Additionally, the *Financial Times* also addresses the deepfake risk for companies as an opportunity for profitability by implementing safety measures against deepfake threats. Overall, the findings of this study had similar results to the existing academic research on the deepfake phenomena and news media and provided further insights into this phenomenon. This paper concludes with this research's theoretical and societal implications, as well as its limitations and possible suggestions for future research.

KEYWORDS: *Artificial intelligence, Deepfake, Thematic analysis, News media, Organisation*

Table of Contents

1. Introduction

In contemporary society, advancements in artificial intelligence (AI) have brought about influential developments, such as deepfakes (Karnouskos, 2020). While AI has enabled individuals greater access to information, its advancements make it difficult for people to determine and believe in information. As with every novel technology, it is backed by varying perspectives that concentrate on the technology's advantages and disadvantages in an effort to provide future forecasts on the influence of the technology on people and society (Karnouskos, 2020). Deepfakes, regarded as one of these technologies, have gained significant attention in the mainstream news media, making it interesting to investigate how their consequences are portrayed in the news. Given the scope of this study, this paper will look into the technology's risks.

1.1 Research question and research gap

Deepfake uses deep learning techniques to create forged pictures, videos, and audio, which poses a risk to our digitalised society (Gamage et al., 2022) by making it difficult to differentiate what is real or fake (Rössler et al., 2019), thereby decreasing trust towards stakeholders, operations, and journalism (Karnouskos, 2020). In fact, Pinhanez et al. (2022) call them "a new wave of discrimination", emphasising their potential to distribute fake information that misleads and hurts people by masking dishonesty. A notable example is from a company in the United Kingdom (UK) that fell victim to deepfake fraud and lost €220,000, underscoring the threat deepfakes pose to an organisation's finance and reputation. Moreover, the low technical knowledge and devices needed to develop such deepfakes suggest that anyone can create and share them online (Karnouskos, 2020). This, along with its easy distribution on social media, heightens the issue of fake news. Yet, only 28% of UK cybersecurity decision-makers implemented measures to safeguard themselves from deepfakes, while 41% intend to within two years, implying that some organisations might underestimate deepfake threats (iProov, 2020). This underestimation of the deepfake risks and the lack of preventive measures implemented by organisations suggests a need for more understanding of the risks posed by deepfakes.

Moreover, considering the significant impact the news media has in influencing public ideas and beliefs (Nguyen & Hekman, 2022) and the influence that deepfakes have on a business's financial and reputational state (de Rancourt-Raymond & Smaili, 2022), it is important for the news media to cover deepfake risk on the organisational level. Insufficient news media coverage of the organisational level of deepfake risks may cause businesses to remain unaware of the possible risks associated with deepfakes. Furthermore, it may hinder the organisation's ability to recognise the importance of implementing measures against deepfake attacks, indirectly contributing to the proliferation of deepfake threats. However, existing academic literature examining the news media coverage of deepfakes often focuses on the individual and societal levels while neglecting the

organisational level. While the individual and societal level of deepfake risks is relevant, Pantserev (2020) also highlights the need to investigate the phenomenon on all levels, including the individual, societal, and organisational levels (these levels will be further discussed in the next chapter). Therefore, it is crucial to study how the news media addresses and presents the deepfake risks, especially on the organisational level.

As such, this study intends to address this gap through an analysis of news media discussions of the deepfake risks within the *Financial Times*. Focusing on serving the corporate world, the *Financial Times* is relevant for this study as they are the primary source of information for businesses, politics and global affairs (*Financial Times,* n.d.), making them appropriate for studying how they address deepfake risks within an organisational context. Accordingly, as Pantserev (2020) emphasised (supra), while this paper's main focus is on the organisational level of deepfake risks, it also looks into the individual and societal levels. Hence, through a qualitative thematic content analysis, this study seeks to answer the research question of "How does the *Financial Times* address the risks of deepfakes for companies?". Two sub-research questions (SRQ) are developed to support the research question:

SRQ1: Which deepfake risk level is present in the *Financial Times* news coverage, and how are these risks presented?
SRQ2: What are the key focuses in the *Financial Times's* coverage of organisational-level deepfake risks?

The first sub-research question uncovers whether the organisational level appears in the *Financial Times* and how it appears compared to the other two levels (i.e., if it is taken seriously or as secondary). Specifically, this question will examine how news media characterise deepfake-related risks. For example, non-consensual deepfake pornography, including its consequences, is a recurring concern in the news media (Westerlund, 2019). However, according to Godulla et al. (2021), non-consensual deepfake pornography is portrayed in a way that the individual consequence is not as important as the political and societal consequences. Furthermore, the existing academic literature examining deepfake coverage in the news media mainly focuses on the individual and societal risk levels while providing limited attention to the organisational level. This lack of representation on the organisational level undermines the risk that deepfakes pose to organisations. Thereby leaving businesses inadequately prepared to prevent fraudulent deepfake activity and indirectly enabling their further proliferation.

Subsequently, the second sub-question attempts to discover other potential patterns or themes surrounding deepfake organisation-level risks within *Financial Times*. This question can be studied by analysing mainstream news media's discussion of deepfakes as they provide a comprehensive

overview of deepfakes from multiple interdisciplinary that allow for informed efforts to address its growing hazards (Nguyen & Hekman, 2022). Furthermore, studying mainstream news media will enable organisations to understand and be prepared for the risks that deepfakes pose, making it essential to study whether and how this can be done.

1.2 Societal and academic relevance

Analysing the coverage of deepfakes in news media is important as they influence society's idea of the future (Wahl-Jorgensen & Carlson, 2021). This is especially relevant for organisations as the news media can increase awareness of the threat deepfakes pose to their operations. However, insufficient media attention towards deepfake issues could lead to a lack of seriousness about the threat. Hence, by analysing deepfake news coverage, this study can boost public understanding and awareness of the deepfake issue, especially on an organisational level.

In this regard, news media will be a valuable data source as it provides a comprehensive interdisciplinary context of a phenomenon, such as deepfakes (Nguyen & Hekman, 2022). Through analysing the news media coverage of deepfakes, this study can determine how deepfake risks are mediated across the three levels. Specifically, it aims to understand whether the media focuses on individual and societal levels over organisational levels.

Moreover, this study significantly contributes to the study of deepfakes, as it offers insights into how the news media presents deepfake risks for organisations. It does so by emphasising the areas within the *Financial Times* that have received greater or lesser coverage of a specific deepfake risk level. Investigating how the different deepfake risk levels are presented, especially on the organisational level, provides significant insights into how the deepfake issue is presented to the public and organisations. Additionally, by revealing potential biases within the *Financial Times's* reporting of a specific level, this study could help future reporters to strive for more comprehensive and unbiased coverage of the deepfake phenomenon.

1.3 Chapter outline

An outline of this paper is provided to address the research and sub-research questions. The following chapter will present the theoretical framework, offering an overview of relevant theories and previous academic literature on deepfakes, focusing on the three deepfake risk levels. The third chapter is the methodology, which will justify selecting a qualitative approach. Additionally, it will discuss the sampling, data collection, and operationalisation, as well as the validity and reliability of this study. The fourth chapter will present the findings derived from the analysis. The final chapter will conclude this study by answering the research and sub-research questions. Furthermore, it will also reflect upon the implications of this study, discuss its limitations, and provide recommendations for future research.

2. Theoretical framework

Since this study intends to form an understanding of how the news media addresses deepfake risks for companies, a theoretical framework exploring prior academic literature is essential. Hence, this chapter will investigate past theories and concepts surrounding the topic of deepfakes. This chapter will first introduce the phenomenon of deepfakes, followed by their risk levels and how they are presented in existing academic literature analysing deepfake coverage in the news media.

2.1 What are deepfakes?

Deepfakes are a by-product of artificial intelligence applications that manipulate images and videos to develop authentic-looking fake videos (Maras & Alexandrou, 2019). Generally, deepfake technology is cheap and easily attainable, allowing individuals with low technical or artistic competency to manipulate videos, switch faces, and change expressions and speech (Westerlund, 2019). They are often used to create manipulated videos portraying an individual conducting things that never occurred. Developing such deepfakes usually involves inserting videos of two individuals into an algorithm and teaching it to switch an individual's face with the other individual's face. By combining manipulated videos with authentic-sounding audio, these deepfakes videos can make many people believe that the content is authentic.

Though deepfakes can bring benefits, for instance, through realistic vocal dubbing, and overcoming language barriers in entertainment, their easy distribution throughout digital media is increasingly concerning (Gamage et al., 2022). Since the first emergence of deepfakes in 2017, mainstream news media, including the general population, reacted to deepfakes with anxiety and curiosity (Lee et al., 2021). These concerns include increased misinformation, jeopardised trust in media content, ruining individual and organisational reputations and manipulating elections (Gamage et al., 2022; Lee et al., 2021).

2.2 Deepfake risk levels

In order to gain a better understanding of how the news media addresses the different levels of deepfake risks, this section will further delve into these levels. Collins (2019) differentiates the three deepfake risk levels according to the individual, organisational and societal levels. When investigating the deepfake phenomena, Pantserev (2020) states that these three levels must be addressed. Hence, to get a comprehensive understanding of how the news media addresses and presents the deepfake risks, it is important to consider the three risk levels.

Firstly, the individual level refers to the potential harm deepfakes can cause individuals, such as abuse and defamation. For instance, fraudsters could use deepfakes to obtain sensitive information from individuals, blackmailing them into sending money or personal data (Chesney & Citrion, 2018). In contrast, the organisational level refers to deepfakes causing harm to a company. This can be

regarding the company's reputation or consumers' trust in them (Collins, 2019). It could also be regarding using deepfakes to obtain sensitive information and money from an organisation (Pantserev, 2020). Finally, the societal level refers to the risks deepfakes pose to a nation's political stability, security and wider influence. This could be, for example, creating a deepfake video of a political figure saying or conducting actions they did not do, resulting in political issues or jeopardising international ties (Pantserev, 2020). It could also be in the form of electoral manipulation, which can result in a loss of trust in governmental institutions and societal distress (Brooks, 2021; Collins, 2019).

While there is not one synonymous definition for these levels, to ensure a comprehensive analysis and the inclusion of all possible insights, this study will take on a broad definition of the three levels by including any discussions about the impact that deepfakes have on the different levels. Further explanations will be discussed within the results chapter. Overall, the three deepfake risk levels serve as a foundation for analysing the multifaceted nature of the deepfake phenomenon. Through these levels, this study can analyse and compare the influence of deepfakes at various levels and how these risk levels are addressed and presented. Thereby facilitating the identification of key focuses and issues that deepfake causes for a specific level, ultimately contributing to a conclusion to the research and sub-research questions.

Deepfakes as fake information

Consequently, given their possible influence on individuals, organisations and society, it is crucial to address the issue of deepfakes. Deepfakes are often associated with fake information, as they are often used to manipulate videos to falsely portray someone conducting things they never did (Westerlund, 2019). In fact, de Rancourt-Raymond & Smaili (2022) state that deepfakes intensifies the issue of fake news. Fake information can be classified into one of the following groups: disinformation or misinformation (Dobber et al., 2021). Disinformation is a deliberate act of spreading fake information with the specific purpose of deceiving, whereas misinformation is spreading fake information without the intention to deceive.

While deepfakes can be regarded as misinformation (Weikmann & Lecheler, 2023), they are usually categorised under the disinformation group since deepfakes can be deliberately used to disinform and reduce trust towards social institutions. This is because deepfakes are usually developed to mislead and give false evidence for an occurrence that never occurred (Weikmann & Lecheler, 2023), which includes manipulated, fraudulent or forged content (Dobber et al., 2021). Furthermore, disinformation often intends to pursue a political goal and may originate from local or foreign sources (Weikmann & Lecheler, 2023). Local political individuals could use illegitimate ways, such as disinformation, to elevate their goals. In contrast, foreign individuals may try to interfere in local discussions by disseminating fake information and creating disputes in public opinion. Moreover, they

might attempt to alter citizens' perspectives to make them distrustful of truthful information and institutions.

Consequently, disinformation, specifically through deepfakes, is seen as an issue of (inter)national security. This is particularly concerning as deepfakes could fasten the transition to a post-truth era (Sloot & Wagensveld, 2022). According to Temir (2020), the concept of post-truth refers to the concerned display of the public that views the "truth" as vital but perceives it as being in danger due to the distorting distinction between authentic and fake. This concept often encourages various "forms of strategic manipulations" on social media. Temir (2020) argues that the post-truth is crucial and will likely remain. In fact, with the rising potential to manipulate the public in various ways, the contemporary society we live in now can be regarded as a "post-truth" era. The concept of the post-truth era highlights the broad and far-reaching implications that deepfakes can pose through misinformation and disinformation. Though, it should be noted that the above issues predominantly revolve around political and social implications. This points to the argument that the discussions of the organisational-level deepfake issue tend to be dismissed or disregarded, aligning with Godulla's et al. (2021) argument, in which they state the news media mainly focuses on the individual and societal level (intra).

2.3 Deepfake news media coverage

This paper argues that the organisational deepfake risk level should be addressed and equally significant at the individual and societal levels. To investigate whether and how the news media address the organisational deepfake risk level compared to the other two levels, this study will look into news media coverage and their discussions of deepfakes. Analysing the news media's coverage of deepfakes is relevant as it is often the primary source of information for many companies, and news media has the ability to raise awareness of the different risk levels (Yadlin-Segal & Oppenheim, 2021). However, considering the lack of academic research on news media coverage of deepfakes, it should be noted that deepfakes are created and distributed on various platforms. Hence, on top of examining existing academic literature on news media discussions of deepfakes, this section will also draw upon existing studies on deepfakes in general, including those that have used other platforms for data analysis. Through analysing existing academic literature on deepfakes, this chapter intends to obtain a general overview of the deepfake phenomena and whether, in existing academic articles, it is described that mainstream news media portrays each deepfake risk level adequately or if there are gaps in their reporting.

Likewise, journalism aims to offer individuals the information they require to be aware and contribute to everyday life (Hanitzsch & Vos, 2018). Thus, news media coverage of deepfake risks is important as they can influence society's ideas of the future and potentially influence the actions and solutions individuals envision and act upon (Wahl-Jorgensen & Carlson, 2021). This highlights the

media's role in influencing societal response to deepfakes and informing people about the world, allowing them to make informed decisions. For example, a detrimental portrayal of deepfakes could impact society's view and trigger requests for legislation or bans on deepfake. These portrayals in the existing literature on deepfake news coverage often relate to individual and political threats.

However, given the complexity of deepfakes which can influence various aspects of society, it is important to consider their implications on an organisational level, and other facets, as Pantserev (2020) also emphasised (supra). Hence, despite this paper's focus on the organisational level, this study will also examine the societal and individual levels to obtain a comprehensive overview of the deepfake phenomena. As such, the first sub-research question (supra) is developed to examine whether the organisational level is recognised in the news media and whether it is taken as seriously as the individual or societal level.

2.3.1 Risk of deepfakes on the societal level:

Social manipulation

In order for an issue to be considered important by the public, it must first be covered by news media (Nisbet & Huge, 2006). Hence, a "triggering event" that renders the broader problem apparent to the people through an example is needed for news media to be intrigued by deepfakes. However, the "triggering event" commonly reported on deepfakes is predominantly a political event operating at the societal level. For example, a deepfake video of a US House Speaker, Nancy Pelosi, appearing inebriated became widespread online (Appel & Prietzel, 2022). The video was distributed by notable politicians and obtained over 2.5 million views within a few days (Westerlund, 2019). Such deepfakes could sabotage electoral campaigns, endanger national security, and increase fake information (Goose & Burkell, 2020).

Moreover, the experiment conducted by Dobber et al. (2021) exemplifies how political deepfakes, such as the one of Nancy Pelosi, can harm politicians and their political parties. In this experiment, Dobber et al. (2021) developed a deepfake of a politician and examined its influence on the audience's political perspective among the microtargeted and target group. Their study found that deepfake videos of politicians led to a stronger pessimistic mindset towards the portrayed politician, but the mindset towards the politician's party stayed similar to the controlled group. Whereas for the microtargeted group, it was found that there was a stronger pessimistic mindset towards both politician and the politician's party. Their study suggests that the influence of malevolent political deepfakes, specifically microtargeting methods, can strengthen the influence of deepfakes on a specific target audience.

Threat to national security

Furthermore, according to Westerlund's (2019) analysis of news media discussion on deepfakes, the news media views the manipulation of video content to portray someone saying or doing something they did not as a potent weapon to change people's perspectives. For instance, on March 2nd of, 2022, a video of the Ukrainian president, Volodymyr Zelenskyy, declaring his country's surrender to Russia was released (Byman et al., 2023). The video was circulated and shared on various social media platforms and reported by the news media. Soon after, Zelenskyy immediately denied the video's genuineness, pointing out that these are the type of deepfakes that he had cautioned the public about prior to the war. Nevertheless, this deepfake video represented a transition in information functions as it was the first high-profile usage of deepfakes during wartime. Even though deception and media manipulation has always been a component of wartime communications, it has never been plausible to create seemingly authentic audio, videos and text (Byman et al., 2023). Deepfakes are, thus, made to strengthen existing ideological predispositions and ideas, leading to more social division and political bias (Weikmann & Lecheler, 2023). As warned in Dowdeswell and Goltz's (2020) article, when used with bad intentions, deepfakes could worsen divisions in societies and government by making it challenging to determine what is real or fake.

Furthermore, with their ability to spread quickly worldwide, the news media have expressed concerns regarding deepfake's ability to undermine societies and countries (Brooks, 2021). In fact, the news media have associated deepfakes with a war-like environment that poses a significant risk to national security, one that societies cannot overcome unless a resolution is provided. These risks include fabricated dangers to a country's safety and falsified political disclosures, potentially jeopardising societies and countries. Specifically, the news media are concerned that such manipulated videos would lead to internal commotion, protests and election interruptions, while other countries could potentially execute foreign policies based on fake information, leading to global disputes (Westerlund, 2019).

2.3.2 Risk of deepfakes on the individual level:
Information apocalypse

Beyond societal concerns, the news media is also concerned about deepfakes' implications on people's safety and privacy. Specifically, deepfakes can jeopardise one's reputation, potentially causing unemployment if a deepfake video of an individual committing misconduct circulates. The news media shares this concern in that deepfakes can potentially mislead and deceive people (Gamage et al., 2022), causing them to have erroneous views that could sabotage the validity and credibility of information (Gosse & Burkell, 2020). More specifically, the main worry lies in the fact that deepfakes have the ability to portray something as "authentic" when, in fact, it is not, thereby leaving people uncertain about the reliability of the information, as well as deteriorating people's trust in what we view, listen and read.

Furthermore, as individuals increasingly become reluctant to trust crucial information that is truthful, the media points to a "collapse of reality" (Brooks, 2021). The news media challenges here lie in the fact that deepfakes can potentially hinder people's digital literacy and belief in official institutions. One news media article suggested that the most harmful part about deepfakes is not disinformation. Instead, it is the continuous exposure to fake information that makes people perceive that all information, including videos, cannot be relied on, leading to a phenomenon called "reality apathy" or "information apocalypse". Reality apathy refers to a situation in which individuals give up trying to figure out authenticity from the fake that they might even begin to believe in misinformation and disinformation (Dowdeswell & Goltz, 2020). This concept results from decreasing reliability of societal institutions – such as news media organisations, legislators, public figures and academics, and leads to an information apocalypse. An information apocalypse occurs when there are no longer any reliable standards on differentiating what is genuine and reliable from the fake and no one in authority to oversee technological advancements. Dowdeswell and Goltz's (2020) article states that the consequences of this occurrence go further than interference during political elections and can be seen in other societal aspects as well.

On the other hand, existing academic research discovered that individuals more resistant to deepfake news have less congruent perspectives (Shin & Lee, 2022). This suggests the existing confirmation bias that individuals participate in while taking in information. In terms of deepfake news content, the availability of a video, despite its quality, can already make individuals whose perspectives align with the news perspective to perceive that the news is reliable as it conforms to their existing opinions. These confirmation biases can persuade individuals to be more or less thoughtful of the impact that deepfake videos can have. Furthermore, Dobber et al. (2021) revealed that the influence of a pessimistic deepfake video of a right-winged politician on the perspective towards the politician was more influential on individuals that do not support the politician's party than those that do. As such, Shin and Lee (2022) suggest that individuals are less critical of deepfake content that aligns with their beliefs and would be more likely to believe its content, establishing the presence of confirmation bias when consuming deepfake news content. Overall, the theories presented in this section offer insight into the interconnectedness of the consequences correlated with deepfake threats, providing a more nuanced understanding of the specific risks faced by the three levels.

Deepfake influence on journalists

Nevertheless, deepfake videos that change the voice and image to make socio-political statements appear realistic to the broadcast (Bryant, 2018) are increasingly worrying journalists. As television journalists depend on visuals for new reporting, deepfake technology makes this industry more problematic (Gutsche, 2019), especially for journalists who create (or are featured in) the changed content (Walker, 2019). A person hoping to make a video viral can use the provided visuals

and audio to manipulate what is displayed and heard. This is harmful because they might not recognise that their content has been manipulated, and it could consequently harm the reputation and validity of their reporting when the manipulated content is utilised to distribute fake information.

Moreover, existing research on disinformation which states that mainstream news media plays a crucial role in the distribution of disinformation, applies to the dissemination of deepfakes as well (Godulla et al., 2021). According to Godulla et al. (2021), deepfakes are more influential if they reach expansive views when distributed by the news media. Journalists have raised concerns that it will become more challenging to verify whether a source is reliable (Gutsche, 2019; Pavlíková et al., 2021; Westerlund, 2019). Consequently, when journalists are incapable of identifying a deepfake, they threaten to sabotage the authorities' news media by incorrectly distributing it to their readers (Godulla et al., 2021). This form of misinformation is consequential, as the spread of deepfakes and intermediating complexities could cause an erosion of trust towards social institutions and increase media scepticism, particularly within at-risk populations such as the less informed, undereducated or politically oppressed people.

Non-consensual deepfake pornographic content

Additionally, in contemporary society, where data is obtained and quickly redistributed on social media platforms, deepfakes can have negative implications for the ones who are the target of the video (Maras & Alexandrou, 2019). This content is often left online for an extended amount of time and could be moved to other platforms, making it difficult to be completely removed from the internet.

This content is often the distribution of non-consensual pornography, also known as revenge pornography. This has raised concerns among the news media regarding the development of non-consensual pornography as deepfake technology continues to advance (Westerlund, 2019). While non-consensual pornographic content has long existed, the increasing advancements in artificial intelligence technology, such as deepfakes, make developing such content easier and more seamless. As a matter of fact, Maras and Alexandrou (2019) argue that in the future, it could become unachievable to determine whether an image or video is authentic or not. Even in the contemporary age, when deepfakes are used in lower-quality videos such as CCTV recordings, it becomes challenging to identify whether they are genuine or fake. The news media's specific concerns on this topic include using non-consensual pornographic content to sabotage, blackmail or shame businesses or individuals (Westerlund, 2019). One example is the case of Rana Ayyub, a journalist based in India. After publishing negative reports about the Prime Minister of India in 2018, Narendra Modi and his political group, a deepfake video of her in a pornography film were found (Ferraro et al., 2020). The incident resulted in Ayyub facing persecution and shame from the public, which led to her being

sent to the hospital for heart palpitations. This example further highlights the significance of the deepfake issue on an individual level.

While the news media raises such concerns, an analysis conducted by Godulla et al. (2021) found that the discussions of deepfakes in the news media predominantly mention deepfake as a risk to individuals and society. However, this focus on individual risk is often followed by discussions of the potential effects deepfakes have on democracy and national welfare, which undermines the significance of the individual risk level. Goose and Burkell (2020) supported this argument as their research found that in various articles, non-consensual pornographic deepfake content functioned as the "origin story" role, leading a segway into dialogues on other outcomes. The subsequent paragraph (as cited in Gosse & Burkell, 2020, p. 10) exemplifies this treatment:

> Face-swapping deepfakes were quickly adopted by darker sides of the internet, especially for placing celebrities' faces onto performers in pornographic content. There are also concerns that these deepfakes may be utilised to distribute fake political information on social media, possibly impacting electoral results. As individuals become more alert to fake information, would they begin to be decided by fake videos instead? Consider the false statements that deepfakes could make politicians say.

While it is vital to outline the past to place deepfake discussions into context, it is troublesome that non-consensual pornographic deepfakes are portrayed as a backstory (Goose & Burkell, 2020). In 2019, Deeptrace studied a total of 14,678 deepfake videos and found that 96% were pornographic (Ajder et al., 2019). Thus, it can be said that the issue of non-consensual pornographic deepfakes is not just a backstory problem. Instead, it is immensely true that when discussing deepfakes is to discuss deepfake pornography. Hence, Godulla et al. (2021) suggest that both societal and individual risk levels should be taken seriously, and it is important to be ready for malevolent deepfakes on those levels.

To exemplify the argument that individual risks are not addressed adequately compared to the societal level, this study references the analysis conducted by Gamage et al. (2020) on deepfake discussions on Reddit. Their study found that while many Reddit users conveyed concerns about the influence deepfakes have on governmental institutions, such as electoral manipulation, few discussions regarding the implications of deepfakes on individuals were mentioned. The fact that individual Reddit users conveyed stronger concerns that deepfakes would influence government institutions more than individuals raises the question of how deepfake risks are discussed and prioritised in the media. This further reinforces the significance of this study's second sub-research question, which intends to look into which level of the deepfake phenomenon is present in the *Financial Times's* news coverage and how it is presented. While deepfake discussions on social media

platforms, such as Reddit, are not this study's main focus, the findings of Gamage et al. (2020) provide a broader context and understanding of deepfakes and their risks.

Synthetic social botnets

Moreover, in order to emphasise the risks deepfakes pose to individuals and to facilitate the identification of the type of deepfake attacks in this study's analysis process, this study draws upon one of the most common fraudulent deepfake methods Bateman (2020) warned about – synthetic social botnets. These botnets include the creation of fake social media accounts that are made from artificial intelligence-generated texts and images, such as deepfakes, posing a significant threat of financial harm. In contrast to the current botnets, synthetic botnets would be more efficient and challenging to detect. It is probable that social bots will inevitably use more AI, exacerbating the technological conflict between social media platforms and malicious attackers.

For instance, in May 2022, videos of Elon Musk emerged promoting his new Cryptocurrency scheme (Habgood-Coote, 2023). Despite having a video of him promoting this scheme himself, the video turned out to be a deepfake. Unfortunately, various people fell victim to this scam, including employees of Musk's company, Tesla (Novak, 2023). The victims not only had their money taken from them but also their personal data, such as their driving license and crypto wallet address, revealed, causing a breach of their privacy. This example serves as an illustration of the potential impact of deepfakes on individuals' finances and privacy. The example also demonstrates deepfake's influences on an organisation. Since these fraudulent activities are conducted under the organisation's name, in this case, Tesla's, it poses a risk to their reputation. These organisational deepfake-related risks will be further discussed in the next section.

2.3.3 Risk of deepfakes on the organisational level

Although societal and individual risk levels are important, this study argues that the organisational deepfake risk levels should also be considered and addressed adequately. While various organisations have banned deepfakes on their platforms, this approach remains insufficient in addressing the possible threats of disinformation which are proliferated by deepfakes (Ferraro et al., 2020). This proliferation of disinformation and deepfakes paves the way for an increasing number of legal and organisational challenges, which will be discussed in this section. Moreover, Bateman (2020) draws upon two other most common fraudulent deepfake methods that can influence organisations: fabricated private remarks and deepfake vishing (intra).

Despite deepfakes being an increasing threat to organisations, there is still insufficient literature on their organisational risk level in existing academic research on news media discussion about deepfakes. Specifically, while researching academic literature on news media coverage of

deepfakes, few articles discussed organisational-level risks and instead focused on politicians and society, aligning with Hasan and Salah's (2019) findings (supra).

Reputational damage and stock market manipulation

Despite insufficient literature, recent research examining news media discussion on deepfakes has shown that deepfake risks on an organisational level are real and can cause significant reputational and financial harm to businesses (de Rancourt-Raymond & Smaili, 2022). In fact, according to a 2022 report by Europol, various organisations are increasingly viewing deepfakes as a larger risk than identity theft, especially when most communications have shifted online due to the Covid-19 pandemic.

Consider the influence on customer confidence of a widely distributed, convincingly fabricated video illustrating an organisation that portrays the firm's high-profile chief executive officer making derogatory statements about a racial group (Ferraro et al., 2020). Bateman (2020) refers to this as fabricated private remarks, a media risk where deepfake videos or audio recordings inaccurately represent a public figure expressing negative remarks. Since verifying that the supposed statements did not happen is challenging, many victims would have to depend on their reputations to counter the false allegations. Moreover, attempting to mend these reputational damages, such as measures to prove that the media was manipulated, could require considerable investment in time and resources, which some individuals may not have (Ferraro et al., 2020).

This ability to create deepfakes that can portray high-profile executives saying things they did not do has sparked concern amongst the news media, as it could also lead to the manipulation of stock markets (Westerlund, 2019). This poses a significant threat, as for the longest time, fraudsters have been learning how to make money through traditional disinformation methods, such as fake texts or images, to tamper with the financial markets (Ferraro et al., 2020). For instance, in 2019, after a fraudulent message was shared on Whatsapp indicating that Metro Bank ran out of liquid assets, many fled to Metro Bank to withdraw their money and jewellery, leading to a sharp reduction of 9% (Sloot & Wagensveld, 2022). Such threats will only increase as authentic-looking manipulated media can be created and distributed on a larger scale through deepfakes (Ferraro et al., 2020). Consider the influence of fraudulent claims when accompanied by compelling fake videos and audio – not merely a blog attempting to scam people, but a realistic video of a firm's CEO confirming the deal. If the fraudulent deepfake media is convincing, it will be increasingly challenging to rectify misconceptions and for the economy to rebound, especially at a time in which individuals would like to believe what they would like to believe.

Corporate fraud and financial risks

As highlighted in Trend Micro's (2019) report, deepfakes are the newest tool for corporate fraud. Fraudsters could use deepfakes to spread disinformation, fooling the company and employees. Particularly, deepfakes fool employees into executing essential decisions (i.e., transferring money), thus affecting organisational finance and reputation. Bateman (2020) termed one of the fraudulent deepfake methods as deepfake vishing, in which cloned audio voices are used to make manipulated phone calls. This method of deepfake fraud has various implications, such as identity theft, imposter and deceitful financial scams. When well-constructed, deepfake vishing could manipulate a call recipient's trust towards the impersonated entity. Various victims who succumbed to this scam tend to associate defects in the cloned voice with a faulty phone connection or cave into psychological manipulation, leading them to believe that the synthetic voice is authentic throughout the call (Bateman, 2020).

Moreover, according to Westerlund's (2019) finding, there is an ongoing concern in the news media that deepfake technology would allow for real-time digital impersonation of a high-level individual in a company, which would allow them to, for instance, request an employee to make financial transfers or send out sensitive data. For instance, a UK-based organisation's chief executive officer (CEO) received a phone call from their German holding company requesting an urgent transfer of €220,000. Believing the caller was genuine, the CEO transferred the amount, but it was soon discovered that the caller used a deepfake voice to commit fraud against the company (de Rancourt-Raymond & Smaili, 2022).

As such, deepfakes and the disinformation accompanying them present an increasing risk to organisations, especially in terms of their financial state (Ferraro et al., 2020). Disinformation has long been a tool to harm companies, alter markets and sabotage trust towards businesses and institutions. In fact, it is roughly calculated that organisations annually lose about $78 billion due to disinformation, and an additional $9 billion is disbursed by both organisations and individuals in an attempt to rectify their tarnished reputations caused to disinformation. Given the advancements in deepfake technology, these numbers will only increase further.

Based on a survey conducted by the Brunswick Group, 88 per cent of investors perceive disinformation attacks on organisations as a profound problem (Moran & Golson, 2019). Hence, organisations should take the threats of deepfakes of utmost importance as they will not only put their financial value and reputation on the line, but they will also risk having their shareholders take action against them, have regulatory examinations, and lose access to funding. To overcome the risk of malicious use of deepfakes, Bansal and Victoria (2022) suggested more joint activities and techniques over policy regulations, technical solutions, and media literacy, as they act as practical ad moral countermeasures.

As deepfakes are increasingly used fraudulently for financial gains, they threaten the finance and reputation of individuals and organisations. Thus, de Rancourt-Raymond and Smaili (2022) argue

that it is crucial to understand deepfakes better to prevent their immoral and unlawful use towards organisations. Hence, the second sub-research question (supra) is developed to discover other potential themes surrounding the risk deepfake poses apart from the three risk levels mentioned above.

2.4 Contribution to the understanding of news media discussions on deepfakes

The difficulties and threats posed by deepfakes on organisations are not limited to financial risks. News media discussions play a significant role in influencing society's idea of the future, going beyond merely reporting about deepfakes (Wahl-Jorgensen & Carlson, 2021). Instead, news media report influences social perception and belief, raise awareness of a phenomenon, and direct attention to the actions and solutions needed (Nguyen & Hekman, 2022; Yadlin-Segal & Oppenheim, 2021), thus making it crucial for them to address deepfakes.

Specifically, news media discussions of organisational-level deepfake risks are particularly relevant as they increase awareness of the threat deepfakes pose to their operations, encouraging them to implement protective measures. Hence, in order to address the risks deepfakes pose to organisations, greater attention must be given to news media coverage and academic research on deepfake risks at the organisational level. It is through news media coverage that the public forms comprehension of the deepfake phenomenon, which is vital for efficient reaction and involvement in policy regulations (Goose & Burkell, 2020). However, people's inability to trust information, referred to as reality apathy, is detrimental to news media journalists as it undermines the credibility of the entire news media industry. Currently, the news media predominantly reports on individual and societal deepfake risk levels (Hasan & Salah, 2019). Suppose the problem of deepfakes is not addressed adequately. In that case, it might lead to various consequences, such as a lack of awareness or insufficient pressure on stakeholders (such as individuals, society or organisations) to implement preventive measures against deepfakes.

Addressing the risk of deepfakes on an organisational level is especially crucial given the lack of measures taken by organisations to address deepfake-related risks (iProov, 2020). iProov (2020) report indicates that only 28% of cybersecurity decision-makers in the UK have implemented measures to protect themselves from deepfakes. While 41% intend to do so within two years, and 38% have no plans to implement any measures (iProov, 2020). These statistics suggest that organisations underestimate the severity of deepfake risks, which indicates a need for greater awareness of potential deepfake risks at the organisational level. By not taking preventive measures against deepfakes, organisations become increasingly vulnerable to deepfake attacks, which could cause financial and reputational harm while exacerbating the spread of disinformation and contributing to reality apathy and an information apocalypse (de Rancourt-Raymond & Smaili, 2022). Consequently, if the media neglects the organisational level or considers it secondary and unimportant, organisations might not

see the threat of deepfakes as a significant risk and hence, overlook the need to implement preventive measures to protect themselves from deepfakes. In other words, by not reporting about deepfakes, news media may indirectly fail to prevent the threat of deepfakes. Hence, understanding how deepfakes issues are presented in the news media is crucial.

By looking into how news media discuss deepfake risk at the organisational level compared to the individual and societal level, this study can help to identify gaps in coverage and highlight areas where more attention is needed. This can help to ensure that news media remain a trusted source of information and continue to play a vital role in society. Thus, this study contributes to the knowledge of deepfake on the three risk levels, particularly on the organisational level, which has not been studied as thoroughly as other levels. Through studying this gap, this study intends to provide an answer to the research and sub-research questions through the results of the analysis process, which is aided by the theoretical concepts introduced in this chapter.

3. Methodology

This chapter will provide and discuss the relevant methodological approaches utilised in this study. In this study, a qualitative research approach was adopted using a deductive approach that focused on the three levels of deepfake risks: individual, organisational and societal. An inductive approach was also used to enable the discovery of new themes to emerge from that data. In terms of the data collected, this study examined news media articles obtained from the news media website of the *Financial Times*. Regarding the method of analysis, a thematic content analysis method was employed as it was used to discover the reoccurrences or patterns amongst categories (Newton Suter, 2012). Further elaboration on these methodologies will be discussed in this section.

3.1 Research design

The objective of this study is to gain a better understanding of how the news media address the risk of deepfakes for companies. It specifically seeks to address the research gap by investigating whether and how news media address the organisational level compared to the individual and societal levels.

To conduct this study, a qualitative content analysis was used as it concentrates on a more profound understanding of a phenomenon by examining texts, views and experiences (Corbin & Strauss, 2008). Since this study intends to discover reoccurring themes, patterns, concepts, and learnings surrounding the deepfake phenomena within the articles from the *Financial Times*, a qualitative analysis is more applicable (Newton Suter, 2012). Hence, through using a qualitative approach, this study allows for a nuanced exploration of the deepfake phenomena as covered in the *Financial Times*.

3.2 Sampling

To conduct a thorough analysis of the coverage of deepfake risks, this study will analyse mainstream news media articles from the *Financial Times.* As a well-respected and influential international newspaper, the *Financial Times* serve as the primary source of news and knowledge for businesses, politics and global affairs (Financial Times, n.d.). Given their wide range of readership from wealthy individuals to individuals in business and politics, data from the *Financial Times* articles are likely to offer a broad range of perspectives. This helps to ensure the inclusion of various insights on deepfakes and a comprehensive analysis of the deepfake risks on all three levels. Thus, the *Financial Times* is chosen as a suitable data source for this study as it can help explore the three deepfake risk levels: the individual, organisational and societal deepfake risk levels.

Nonetheless, this study applied a criterion sampling strategy when obtaining articles from the *Financial Times*, as the data was picked in accordance with pre-established criteria (Omona, 2013). This sampling strategy is often used to ensure the specific quality standard in the data obtained.

According to Palinkas et al. (2015), a dataset that fulfils the criteria established makes them information-rich. Hence, by using this sampling strategy, this study was able to obtain data that would provide valuable insights into the matter being researched.

To ensure a comprehensive analysis of this study, this section will provide the established criteria for selecting the articles in the *Financial Times*. Firstly, each article selected needed to have a minimum length of 400 words and primarily discuss the risk of deepfakes. To ensure that the relevant articles are selected, this study searched for the keywords "deepfake" or "deepfakes" on the *Financial Times's* website itself. The articles would meet the criterion if any of the two keywords were mentioned in the article's heading or description. The articles selected for the analysis were published between the 1st of January 2019 and the 17th of March 2023. This specified time period is selected to make sure that this study's analysis uses the most recent media coverage made available. However, given the current timeline of this paper's writing, which is still in early 2023, the collection of articles published on deepfakes in 2023 will likely be limited. Nonetheless, the existing articles published in 2023 on deepfakes would be included for analysis as it provides the most recent media coverage of deepfakes. Moreover, the selected articles were categorised under the news, newsletters, opinions, in-depth news, and feature genres, which can be filtered on the *Financial Times* website. The other genres that were available, such as reviews and photo essays, were excluded as they were irrelevant to this study's topic or did not include textual data that this study intends to research. After narrowing down the articles to these criteria, a total of 55 articles are obtained for the analysis.

3.3 Operationalisation

To further address the research question of "How does the *Financial Times* address the risks of deepfakes for companies?" two sub-questions are developed. The first sub-question is "Which deepfake risk level is present in the *Financial Times'* news coverage, and how are these risks presented?". According to Godulla et al. (2021) and Goose and Burkell (2020), existing academic literature and news media articles tend to prioritise the societal risk level. Hence, this sub-research question seeks to determine whether the organisational level is given adequate attention or is taken seriously as a threat or secondary compared to the individual or societal level. Furthermore, this sub-question can help demonstrate and address any pattern or themes surrounding the coverage of deepfake risk at different levels.

Furthermore, the second sub-research question is "What are the key focuses in the *Financial Times's* coverage of the organisational level issues?". Through an inductive approach, this allows for discovering other potential themes surrounding organisational risks within news media. This sub-research question will provide a more comprehensive analysis of potential patterns or themes in the *Financial Times's* coverage of organisational-level issues that might have been overlooked, not covered, or initially anticipated. Altogether, both sub-research questions provide an in-depth

understanding of how the *Financial Times* addresses the risk of deepfakes for organisations and the broader context in which they are discussed.

Defining the three deepfake risk levels

In order to answer the first aforementioned sub-research question, this section will define the three deepfake risk levels to determine whether a text from an article will be categorised under the individual, organisational or societal level. Moreover, due to the complexity of deepfake, these definitions are essential because articles could address various levels of deepfakes risks, making it noteworthy to know how to differentiate them. By analysing which deepfake risk levels are present and how the levels are presented in the articles, this study can provide an overview of whether there is a bias within the news media to prioritise or deem one level more important.

At the individual level, any news media coverage that discusses the possible threat of deepfakes to an individual will fall under the individual level. According to Collins (2019) and van Huijstee et al. (2021), these discussions could include, for example, personal, financial, psychological, and reputational security risks. As for the organisational level, any news media discussions revolving around the potential risks deepfake poses to an organisation will fall under this level. Generally, deepfake risks on an organisational level entail anything that could compromise an organisation's reputation, reliability, or financial security (Pantserev, 2020). This could include, for example, coverage of deepfakes being used to impersonate high-level executives or employees or blackmailing businesses (van Huijstee et al., 2021). Lastly, the societal level includes any news media coverage of deepfakes jeopardising societal or political stability and security, as well as democracy (Brooks, 2021; Collins, 2019). This may include coverage of deepfakes being used to distribute disinformation about politicians, such as the case of Nancy Pelosi, which can lead to political unrest (Appel & Prietzel, 2022). Furthermore, van Huijstee et al. (2021) included that it includes the sabotaging of the societal system and the decline of trust towards institutions. Through these categorisations of the three different deepfake risk levels, this study will be able to analyse and compare how each level is presented.

3.4 Data analysis

For this study, thematic content analysis will be used as a foundation to conduct the qualitative content analysis. To conduct this analysis method, this study refers to Braun and Clarke's (2006) strategy for thematic analysis, as they were the authors of this technique for analysing qualitative data (Astrid, 2021). Thematic analysis is often used in qualitative studies to help grasp the intricacies of meaning within texts by allowing for the categorisation and depiction of data (Guest et al., 2012). As this research attempts to uncover the risks deepfakes impose on companies through analysing text, this approach was deemed suited to conduct the analysis. Braun and Clark (2006) state

that thematic analysis is a technique for recognising, investigating, and documenting patterns (themes) among data. In this case, themes capture significant aspects of the data relevant to the topic being studied and provide insights into patterns or meanings deriving from the dataset (Braun & Clarke, 2006). It should be noted that themes can be considered relevant without reoccurring frequently in the dataset. Rather, themes capture significant meanings of the data in relation to the research question. Since this research investigates the discussion surrounding deepfakes in news media, using a thematic analysis can help this study identify the patterns surrounding the risk of deepfakes. Therefore, a thematic analysis is useful as it provides in-depth detail and arranges the data, making it helpful in exploring various outlooks and uncovering unexpected insights (Nowell et al., 2017).

According to Braun & Clarke (2006), there are six phases of analysis data in a thematic analysis to help provide a thorough method of filtering, decreasing and organisation the data to discover themes. The first step to conducting thematic analysis is to get acquainted with the data by conducting various rounds of reading the data while writing initial thoughts about it. After filtering and narrowing down the dataset according to the aforementioned criteria, the articles selected are saved as an HTML file and imported into Atlas.ti. Atlast.ti was used for this process as it is a software designed to organise big chunks of data (Soratto et al., 2020). As such, all the coding processes will be conducted on that platform.

The second step of the thematic analysis process was to develop initial codes by coding interesting aspects of all the data in an orderly manner (Maguire & Delahunt, 2017). These steps help to decrease large amounts of data into smaller chunks of meaning. These codes generated from the data can be recognised from a data-driven inductive (bottom-up) approach or a theoretical deductive (top-down) approach (Braun & Clarke, 2006). An inductive method suggests that the themes found are correlated to the data itself without attempting to conform to pre-established conceptual structures. A deductive approach is guided by a theoretical interest in a subject, hence, being more data-driven. This study will use a combination of inductive and deductive approaches. Using both approaches to analyse the data, this study can help fill the existing literature gap and provide an understanding of the risks deepfakes pose for companies. Specifically, a deductive approach was used to address the research question by examining the first sub-research question. This research analysed how the *Financial Times* address the risks of deepfakes for companies by categorising the risks according to the three deepfake risk levels. The data was then analysed to find recurring patterns with these levels in mind. Through this approach, chunks of data were coded that were deemed significant to this study's research question. In contrast, an inductive approach was utilised to help answer the second sub-research question and allow the discovery of new themes related to organisational-level deepfake risks that could emerge from that data. This flexible approach allows for discovering new interpretations or patterns without implying preconceived ideas (Kohlbacher, 2006). During this process, an open coding approach was taken, which involved generating and adjusting codes through

the coding process without any pre-established codes (Maguire & Delahunt, 2017). Open coding allowed for the discovery of new concepts and interpretations from the dataset (DeCuir-Gunby et al., 2011). While conducting open coding, codes or concepts were developed and were classified into themes that grasped something important or noteworthy within the dataset (Maguire & Delahunt, 2017). As Braun and Clarke (2006) stated in their study, there are no regulations set in stone on what would be considered a theme. Instead, themes are represented through their significance. After the open codes were developed, they were analysed using axial coding.

The process of axial coding allowed for the discovery of any associations between the codes (DeCuir-Gunby et al., 2011) by linking codes of data to each other (Simmons, 2017). Meaning either through a deductive or inductive approach, axial coding is a procedure of seeking a connection between the previously developed open codes. This process does so by combining open codes into subcategories that allow for the discovery of themes (Simmons, 2017). Selective coding is then conducted after axial coding. Selective coding allows this study to collate subcategories, organised through axial coding, in an adhesive and meaningful manner (Williams & Moser, 2019). The result of selective coding allows this study to provide a correct and effective portrayal of every aspect of the coding process, thereby obtaining a comprehensive understanding of the dataset. According to Williams and Moser (2019), an open, axial and selective coding process enables a study to access various ideas, beliefs and responses on a specific subject. Overall, using a mixed method of deductive and inductive approaches allows this study to answer the sub-research questions and, ultimately, the main research question.

After establishing potential themes, the fourth step of the thematic analysis process includes clarifying and improving them. Braun and Clark (2006) state that this step involves evaluating the potential themes and determining their viability. The fifth step then involves defining the final themes based on the subcategories, in which three main themes were derived. This step includes understanding what the themes and subcategories are about and how they correlate (Maguire & Delahunt, 2017). These main themes would then help provide an answer to the overall research question. After completing these five steps, the analysis report will be developed.

3.5 Validity and reliability

According to Stenfors et al. (2020), there are five ways to evaluate trustworthiness in qualitative research. First is credibility, which refers to the study's findings being convincing and reliable in that there is a consistency between the theory, research question, data collection, analysis, and results (Stenfors et al., 2020). In this study, this refers to the three deepfake risk levels, namely, individual, organisational and societal level, as they are referred to and used to ensure that there is consistency throughout the study.

The second criterion is dependability which is the degree the study can be duplicated in similar conditions (Stenfors et al., 2020). This criterion can be recognised when enough data is provided about the steps taken to conduct this study so that other researchers can refer to and attempt to replicate it. In contrast, the third criterion is transferability which suggests that results from one study can be applied to other situations or groups (Stenfors et al., 2020). To ensure both dependability and transferability, a detailed description of the sample selection process and a detailed description of the steps taken for data collection and analysis were provided. This would allow other researchers to refer to these steps and attempt to duplicate this study. Moreover, since thematic analysis outlines the main characteristics of a large amount of information, it contributes to the validity and reliability of this study as the researcher must utilise a well-structured procedure to manage data and create a precise and organised report. As such, a transparent description of how this research analysed the collected data was previously discussed to ensure this study is conducted ethically.

Fourthly, confirmability indicates an explicit association between the data and the findings (Stenfors et al., 2020). This study abides by this by providing a detailed description of how the findings come about through a code tree (as shown in Appendix B). The last criterion is reflexivity, a recurring process of confronting and reflecting on the researcher's position and whether their background could influence the study (Stenfors et al., 2020). This criterion will be elaborated in the concluding chapter of this study. Regarding ethical considerations, this study deals with already published texts in the *Financial Times*. Thus, no ethical risks are anticipated.

4. Results: Key issues covered by the *Financial Times* on deepfakes

Through the aforementioned method of analysis, that is, thematic analysis, this chapter looks into the main themes and overall findings by analysing the selection of articles in the *Financial Times*. The findings from the analysis are interpreted and correlated in relation to the research question and theoretical framework. The research question investigated how the *Financial Times* addresses the risks of deepfakes for companies. Through a thematic analysis, a total of three main themes emerged: (1) manipulation, (2) security risk, and (3) regulation.

Themes	**Subcategories**
Manipulation	Non-consensual pornography
	Electoral manipulation
	Impersonation
Security risks	Scams
	Privacy issue
	Misuse and denial
	Information apocalypse
Regulation	Collaborative efforts
	Education and awareness
	Legal measures

Table 1: An overview of the themes and subcategories derived from the analysis

The manipulation theme closely corresponds to the security risk, as they both provide an understanding of the potential threats deepfake poses to the three deepfake risk levels. The difference between both themes is that the manipulation theme focuses on how deepfakes are used to exploit people and information. Whereas the security risk theme discusses the possible risks and vulnerabilities deepfake poses to organisations, individuals, and society. The *Financial Times* discusses these risks in accordance with possible regulatory measures, hence, relating to the regulation theme. The regulation theme discusses actions and policy measures needed to mitigate the risks

associated with deepfakes. Overall, these themes aid in providing an understanding of how the deepfake risk levels are presented in the *Financial Times*. This allows the study to highlight areas the *Financial Times* primarily focuses on when discussing deepfakes, as well as highlight the levels which would need more attention.

4.1 Manipulation

One of the themes of importance throughout the articles from the *Financial Times* was the aspect of manipulation that deepfake could create. Upon analysing the *Financial Times* articles through the lens of the individual, organisational, and societal deepfake risk levels, a consistent pattern of deception within the three deepfake risk levels was discovered. The manipulation theme refers to the depiction of deepfakes to exploit people and information for various reasons. Specifically, throughout the analysis, the *Financial Times's* coverage of deepfakes primarily concentrated on the potential of deepfakes to spread false or misleading information.

The manipulation theme is relevant as it provides an understanding of how the *Financial Times* addresses the manipulation risk posed by deepfakes and its potential to be used for fraudulent activities and manipulative intentions. Furthermore, it illustrates how manipulation-related deepfake risks can influence the individual, organisational, or societal level. As such, the most prominent topics found in the articles surrounding the manipulation of deepfakes can be best described through the following three subcategories: non-consensual pornography, electoral manipulation, and impersonation.

4.1.1 Non-consensual deepfake pornography

The analysis conducted in this study found that various articles discussed non-consensual pornography in relation to deepfakes. Based on the findings, non-consensual deepfake pornography is often created for the purpose of revenge porn, which can create psychological distress for the targeted individual while the attacker gains financially. This relates to the aforementioned argument presented by Westerlund (2019) in which they state that non-consensual deepfake pornography is often used as a tool for sabotage, blackmail or shaming businesses or individuals (Westerlund, 2019), illustrating the severity of the deepfake issue. However, as further results uncovered, the discussions around non-consensual deepfake pornography do not only revolve around the individual level but also the societal level. Politicians and civil rights campaigners are often found to be targets of this type of deepfake attack. This is evident from the article by Thornhill (2021, article #10[1]) in which they state: “But

[1] The news media articles from the *Financial Times* are numbered to differentiate the articles from the theoretical framework and the analysis. The list of news media articles and their associated number can be found in Appendix A.

much deepfake content has more sinister intent. A study from 2019 found that 96 per cent of deepfake videos involved non-consensual face-swapping pornography, targeting celebrities or civil rights campaigners.". Based on this finding, it is worth mentioning that most of the non-consensual pornography cases discussed in the articles analysed involve celebrities. By narrowing down non-consensual deepfake pornography cases to celebrities or politicians, it suggests that this only occurs to high-profile individuals and that other individuals are less important or relevant in this discussion. This can be problematic as other regular individuals can fall victim to such attacks but may not have the financial or legal resources to address the issue effectively. This could lead to further psychological distress and negative consequences as victims might not be taken seriously or given the necessary support to address their situation.

Moreover, as previously discussed in the theoretical framework, Godulla et al. (2021) and Goose and Burkell (2020) argue that individual risks, such as non-consensual pornography, are often followed by discussions about other outcomes, such as deepfake on democracy and national welfare, which ultimately undermines the individual risk level. One of the main findings from the analysis aligns with this argument, as the articles mention the organisational level, but only regarding how the organisations have banned deepfakes from being on their platform. These analysed discussions are often accompanied by societal-level issues, such as deepfake's potential to influence election results due to the distorted image of individual politicians that non-consensual deepfake pornography can create. Instead of placing responsibility or putting pressure on organisations, there are calls for governments to implement regulations. The following quote can exemplify this argument gathered from Criddle (2022, article #25):

> Companies including Twitter, Reddit and PornHub have already banned deepfake porn generated without the person's consent. In the US, Virginia and California have also made it illegal, while Scotland has also made it illegal to distribute deepfake porn. Last month the European Union also strengthened its disinformation rules to include deepfakes. Under a new EU code of practice, regulators can fine technology companies up to 6 per cent of their global turnover if they do not crack down on deepfakes.

Though the author discusses how organisations and governments have taken measures to ban or make it illegal to share non-consensual deepfake pornography, the emphasis in this quote is predominantly on governments. This undermines the organisation's responsibility to implement further measures that could curb the distribution of deepfakes on their platforms. While some organisations have banned the distribution of deepfakes on their platforms, as Ferraro et al. (2020) argued, this approach is ineffective in addressing the threat of deepfakes. As such, in the case of non-

consensual deepfake pornography content, the organisational level is not taken seriously or given much responsibility compared to the societal level.

4.1.2 Electoral manipulation

Additionally, various findings from the analysis of the *Financial Times* news articles revealed that deepfakes are often associated with electoral manipulation. In this study, electoral manipulation can be referred to as deepfakes being used to interfere in a country's election processes. The findings indicate that the use of deepfake on both individual and societal levels has been linked to attempts to influence electoral outcomes. This suggests that deepfakes have been used to create non-existent fake identities to support specific political parties or candidates. These findings align with one of Bateman's (2020) warnings about synthetic social botnets as a common fraudulent deepfake method. Synthetic social botnets are fake social media accounts using artificial-generated images, such as deepfakes, which are more challenging to detect. They have the potential to create or alter an individual's perspective of a specific political party. Hence, synthetic social botnets can threaten democratic norms by undermining the democratic processes of politicians, individuals, and private individuals (Cookson, 2020, article #15). In fact, Murphy (2020, article #19) even associated the growth of synthetic social botnets with the "democratisation of propaganda", as it is easy and affordable to purchase such bots to operate a programme that will develop deepfake profiles for a specific agenda.

However, it is not only individuals that would use synthetic social botnets. Foreign personnel have also been found to use deepfakes to create a "troll farm" of synthetic social botnets to manipulate election results. These sorts of deepfakes can possibly distort global news and often have a greater influence on groups of individuals who are less exposed to credible news sources. This relates to the subcategory propaganda, as foreign countries often use these "troll farms" to create and distribute deepfakes with a specific agenda and bias. As synthetic social botnets are increasingly easy to create, foreign countries have even been found to fund the creation of these accounts to support a specific agenda or politician. Notably, Murphy (2020, article #19) identified the trend of "manipulation-for-hire", in which they pointed out the rising trend of operations hiring third parties to conduct deceitful actions using deepfakes. Such services make it more challenging to identify the perpetrators and take measures against them. This paragraph can be exemplified by the following segment from Venkataramakrishnan's (2020a, article #6) article:

> Already, fake faces have been identified in bot campaigns from China and Russia, as well as in rightwing online media outlets and purportedly legitimate businesses. Their proliferation has led to concerns that the technology could represent a more ubiquitous and pressing threat

than deepfakes, as online platforms grapple with a rising tide of misinformation ahead of the US election.

This shows that the impact of deepfakes on societal perception and their ability to manipulate the public makes deepfakes a significant geopolitical concern. While these synthetic social botnet accounts are created and used on online platforms, the findings found a lack of discussions relating to the responsibility of the platform-owning organisations to prevent these manipulations from occurring. Nonetheless, the use of synthetic social botnets does not just end with the support of a specific politician or political party. It also extends to deceive others through a form of a disinformation campaign. Kaminska (2020, article #22) highlights that deepfakes are not merely bot-controlled Twitter accounts or modified videos of actual individuals in public. Rather, they are masquerading as everyday individuals or journalists. The article by Kew (2020, article #26) exemplified this with the case of Oliver Taylor, supposedly a freelance editor for the Jerusalem Post and the Times of Israel. Taylor's goal was apparently to deceive editors into publishing their stories to create a sense of credibility in his profile while advocating their agenda. However, this was not the only encounter using deepfake personas to pose as journalists. In fact, Kew (2020, article #26) noted that a minimum of 19 fake personas were used to pitch news content to news media organisations, such as the Washington Examiner and the South China Morning Post. This use of synthetic social botnets through deepfakes to create fake journalists posing as part of a well-known organisation threatens journalistic integrity. If these fake journalists gain credibility, they can publish disinformation and propaganda content, influencing public opinion and political outcomes. Thus, this study argues that organisations must take responsibility for implementing measures to curb fraudulent deepfakes instead of relying merely on governmental measures.

4.1.3 Impersonation

Additionally, deepfakes also allow fraudsters to pose as someone who may or may not exist, which in this case, is referred to as impersonation. It should be noted that these impersonations are not only limited towards individuals and political agendas, but they also have an influence on the organisational level. Specifically, the impersonation of CEOs through deepfakes is a prominent risk throughout the analysis of the *Financial Times articles*. The findings found that deepfakes, in this case, are used to deceive employees into transferring monetary funds into the attacker's account by cloning the voices of a CEO in order to impersonate them. The articles analysed from the *Financial Times* refer to this act of targeted deepfake attacks as "narrowcast". Specifically, it relates to targeted fraudulent attacks against a specific person or an organisation (Minsky, 2021, article #27). According to the study by Marchetti (2022), narrowcasts can target individuals, customers, public figures and organisations. The scope of the narrowcast covers corporate manipulation, identity theft for financial

gain, cybersecurity risks and blackmail. Deepfakes are used to assist in narrowcast attacks as deepfakes can raise the effectiveness from 60-70 per cent to 100 per cent. Similarly, another form of deepfake attack found throughout the analysis of the articles is the concept of "spear-phishing". Attackers conduct spear-phishing by, for example, impersonating a colleague or family member of the targeted individual through text or audio to obtain personal information, such as passwords (Kew, 2020, article #26). Kew (2020, article #26) adds that such attacks can snowball into one's LinkedIn connections, making the fraudster perceived as more credible to the victim's network. Additionally, the abundance of data that can be found online has made spear-phishing attacks simpler to conduct, as information can be easily found on social media (Venkataramakrishnan, 2019, article #28), making it an urgent matter to address. Hence, Kew (2020, article #26) also refers to this form of deepfake attack as "social engineering", which is a more significant threat than viral misinformation.

These narrowcast deepfake attacks can be related to one of Bateman's (2020) most common fraudulent deepfake methods, deepfake vishing, in which cloned audio voices are utilised to manipulate individuals over phone calls. Bateman (2020) argues that this deepfake fraud technique has far-reaching consequences, such as identity theft and financial scams. In fact, Murphy (2019, article #18) exemplifies this through one scenario in which fraudsters used deepfake vishing to pose as an executive over a phone call to scam an organisation's employees to transfer up to even ten million dollars. However, there are not merely financial consequences to these deepfake attacks. Instead, Kew (2020, article #26) finds that some fraudsters may be after sensitive data about an individual or an organisation. With access to sensitive information, fraudsters can use that information to threaten relevant personnel and coerce them into providing financial compensation. This aligns with Marchetti's (2022) argument, stating that narrowcast attacks can lead to blackmail.

Furthermore, the analysis revealed that some CEOs had been deepfake into saying something they did not do, which can have severe reputational damage to the individual and the company. Such deepfake attacks on CEOs can have reputational damage to the company and the company's stock prices. The findings that deepfakes can manipulate stock prices align with Westerlund's (2019) findings that deepfakes impersonation of high-profiled executives can lead to the manipulation of stock prices. This indicates that deepfakes can cause not only harm to an individual or organisation's reputation but consequences extend to the financial market. In fact, one finding of this study found that the influence of a successful deepfake attack could be "extremely painful, knock billions off share prices and cost CEOs their jobs" (Murphy & Reed, 2020, article #29). Moreover, the article from Murphy and Reed (2020, article #29) also found that due to the increasing ease of creating deepfakes, there would be more fraudulent activities happening to organisations, emphasising the risk deepfakes can cause individuals and companies. These findings highlight the need for organisations to implement preventive measures to mitigate the risk posed by deepfakes. By doing so, organisations

can protect not only individuals but themselves and their stakeholders from the potential harm caused by deepfakes.

Additionally, another main finding reveals that manipulated video content is one of the top methods artificial intelligence is used for fraudulent purposes and is becoming an increasing concern amongst customers. In fact, financial clients are aware of the threats deepfake poses, as one article states that 85 per cent of survey respondents state that deepfake makes it more difficult to believe what they see online (Vincent 2020, article #14). This aligns with Bateman's (2020) warning of another one of the most common fraudulent deepfake methods, fabricated private remarks, where deepfake videos or audio recordings are used to falsely represent a public figure expressing negative remarks. The implication of these findings exemplifies that the organisational risk level is ever-present in the impersonation subcategory and presented more as a financial and reputational risk to the employee and organisation. When these deepfake scams occur, it often has detrimental consequences for the organisation's reputation and reliability, especially if the scam targets an organisation's client, particularly a financial organisation. Venkataramakrishnan (2022, article #16) notes that the impacts of deepfakes on an organisational level, including its reputational and social consequences of developing and producing synthetic personas, are something that should be important to decision leaders, and not only the technological unit. Their article further suggests that: "Today, online conversations drive brand identities. Given the speed, scale and power of viral disinformation, its greatest immediate risk to business is reputational harm." (Venkataramakrishnan, 2022, article #16). Hence, the finding demonstrates that similar to fraud, safeguarding reputation demands companies to be quick and responsive from the top down. However, the findings predominantly portray reputational risk as a responsibility of the government sectors, with frequent mentions of the need for government and legal regulation, which will be discussed later in this chapter.

Overall, within this theme of manipulation, the *Financial Times'* key focus on the organisational level revolves around the impersonation subcategory. Specifically, Bateman's (2020) concept of deepfake vishing was used to conduct narrowcast attacks targeting specific organisations or employees. The threat that the *Financial Times* highlights here is the threat to the organisation's finances and reputation. Moreover, the individual level is also covered by *Financial Times* within this theme, especially concerning the non-consensual deepfake pornography subcategory. However, the societal level overshadows the coverage of the individual and organisational level implications, aligning with Goose and Burkell's (2020) findings (supra).

4.2 Security risk

The following main theme derived from the analysis was a security risk, which relates to the possible threats associated with deepfakes. This theme is relevant as it highlights the potential risks and vulnerabilities that organisations, including individuals and society, could face. Similar to the

manipulation theme, the security risk theme is relevant as it sheds light on how the *Financial Times* discusses the security risks related to deepfakes and the potential vulnerabilities that can arise across the three deepfake risk levels. This theme encompasses the following subcategory: scams, privacy issues, misuse and denial, and information apocalypse.

4.2.1 Scams

In terms of the scam subcategory, one finding of this study suggests that deepfakes play a pivotal role in the success of the theft of information, also known as scams. Specifically, one common scam which deepfakes have been found to support is cryptocurrency scams, which involve using fabricated private remarks where the CEO of the cryptocurrency or platform is visually and vocally deepfaked (Bateman, 2020). The motive behind this scam is to send false messages that deceive users into believing they will get a benefit in return for their investments when in reality, they do not. A notable example of this scam is the cryptocurrency scam mentioned earlier involving Elon Musk, as highlighted by Habgood-Coote (2023). In this incident, a deepfake video of Musk was used to promote a new Cryptocurrency scheme, leading various people, including one of Musk's employees, to fall victim to the scam. This example highlights the risks that deepfakes pose, as they can compromise an individual's privacy and financial state.

However, the use of deepfakes in scams extends beyond cryptocurrency scams to other scams, such as the job-recruitment scam. The article by Johnston (2023, article #3) reveals that fraudsters often target jobseekers and organisations in which the fraudster reaches out to individuals via LinkedIn messaging. The organisations that are targeted are often those that are currently recruiting people. The scammers then developed a copy of the organisation's website with the same job posting and, through LinkedIn's InMail feature, they requested job seekers to put their personal data into the website copy before having online interviews through Skype. According to Kaminska's (2020, article #22) article in the *Financial Times*, LinkedIn prevented the creation of up to 19.5 million synthetic social botnet accounts during account registration. While another 2 million accounts were taken down after registration, and another 67,000 were taken down after being reported by users. However, Kaminska (2020, article #22) also notes that these numbers only account for the synthetic social botnets that were detected and found, and it is difficult to tell the actual number of synthetic social botnets that went undetected or unreported. This illustrates that while LinkedIn had successfully detected and prevented many synthetic social botnets, many could remain undetected. This emphasised the need for organisations such as LinkedIn to improve their current methods of mitigating deepfake-related issues. Therefore, it is vital for organisations to develop and implement more effective methods to address the risk posed by deepfakes.

Furthermore, fraudsters would also utilise synthetic social botnets to develop fake Skype accounts, with the image of the actual recruiter from the organisation, to conduct interviews with the

participant. Jobseekers would have provided the fraudsters with crucial information through this job-recruitment scam. Johnston (2023 article #3) adds that some fraudsters even sought money for appliances or third-party coaching for which the victims would not be compensated. Given that these scams heavily rely on synthetic social botnets, it aligns with Bateman's (2020) argument that the increasing use of AI by these botnets will exacerbate the technological conflict between social media platforms and malicious attackers, resulting in harmful implications. This is evident with the following quote from Johnston (2023, article #3):

> The attacks come as the amount jobseekers lose in employment-related scams increases. Figures from the US Federal Trade Commission show there were more than 92,000 job-related and business scams in 2022, with $367.4mn reported lost. This compared to the 105,000 in the whole of 2021, when $209mn was lost.

The author illustrates the rise of job recruitment scams and their financial severity as a growing concern. However, the author also suggests that these scams are not only limited to individual job seekers but also impact organisations and their reputations, as these scams are usually conducted under the names of real organisations. These scams can, hence, negatively influence these organisations because they could lead to a negative perception and loss of trust from potential employees. For instance, due to the decrease in the trust of potential employees, fewer candidates would apply for a job with the organisation. This would result in the organisations having difficulty finding qualified candidates for job postings, possibly causing lower efficiency and revenue. As such, recruitment scams can cause a deterioration in brand image and financial loss for both the individual and the organisation. Other than financial and reputational threats, these scams have in common that the victim's personal information, including their addresses, identity and driving licences, are obtained (Novak, 2023), relating to the next subcategory of privacy issues.

4.2.2 Privacy issues

In this study, the subcategory of privacy issues relates to the use of deepfakes to obtain personal information. One of the findings of this study indicates that even without initiating scams, it is already easier for fraudsters to obtain personal information from an individual. This is due to the ample self-disclosed information that people are willing to publish about themselves online. The article by Kaminska (2020, article #22) illustrates this well with the following quote regarding how synthetic social botnets could be managed by artificial intelligence to: "… take advantage of the personal data we shed online to pinpoint our vulnerabilities, befriend us, and then manipulate us into doing their bidding. They are sinister precisely because they know us, and our weaknesses, so well.". Their article suggests that these deepfake accounts, managed by artificial intelligence, may attempt to

befriend individuals or recruit them in order to obtain personal information. Kaminska (2020, article #22) further adds that there is insufficient protection against these systems as most data that powers these artificial intelligence programs are already widely available online, being utilised by third-party algorithms for advertising. This makes it evident that the widely available personal information online is being exploited not only by fraudsters but also by organisations for financial gain.

On the other hand, Minsky (2019, article #9) reveals that some major organisations have implemented liveness detection into their identity verification operation, which requires the user to perform actions such as speaking or moving. This effort is an attempt to prevent fraudulent activities from occurring. However, due to deepfakes' ability to manipulate videos, pictures and audio, Minksy (2019, article #9) adds that deepfakes are the biggest risk to these online biometric verification processes. Though such biometric security processes are supposedly developed to ensure a more secure verification system, Minksy (2019, article #9) mentions that storing such data could increase the threat of security breaches. Their article reveals that a group of cybersecurity researchers had gained access to the fingerprints, facial recognition data, and various information of over one million individuals. In fact, during the analysis of the *Financial Times* articles, it was found that deepfakes constitute a significant cybersecurity challenge (Venkataramakrishnan, 2020a, article #6). Specifically, Warrell (2020, article #7) states that AI-developed attacks, such as deepfakes, are better at overcoming standard security measures and distributing quickly via networks outmatching human cybersecurity personnel. Their article adds that mitigating the risk of deepfakes requires AI technologies, as "only AI can fight AI". This paragraph emphasises the dual nature of artificial intelligence, serving as a tool for fraudulent attacks while also serving as a potential solution to prevent these fraudulent attacks. Hence, it highlights the necessity of developing AI technologies to address the major cybersecurity challenge of deepfakes.

4.2.3 Misuse and denial

Aside from fraudulent purposes, deepfakes can also be misused in the sense that people can deny their authentic wrongdoing by claiming that it was merely a "deepfake" of them when it is an authentic video. These issues fall within the subcategory of misuse and denial. Throughout the analysis, a prevalent concern was that deepfakes give politicians an excuse to deny wrongdoing. To further support this argument, the analysed article from the *Financial Times* draws upon the "liars dividend". Chesney and Citron (2018) refer to this concept as the way in which deepfakes make it simpler for liars to refute the truth. They argue that one of the biggest threats of deepfakes is that it encourages liar's dividends to occur, making people doubt and devalue the truth (Chesney & Citron, 2018).

Additionally, the analysis found that people who promote disinformation thrive and exert influence, even when its contents are proven false, causing a progressive decline of trust in established

authoritative sources (Nigam, 2021, article #12). Thornhill (2021, article #10) exemplifies this argument with the following quote: “The greatest danger from deepfake content is that it inflates the “liar’s dividend”, making everyone question everything and devaluing the currency of truth.”. This finding highlights how deepfakes can make individuals more doubtful about authentic information. To illustrate this point further, Moore (2021, article #13) provided an example that occurred to the president of Gabon in 2018 when a video of him was dismissed as a deepfake by people convinced that the government was concealing his death. No proof was provided that the video was a deepfake, but it did assist in starting a coup in their country. This example illustrates that not only can deepfakes deceive individuals into believing fake information, but they can also deceive them into thinking that authentic information is fake. Furthermore, it highlights the far-reaching consequences of deepfakes, that it erodes trust and distorts reality.

Moreover, another main finding from this study shows that deepfakes reinforce confirmation bias as people are more likely to believe information that confirms their existing views, even if they might be fake. This is evident from the quote from Waters’s (2019a, article #11) article, in which they state: “The rise of fake news has exposed the uncomfortable truth that many people are open to anything that confirms their existing views, even if they suspect some of it may be fake.”. This aligns with Shin and Lee’s (2022) and Dobber’s et al. (2021) research, which points out that confirmation bias exists in deepfake news consumption. Specifically, when the deepfake news aligns with the person’s perspective, they are more likely to perceive that the deepfake news is reliable and credible. This is harmful as it further allows for misinformation or disinformation to persist and could lead to societal biases. The repercussions of confirmation bias in deepfake news consumption are alarming because it reduces the evaluation of information and inhibits critical thinking. In turn, this would improve the continuous efficacy of misinformation and disinformation. By reinforcing established perspectives, confirmation bias of deepfake news content could lead to possible societal division and bias. Furthermore, the confirmation bias in deepfake news consumption relates to reality apathy in which individuals would give up attempting to determine authenticity from fake, and they might even start to believe in misinformation and disinformation (Dowdeswell & Goltz, 2020). In this case, individuals are exposed to news that they may or may not know is fake but do not put in the effort to determine whether it is real. As such, this study argues that this is a relevant and concerning matter as it further segregates people and creates a society that accepts fake information without determining whether it is authentic or not, as long as it coincides with the reader’s beliefs.

4.2.4 Information apocalypse

The concept of reality apathy results from the decreasing reliability of societal institutions – such as the news media, legislators, public figures and academics, and leads to an information apocalypse. Ovadya defines the information apocalypse as a state where people become increasingly

weary and distrustful towards social institutions (Dowdeswell & Goltz, 2020). In an information apocalypse scenario, no reliable standards for differentiating real or fake exist. In fact, the findings suggest that the aforementioned "liar's dividend" can also lead to a state of information apocalypse. The liar's dividend indicates that people who set out to distribute disinformation are in line to profit even if their attempts are discredited, leading to an incremental decrease in trust towards sources of authority (Nigam, 2021, article #12).

Building on this notion, Vincent (2020, article #14) discusses a survey involving 2,000 financial users, revealing that 85 per cent of respondents had stated that deepfakes make it challenging to believe what they view online. This finding underlines the prevalence of the information apocalypse, where individuals already have an elevated level of disbelief that hinders their ability to perceive the information they come across as authentic. This also aligns with Temir's (2020) study, which argues that contemporary society lives in a post-truth era, denoted by distrust towards information. As such, these findings (Nigam, 2021, article #12; Vincent, 2020, article #14) suggest that while the public deems the truth as important, deepfakes have the potential to jeopardise the dependability of the truth itself. Consequently, this poses a significant risk to the credibility and reliability of the aforementioned societal institutions. Cookson (2020, article #15) highlights this concern, emphasising that deepfakes can cause a possible information apocalypse and would threaten "not only politicians and the democratic process but also businesses and private individuals". The author further suggests that if an information apocalypse situation occurs due to deepfakes, it influences all three deepfake levels. For example, on an organisational level, individuals would be more likely to perceive content produced by news media organisations as unreliable, even when authentic, possibly resulting in a decline in their news consumption and sales, leading them to be almost insignificant. This erosion of trust would also impact the societal level. Due to individuals' lack of trust and confidence in their societal institutions and leaders, people might doubt the authenticity of political campaigns, speeches, or public statements, making informed societal-level decisions challenging.

Overall, as presented by the *Financial Times*, the key focuses of the organisational level within the security risk theme are predominantly discussed throughout most subcategories. Bateman's (2020) notion of fabricated private remarks and synthetic social botnets are used to conduct fraudulent scams such as cryptocurrency or job recruitment. The consequences of such scams include the exploitation of one's personal information. These consequences relate to the organisational level, as these fraudulent activities occur on an organisational-owned social media platform. Yet, the measures reported by the *Financial Times* to combat fraudulent deepfake activities are merely banning the distribution of deepfakes on these organisations' platforms. Regarding the individual and societal levels, the *Financial Times* primarily discusses them within the misuse and denial and the information apocalypse subcategory. The individual level is discussed as a means for individuals to easily deny the

truth, referring to the "liar's dividend" concept. This could lead to an information apocalypse, influencing all three deepfake risk levels. As such, in this theme, each level is presented with equal importance as they are interconnected and can influence one another, highlighting the need for comprehensive actions across the three levels to address the risk of deepfakes efficiently. This observation aligns with the findings from the regulation theme, which results from the analysis of the remaining codes.

4.3 Regulation

The regulation theme looks into the call for regulatory frameworks and measures to address the risks that deepfakes pose. The theme includes the following subcategories: collaborative efforts, education and awareness, and legal measures. This theme is relevant as it illustrates that *Financial Times* addresses the deepfake risk as something that should not be an individual effort to combat but instead a collaborative effort of the individual, organisational and societal levels. It suggests that these levels should be more intertwined than segregated. This can already be illustrated through the first subcategory, collaborative efforts.

4.3.1 Collaborative efforts

The subcategory of collaborative efforts refers to articles from the *Financial Times* advocating for the corporation and collaboration between different stakeholder groups to tackle the aforementioned deepfake issues discussed within the manipulation and security risk theme. As deepfakes become increasingly intricate, there are already collaborative efforts between organisations and other stakeholders, such as cooperation between researchers, governments and civil rights parties, to manage the moral and legal concerns surrounding using artificial intelligence for federal security (Warrell, 2020, article #7). To illustrate this collaborative effort, Nuttall (2019c, article #24) provides an example from the collaboration between Facebook, Microsoft and artificial intelligence researchers from renowned universities, such as Oxford and Berkeley. Together these organisations collaborated to identify deepfake content, which has a role in combatting disinformation. This collaboration between major organisations and academic institutions highlights the pressing issue of deepfakes and the need for collaborative efforts to address it effectively.

However, it was also found that despite the risks associated with deepfakes, some organisations and stakeholder groups had merely expressed intentions to address the risks of deepfake but have not taken concrete actions (Murphy, 2019, article #18). This finding aligns with the discussion in the theoretical framework, in which iProov's (2020) report indicates that merely 28% of cybersecurity decision-makers in the UK have implemented measures to protect themselves from deepfakes. While 41% intend to do so in the next two years, and 38% have no intentions to implement any measures, suggesting that some organisations do not take the risk of deepfake seriously (iProov,

2020). This finding highlights the potential vulnerability that organisations might face if they fail to address the risk of deepfakes, as de Rancourt-Raymond and Smaili (2022) suggest, organisations who do not implement measures against deepfakes will be increasingly vulnerable to their attacks, which could cause financial and reputational harm.

It is also worth noting that while some effort is being put into handling the threats of deepfakes, there will unavoidably be more difficulties in the future that no one sole organisation or industry can resolve on their own (Pichai, 2020, article #20). As Monstert and Franks (2020, article #17) point out, any security measure against deepfakes can be opposed through subsequent software updates. This is already evident in the ongoing struggle with human-generated disinformation, exemplifying the challenges in finding a definitive solution. Nonetheless, such collaborative efforts among businesses and other stakeholders are still vital, as according to Venkataramakrishnan (2022, article #16), businesses are still far behind in defending themselves against the risk of deepfakes. Their article exemplifies this well with the following quote: “One way to think about this issue is that disinformation and deepfakes risk is today where cyber security was 15 years ago, […] but the dangers are coming — and closing quickly.” (Venkataramakrishnan, 2022, article #16). This portrays the pressing need for organisations and other stakeholders to work together in combating deepfakes. Therefore, Murphy (2020, article #19) highlights that it is more vital than ever to seek resolutions to combat the threats that come along with deepfakes, and having collaborations between individual, organisational and societal is key to doing so. While determining a suitable measure to implement will be difficult, Hall (2019, article #23) states that a failure to do so would result in an erosion of democracy. The author underscores the severity of the threats of deepfakes, stating that “we must act now, collectively, to turn the tide”, further emphasising the urgency and collective responsibility needed to address this issue.

Moreover, despite calls for organisations and other stakeholders to collaborate, it should be noted that the threats of deepfakes extend beyond the technical division. Though businesses tend to perceive cybersecurity threats, such as deepfakes, as merely a technical concern, it is vital to recognise deepfakes as a threat to the entire business (Venkataramakrishnan, 2019, article #28). Hence, deepfake threats should be understood as an issue for all employees (Venkataramakrishnan, 2022, article #16). Furthermore, one main aspect of importance, as found within the analysis of the *Financial Times* articles, is that C-level executives need to take the issue of deepfakes seriously. While deepfakes often correlate with political agenda tools, the United State’s Federal Bureau of Investigation has cautioned that fraudsters will undoubtedly utilise deepfakes to attack organisations (Venkataramakrishnan, 2022 article #16). This can be exemplified by Venkataramakrishnan's (2022, article #16) article: “Disinformation is a problem that should not be the concern only of the IT department but also of the C-suite [...] The dangers posed by viral false narratives and realistic bogus media require more than technical solutions.”. This quote highlights the need for adopting a broader approach to combating the

risk of deepfakes. Therefore, the authors suggest that solutions should go beyond mere technical solutions and involve all employees' perspectives, including higher-level executives, such as the C-suites (Venkataramakrishnan, 2022 article #16).

4.3.2 Education and awareness

Additionally, other than calls for C-level executives to be aware of the threats deepfakes pose, there are also calls for education and awareness on this matter. This relates to the second subcategory of the regulation theme: education and awareness, referring to discussions around the importance and need for promoting knowledge and understanding about deepfakes. Some of these calls include digital and media literacy among users. Venkataramakrishnan (2020a, article #6) discusses that with improved deepfake identification software, and higher levels of media literacy, the negative consequences of deepfakes would be reduced. As most concerns about deepfakes regard their negative consequences, improving media literacy would be beneficial as it can potentially mitigate the concerns surrounding deepfakes. Mostert and Franks (2020, article #17) support this argument as they state that the response to deepfakes should be cyber-sociological, emphasising building digital media literacy. Their article suggests that people should be cautious and not solely rely on the content they encounter online. It emphasises the importance of educating both employees and the general public on the issue of deepfakes. Mostert and Franks (2020, article #17) go as far as to say that merely developing deepfake detection software is insufficient. They assert that educating individuals is the most efficient tool for combating the threats of deepfakes and disinformation. To do so, Nuttall (2019c, article #24) suggests that one method to do so is to "immunise" individuals against deepfakes by improving their "mental antibodies". As Mostert and Franks (2020, article #17) state: "The greater public awareness is of the technology and its uses, the more they will be able to think critically about the media they consume and apply caution where needed.". This emphasises the need for not only deepfake detection software but also education and awareness on deepfake technology to cultivate digital media literacy, aligning with Bansal and Victoria's (2020) suggestion that there should be increased digital media literacy on the topic of deepfakes as they act as a tool to combat deepfakes. This approach would help overcome the concern Brooks (2021) raised that deepfakes can pose a challenge to news media organisations, as they could hamper one's digital media literacy and trust towards social institutions, such as news media organisations.

However, the challenge here is that it would be difficult to educate individuals not to believe things they read and hear at face value, without, at the same time, eroding social trust (Cookson, 2020, article #15). According to Minksy (2021, article #27), the challenge is maintaining an appropriate level of awareness and caution regarding deepfakes without making one become overly sceptical and dismissing all media as potentially fake (information apocalypse). On the one hand, individuals and organisations need to be aware of the risks and harms posed by deepfakes. On the other hand, it is also

important not to become too sceptical and distrustful of all media that it becomes difficult to discern what is real or fake relating to the information apocalypse. Finding a balance between these two perspectives is challenging but crucial for effectively addressing deepfake risks. Therefore, it is also essential for legal and policy measures to be placed.

4.3.3 Legal measures

The third subcategory, legal measures, highlights the importance of implementing policies to prevent the negative implications of deepfakes. Given social media platforms' authority on unauthorised investments, such as the popular cryptocurrency investment scam, Barrett (2021, article #30) calls for prompt actions by financial authorities. However, even when there are regulations placed, organisations themselves would find it difficult to regulate the spread of deepfakes, as one of the findings from the analysis suggests that the growth of deepfakes can be attributed to profit motives. Developed to gain clicks and page views, various technology organisations' algorithms allow for developing and distributing artificial content, such as deepfakes (Thornhill, 2021, article #10). This is in hopes for the organisations to reach large audiences and even award the creators advertising revenue. The commercial incentives for organisations to develop and distribute deepfakes further emphasise the need for robust legal measures to prevent the negative consequences of deepfakes, as these incentives indirectly contribute to the proliferation of fraudulent deepfakes.

As an alternative incentive for organisations, one of the findings from the analysis reveals that companies can implement fraud prevention. According to Murphy (2019, article #18), various cybersecurity organisations are working rapidly to come up with a way to curb possible deepfake attacks. Likewise, as the executive director of Georgia Tech's Institute for Information Security and Privacy notes, "There is a significant opportunity for cyber security companies to play in this space when it comes to fraud prevention" (Murphy, 2019, article #18). Murgia (2022, article #31) exemplifies this with the following argument: "A lot of people have expressed concerns [about AI] but very few people are working on solutions to them". This suggests that if organisations can develop effective deepfake prevention software, it will serve as a unique selling point for the organisation, as a limited number of organisations can offer such solutions. This would incentivise organisations to shift their focus and implement strategies to prevent the threats posed by deepfakes while ensuring the safety of their users and customers. Nevertheless, one main finding from this study highlights the importance of having government regulation on deepfakes. For instance, to ensure that organisations are preventing fraudulent deepfake activities, under the new European code of conduct, technology companies can be penalised by up to 6 per cent of their annual revenue if measures to curb deepfake attacks are not implemented (Criddle, 2022, article #25). By doing so, organisations would be motivated to safeguard themselves from deepfake attacks. As such, the calls for regulations formulated in the *Financial Times* articles and the laws can be seen as targeted towards organisations.

Overall, the regulation theme in the *Financial Times* addresses all three deepfake risk levels, highlighting them as having equal importance. The articles emphasise the need for collaborative efforts between organisations and stakeholders from different levels to combat deepfakes effectively. This perspective suggests that instead of considering the three levels as distinct entities, they should be interconnected. By recognising these levels as connected, a more thorough and united approach can be developed to combat the risk of deepfakes. Moreover, the *Financial Times* emphasises the importance of organisations implementing measures to combat deepfakes. The articles acknowledged that organisations lack measures to counter the threats of deepfakes, aligning with de Rancourt-Raymond and Smaili's (2020) argument (supra). Hence, the *Financial Times* presents deepfakes as an opportunity for organisations to gain profitability, illustrating that organisations are more likely to take action if incentives are provided.

5. Conclusion

In contemporary society, the rapid advancements of artificial intelligence have brought about significant developments, including the rise of deepfakes. The emergence of deepfakes resulted in increased concerns about their threat towards individuals, organisations, and society. However, some organisations are still not implementing measures to combat these threats. In this case, the news media plays a pivotal role as they can influence the public's ideas and beliefs. Hence, analysing how the *Financial Times* addresses deepfake risks for companies is relevant as it can raise awareness and understanding of the organisational-level implications of deepfakes.

To conduct this study, a thematic analysis was employed to analyse a dataset of 55 news media articles obtained from the *Financial Times*, which resulted in three main themes: manipulation, security risk and regulation. This method of data analysis was used as it allows this study to understand the complexities of meaning within the articles by allowing for the categorisation and characterisation of the texts. Ultimately, the three themes derived from this analysis assisted in providing an answer to the main research question of how the *Financial Times* address the risks of deepfakes for companies. To support the research question, two other sub-research questions were developed. The first sub-research question focused on which levels of deepfake phenomena are present in the *Financial Times's* news coverage and how they are presented. While the second sub-research question investigated the key focuses in the *Financial Times's* coverage of organisational-level deepfake risks.

The first theme, manipulation, focuses on the exploitation of individuals and information through deepfakes. The *Financial Times* addresses this through discussion about non-consensual deepfake pornography, electoral manipulation through the use of synthetic social botnets, and the potential for impersonation. Secondly, the security risk theme discusses possible threats associated with deepfakes, including various scams, resulting in financial loss, reputational damage, and privacy issues. Furthermore, the discussion highlights how deepfakes can allow individuals to deny wrongdoing by claiming it was a deepfake, contributing to an information apocalypse. These two themes are closely related to the regulation theme, highlighting the need for collaborative efforts across the three deepfake levels to address deepfake risks effectively. The *Financial Times* stresses the importance of implementing education, awareness, and legal measures to mitigate the risks further. Notably, the *Financial Times* emphasises that combating deepfakes should not exclusively be the responsibility of the technical division but should be recognised as a concern for the entire business, including C-level executives.

Based on these themes, an answer to the research question is provided. The *Financial Times* coverage involves all deepfake risk levels but with varying emphasis. The societal level receives more coverage than individual and organisational levels, highlighting their greater significance. Regarding the organisational level, deepfake risks are predominantly addressed as financial and reputational

threats for companies. Moreover, the *Financial Times* discusses the need for collaboration between organisations and other levels to mitigate these threats effectively. The *Financial Times* presents this risk for companies as an opportunity to combat and gain profitability, thereby incentivising the implementation of countermeasures against deepfakes. This chapter will conclude this study by segregating it into three sections: the theoretical implications, societal implications, limitations and suggestions for future researchers.

5.1 Theoretical implications

When evaluating the theoretical implications of this research, it is apparent that numerous inferences can be drawn based on the results. While the study of deepfakes is not unconventional, it is worth noting that there is a lack of research on this subject, especially focusing on the organisational level within the news media. Thus, this study uses theories from various authors that looked into this topic from various perspectives. The findings from this study aligned with the prior studies introduced in the theoretical framework. However, some findings contradict prior studies, and some provided new insights.

Firstly, this study provides new insights and further understanding into deepfakes and their related risks. As such, one of the notable insights includes the liar's dividend, where deepfakes make it simpler for liars to refute the truth (Chesney & Citron, 2018). This is a cause for concern as when people get persistently exposed to fake information, it contributes to a state of reality apathy and information apocalypse as they would give up trying to determine the authenticity of the information, making them doubt all information (Dowdeswell & Goltz, 2020). Consequently, this leaves people susceptible to misinformation and disinformation, putting the reliability of businesses and news media organisations at risk.

Another notable finding from the results is that while deepfakes can erode people's trust in information, they can also reinforce existing beliefs. This relates to the concept of confirmation bias in which people are more inclined to believe information that confirms their existing views, even if they might be fake, aligning with Shin and Lee's (2022) and Dobber et al. (2021) finding on confirmation bias in deepfake news consumption.

Moreover, most of the causes of deepfake risks discussed in the *Financial Times* can be attributed to Bateman's common deepfake methods: (1) synthetic social botnets, (2) deepfake vishing, and (3) fabricated private remarks. To extend on Bateman's common deepfake methods, the findings found spear-phishing to be another common method of fraudulent deepfake use. Nonetheless, the findings suggest that although organisations have attempted to prevent these fraudulent deepfake activities, the measures implemented, such as banning, remain inefficient, aligning with Ferraro et al. (2020).

Another theoretical implication is that while the *Financial Times* does acknowledge the risks of deepfakes for organisations, there is a tendency for their coverage to focus more on the individual and societal levels rather than the organisational level. A prominent example can be seen in the discussions about non-consensual deepfake pornography, which primarily addresses societal concerns, supporting Godulla et al. (2021) and Goose and Burkell's (2020) argument (supra). However, this study's findings also contradict the arguments of Godulla et al. (2021) and Goose and Burkell (2020), as the security risk theme predominantly discusses the individual and organisational levels instead of the societal level, as the authors argued. Thus, it can be said that the significance given to either of the three deepfake risk levels in the *Financial Times's* coverage varies depending on the topic being discussed in the articles.

5.2 Societal implications

As a relatively new form of artificial intelligence, deepfakes remain an interesting and understudied phenomenon whose usage is unlikely to decrease due to the advancements in artificial intelligence. This study has shown that deepfakes can significantly threaten individuals, organisations and society. Hence, this study provides significant insights not only for individuals or society but also organisations, helping raise awareness of the threat that deepfakes can pose to their operations while providing possible solutions to mitigate such risks that could be beneficial and profitable for companies. Through emphasising the diverse nature of deepfake threats, this study encourages organisations to consider deepfake risks as a concern for the entire organisation rather than merely for technological division. Additionally, this study highlights news media organisations' significant role in addressing the risk of deepfakes. Specifically, the findings emphasised the need for unbiased and comprehensive coverage of deepfakes, avoiding bias towards any particular deepfake risk levels. This would allow news media organisations to improve their coverage of deepfakes and foster general understanding and knowledge of the deepfake phenomenon.

Furthermore, this study benefits policymakers by providing them with the regulatory suggestions covered in the *Financial Times*. By incorporating the insights and ideas presented in the *Financial Times*, policymakers can develop effective policies to address the risk of deepfakes and safeguard individuals, organisations and society.

5.3 Limitations and future research

Despite attempts made to ensure objectivity during the thematic analysis process of this study, it should be acknowledged that the results found were based solely on the interpretation of one researcher, which could lead to the subjectivity of the results. To mitigate this, this study recommends that future studies have multiple researchers analyse the data independently and compare and validate

their findings. This collaborative analysis process could help alleviate individual researchers' biases and improve the study's reliability and validity.

Furthermore, though the *Financial Times* was a suitable and primary source for this study's analysis and provided meaningful insights into deepfakes and the risk they pose for organisations, the findings of this study may only be generalisable to some news media articles. Thus, future researchers could improve this study's comprehensiveness and generalisability by including articles from other news media organisations. By analysing and comparing an analysis across various news sources, a greater comprehensive understanding of how the news media addresses the risk of deepfakes for companies can be obtained.

Another recommendation for future research to explore is the interconnected nature of the three deepfake risk levels. While this study has discussed the differences in coverage of the three levels by the *Financial Times*, it is crucial to acknowledge these levels as interconnected as they can influence one another. By exploring the relationship between these levels, future studies can offer a more in-depth understanding of the risks deepfakes pose and facilitate the development of a more unified approach to combat them effectively.

References

Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). The state of deepfakes: Landscape, threats and impact. https://regmedia.co.uk/2019/10/08/deepfake_report.pdf

Appel, M., & Prietzel, F. (2022). The detection of political deepfakes. *Journal of Computer-Mediated Communication*, 27(4). https://doi.org/10.1093/jcmc/zmac008

Astrid, C. (2021, November 30). *'Thematic analysis has travelled to places that we've never heard of'*. BPS. https://www.bps.org.uk/psychologist/thematic-analysis-has-travelled-places-weve-never-heard

Bansal, E., & Victoria, A. H. (2022). Deepfake detection. https://easychair.org/publications/preprint/7Nqc

Bateman, J. (2020). Deepfakes and synthetic media in the financial system: Assessing threat scenarios. https://carnegieendowment.org/files/Bateman_FinCyber_Deepfakes_final.pdf.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brooks, C. F. (2021). Popular discourse around deepfakes and the interdisciplinary challenge of fake video distribution. *Cyberpsychology, Behavior, and Social Networking*, 24(3), 159–163. https://doi.org/10.1089/cyber.2020.0183

Byman, D. L., Gao, C., Meserole, C., & Subrahmanian, V. S. (2023). Deepfakes and international conflict. https://www.brookings.edu/research/deepfakes-and-international-conflict/

Chesney, R., & Citron, D. K. (2018). Deep fakes: A looming challenge for privacy, democracy, and national security. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3213954

Collins, A. (2019). *Forged authenticity: governing deepfake risks*. Infoscience; EPFL International Risk Governance Center (IRGC). https://doi.org/10.5075/epfl-irgc-273296

Corbin, J., & Strauss, A. (2008). Basics of qualitative research (3rd ed.): Techniques and procedures for developing grounded theory. SAGE Publications, Inc. https://doi.org/10.4135/9781452230153

de Rancourt-Raymond, A., & Smaili, N. (2022). The unethical use of deepfakes. *Journal of Financial Crime*, *30*(4), 1066–1077. https://doi.org/10.1108/JFC-04-2022-0090

DeCuir-Gunby, J. T., Marshall, P. L., & McCulloch, A. W. (2011). Developing and using a codebook for the analysis of interview data: An example from a professional development research project. *Field Methods, 23*(2), 136–155. https://doi.org/10.1177/1525822X10388468

Dobber, T., Metoui, N., Trilling, D., Helberger, N., & de Vreese, C. (2021). Do (microtargeted) deepfakes have real effects on political attitudes? *The International Journal of Press/Politics, 26*(1), 69–91. https://doi.org/10.1177/1940161220944364

Dowdeswell, T. L., & Goltz, N. (2020). The clash of empires: Regulating technological threats to civil society. *Information & Communications Technology Law, 29*(2), 194–217. https://doi.org/10.1080/13600834.2020.1735060

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*. https://data.europa.eu/doi/10.2813/08370

Ferraro, M., Chipman, J., & Preston, S. (2020). Identifying the legal and business risks of disinformation and deepfakes: What every business needs to know. https://www.wilmerhale.com/en/insights/publications/20200622-wilmerhales-ferraro-chipman-and-preston-explain-in-article-what-companies-should-know-about-disinformation

Gamage, D., Chen, J., & Sasahara, K. (2021). The emergence of deepfakes and its societal implications: A systematic review.

Gamage, D., Ghasiya, P., Bonagiri, V., Whiting, M. E., & Sasahara, K. (2022). Are deepfakes concerning? Analyzing conversations of deepfakes on Reddit and exploring societal implications. *CHI Conference on Human Factors in Computing Systems*, 1–19. https://doi.org/10.1145/3491102.3517446

Godulla, A., Hoffmann, C. P., & Seibert, D. (2021). Dealing with deepfakes – an interdisciplinary examination of the state of research and implications for communication studies. *SCM Studies in Communication and Media, 10*(1), 72–96. https://doi.org/10.5771/2192-4007-2021-1-72

Gosse, C., & Burkell, J. (2020). Politics and porn: How news media characterizes problems presented by deepfakes. *Critical Studies in Media Communication, 37*(5), 497–511. https://doi.org/10.1080/15295036.2020.1832697

Gutsche, R. E. (2019). The state and future of television news studies: Theoretical perspectives, methodological problems, and practice. *Journalism Practice, 13*(9), 1034–1041. https://doi.org/10.1080/17512786.2019.1644965

Habgood-Coote, J. (2023). Deepfakes and the epistemic apocalypse. *Synthese, 201*(3), 103. https://doi.org/10.1007/s11229-023-04097-3

Hancock, J. T., & Bailenson, J. N. (2021). The social impact of deepfakes. *Cyberpsychology, Behavior, and Social Networking, 24*(3), 149–152. https://doi.org/10.1089/cyber.2021.29208.jth

Hanitzsch, T., & Vos, T. P. (2018). Journalism beyond democracy: A new look into journalistic roles in political and everyday life. *Journalism, 19*(2), 146–164. https://doi.org/10.1177/1464884916673386

Hasan, H., & Salah, K. (2019). Combating deepfake videos using blockchain and smart contracts. *IEEE Access, 7,* 41596–41606. https://doi.org/10.1109/ACCESS.2019.2905689

Karnouskos, S. (2020). Artificial Intelligence in Digital Media: The Era of Deepfakes. *IEEE Transactions on Technology and Society, 1*(3), 138-147. https://doi.org/10.1109/TTS.2020.3001312

Lee, Y., Huang, K.-T. (Tim), Blom, R., Schriner, R., & Ciccarelli, C. A. (2021). To believe or not to believe: Framing analysis of content and audience response of top 10 deepfake videos on YouTube. *Cyberpsychology, Behavior, and Social Networking, 24*(3), 153–158. https://doi.org/10.1089/cyber.2020.0176

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Higher Education, 9*(3), Article 3. https://ojs.aishe.org/index.php/aishe-j/article/view/335

Maras, M.-H., & Alexandrou, A. (2019). 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*(3), 255–262. https://doi.org/10.1177/1365712718807226

Marchetti, S. (2022). Rolling in the deep(fakes). *Bank of Italy Occasional Paper*. https://doi.org/10.2139/ssrn.4032831

Moran, R., & Golson, P. (2019). Enter the Imposter. https://www.brunswickgroup.com/disinformation-attacks-insight-research-integrity-i12018/

Newton Suter, W. (2012). Introduction to educational research: A critical thinking approach. *SAGE Publications, Inc*. https://doi.org/10.4135/9781483384443

Nguyen, D., & Hekman, E. (2022). The news framing of artificial intelligence: A critical exploration of how media discourses make sense of automation. *AI & Society*. https://doi.org/10.1007/s00146-022-01511-1

Nisbet, M. C., & Huge, M. (2006). Attention cycles and frames in the plant biotechnology debate: Managing power and participation through the press/policy connection. *Harvard International Journal of Press/Politics, 11*(2), 3–40. https://doi.org/10.1177/1081180X06286701

Novak, M. (2023, January 31). 25 Elon Musk impersonator scams on social media people actually fell for. *Forbes*. https://www.forbes.com/sites/mattnovak/2023/01/31/25-elon-musk-impersonator-scams-on-social-media-people-actually-fell-for/

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1609406917733847. https://doi.org/10.1177/1609406917733847

Omona, J. (2013). Sampling in qualitative research: Improving the quality of research outcomes in higher education. *Makerere Journal of Higher Education, 4*(2), Article 2. https://doi.org/10.4314/majohe.v4i2.4

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research, 42*(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Pantserev, K. A. (2020). The malicious use of AI-based deepfake technology as the new threat to psychological security and political stability. In H. Jahankhani, S. Kendzierskyj, N. Chelvachandran, & J. Ibarra (Eds.), *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity* (pp. 37–55). Springer International Publishing. https://doi.org/10.1007/978-3-030-35746-7_3

Pavlíková, M., Šenkýřová, B., & Drmola, J. (2021). Propaganda and disinformation go online. In M. Gregor & P. Mlejnková (Eds.), *Challenging Online Propaganda and Disinformation in the 21st Century* (pp. 43–74). Springer International Publishing. https://doi.org/10.1007/978-3-030-58624-9_2

Pinhanez, C. S., Flores, G. H., Vasconcelos, M. A., Qiao, M., Linck, N., de Paula, R., & Ong, Y. J. (2022). Towards a new science of disinformation. http://arxiv.org/abs/2204.01489

Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (2019). FaceForensics++: Learning to detect manipulated facial images. http://arxiv.org/abs/1901.08971

Shin, S. Y., & Lee, J. (2022). The effect of deepfake video on news credibility and corrective influence of cost-based knowledge about deepfakes. *Digital Journalism, 10*(3), 412–432. https://doi.org/10.1080/21670811.2022.2026797

Silverman, D. (2006). *Interpreting qualitative data: Methods for analyzing talk, text and interaction, 3rd ed*. Sage Publications Ltd.

Simmons, N. (2017). Axial Coding. In *The SAGE encyclopedia of communication research methods* (Vol. 1–4, pp. 80–82). SAGE Publications, Inc. https://doi.org/10.4135/9781483381411

Soratto, J., Pires de Pires, D., & Friese, S. (2020). Thematic content analysis using ATLAS.ti software: Potentialities for researchs in health. *Revista Brasileira de Enfermagem, 73*(3). https://doi.org/10.1590/0034-7167-2019-0250

Stenfors, T., Kajamaa, A., & Bennett, D. (2020). How to … assess the quality of qualitative research. *The Clinical Teacher, 17*(6), 596–599. https://doi.org/10.1111/tct.13242

Temir, E. (2020). Deepfake: New era in the age of disinformation & end of reliable journalism. doi:10.18094/JOSC.685338

Sloot, B. van der, & Wagensveld, Y. (2022). Deepfakes: Regulatory challenges for the synthetic society. *Computer Law & Security Review, 46*, 105716. https://doi.org/10.1016/j.clsr.2022.105716

van Huijstee, M., van Boheemen, P., Das, D., Nierling, L., Jahnel, J., & Karaboga, M. (2021). Tackling deepfakes in European policy. Publications Office. https://data.europa.eu/doi/10.2861/325063

Vreese, C. H. (2005). News framing: Theory and typology. *Information Design Journal, 13*(1), 51–62. https://doi.org/10.1075/idjdd.13.1.06vre

Wahl-Jorgensen, K., & Carlson, M. (2021). Conjecturing fearful futures: Journalistic discourses on deepfakes. *Journalism Practice, 15*(6), 803–820. https://doi.org/10.1080/17512786.2021.1908838

Walker, A. S. (2019). Preparing students for the fight against false information with visual verification and open source reporting. *Journalism & Mass Communication Educator, 74*(2), 227–239. https://doi-org.eur.idm.oclc.org/10.1177/1077695819831098

Weikmann, T., & Lecheler, S. (2023). Cutting through the hype: Understanding the implications of deepfakes for the fact-checking actor-network. *Digital Journalism*. https://doi.org/10.1080/21670811.2023.2194665

Williams, M., & Moser, T. (2019). The art of coding and thematic exploration in qualitative research. *International Management Review, 15*(1). http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v15n1art4.pdf

Yadlin-Segal, A., & Oppenheim, Y. (2021). Whose dystopia is it anyway? Deepfakes and social media regulation. *Convergence: The International Journal of Research into New Media Technologies, 27*(1), 36–51. https://doi.org/10.1177/1354856520923963

References: *Financial Times* Articles

Barrett, C. (2021, February 5). Where do the next generation of investors go from here? *Financial Times*. https://www.ft.com/content/f520cd54-98ba-44cc-85f2-88057b624ef8

Bradshaw, T. (2019, October 10). Deepfakes: Hollywood's quest to create the perfect digital human. *Financial Times*. https://www.ft.com/content/9df280dc-e9dd-11e9-a240-3b065ef5fc55

Cookson, C. (2020, January 3). Science: What breakthroughs will the 2020s bring? *Financial Times*. https://www.ft.com/content/19fb2702-2646-11ea-9a4f-963f0ec7e134

Criddle, C. (2022, July 6). Call for sharing of deepfake porn to be made illegal in the UK. *Financial Times*. https://www.ft.com/content/dca5309d-2f54-4922-80ec-cc28c274f328

Dodd, D. (2023, March 17). Banking crisis blurs central bank focus on inflation. *Financial Times*. https://www.ft.com/content/02d89960-9c45-4de0-b740-3a70411901e7

Facial recognition: Big data is watching you. (2019, September 15). *Financial Times*. https://www.ft.com/content/1ad2977a-5b57-3986-b225-582438d2b0f1

Ganesh, J. (2019, March 6). Fake news is a comfort blanket for moderates. *Financial Times*. https://www.ft.com/content/8dbe797a-3f31-11e9-b896-fe36ec32aece

Hall, T. (2019, February 11). Disinformation campaigns are distorting global news. *Financial Times*. https://www.ft.com/content/0df496e2-2a0b-11e9-9222-7024d72222bc

Hedge funds holding PG&E bonds score win in bankruptcy proceedings. (2019, October 11). *Financial Times*. https://www.ft.com/content/a0ac23e2-ebb7-11e9-a240-3b065ef5fc55

Huber, N. (2019, October 14). A hacker's paradise? 5G and cyber security. *Financial Times*. https://www.ft.com/content/74edc076-ca6f-11e9-af46-b09e8bfe60c0

Jack, A. (2022, February 13). MBAs and rankings must reflect new priorities. *Financial Times*. https://www.ft.com/content/47aba9c8-631b-41d6-8bbf-533be21dced2

Johnston, I. (2023, February 27). LinkedIn scammers step up sophistication of online attacks. *Financial Times*. https://www.ft.com/content/a8d262f4-5d52-4464-8714-e21a457aab33

Johnston, I., Criddle, C., & Cameron-Chileshe, J. (2022, November 28). UK government drops 'legal but harmful' clause from new online law. *Financial Times*. https://www.ft.com/content/8a97c03f-5b79-4441-9267-84fb56a4d55e

Kaminska, I. (2020, August 11). We cannot rely on a digital A-Team to fight deepfakes. *Financial Times*. https://www.ft.com/content/10781c77-5fa6-405a-85f6-a799e24172ff

Kew, S. F. (2020, August 17). Who's been spoofing the FT? *Financial Times*. https://www.ft.com/content/d79c644f-498f-4368-90fb-6603316c49f6

Manson, K., Murphy, H., Stefano, M. D., & McGee, P. (2020, March 20). Huge text message campaigns spread coronavirus fake news. *Financial Times*. https://www.ft.com/content/34b6df5a-ea4a-471f-8ac9-606580480049

McMorrow, R., Yang, Y., & Kruppa, M. (2021, May 22). ByteDance staff and investors shocked as founder steps back. *Financial Times*. https://www.ft.com/content/150e88ae-7ded-4400-9cb5-af2a6d765048

Minsky, C. (2019, November 20). Ecommerce turns to biometrics to validate shoppers. *Financial Times*. https://www.ft.com/content/5d8100b6-ca6e-11e9-af46-b09e8bfe60c0

Minsky, C. (2021, January 26). 'Deepfake' videos: To believe or not believe? *Financial Times*. https://www.ft.com/content/803767b7-2076-41e2-a587-1f13c77d1675

Moore, E. (2021, August 11). Lex Midweek Letter: Is there any merit to deepfakes? *Financial Times*. https://www.ft.com/content/757aef84-028c-4ea5-92a8-d8d2976f7f32

Mostert, F., & Franks, H. (2020, June 18). How to counter deepfakery in the eye of the digital deceiver. *Financial Times*. https://www.ft.com/content/ea85476e-a665-11ea-92e2-cbd9b7e28ee6

Murgia, M. (2022, February 16). Eric Schmidt creates $125mn fund for 'hard problems' in AI research. *Financial Times*. https://www.ft.com/content/68a4ba34-9785-411c-b7f6-3a9ae2f37cd6

Murgia, M. (2023, February 15). The Vatican and the moral conundrums of AI. *Financial Times*. https://www.ft.com/content/40ba0b91-7e72-415b-8ac6-4031252576cc

Murgia, M., & Daniels, J. (2023, March 17). Deepfake 'news' videos ramp up misinformation in Venezuela. *Financial Times*. https://www.ft.com/content/3a2b3d54-0954-443e-adef-073a4831cdbd

Murphy, H. (2019, August 16). Cyber security companies race to combat 'deepfake' technology. *Financial Times*. https://www.ft.com/content/63cd4010-bfce-11e9-b350-db00d509634e

Murphy, H. (2020, May 10). The new AI tools spreading fake news in politics and business. *Financial Times*. https://www.ft.com/content/55a39e92-8357-11ea-b872-8db45d5f6714

Murphy, H., & Reed, J. (2020, February 12). Facebook accuses telecoms groups of disinformation tactics. *Financial Times*. https://www.ft.com/content/1096ad54-4d5f-11ea-95a0-43d18ec715f5

Nicolaou, A. (2020, March 5). James Murdoch makes investment to combat fake news. *Financial Times*. https://www.ft.com/content/88406ad2-5e50-11ea-b0ab-339c2307bcd4

Nigam, N. (2021, February 2). Finland shows that education is best tool to fight 'deepfakes.' *Financial Times*. https://www.ft.com/content/3b51ce79-28b2-4931-81cd-9daffa4dcb16

Nuttall, C. (2019a, September 6). Taking apart the smartphone market. *Financial Times*. https://www.ft.com/content/c3e66590-d0c6-11e9-99a4-b5ded7a7fe3f

Nuttall, C. (2019b, October 24). Nokia plays generation game. *Financial Times*. https://www.ft.com/content/b73b9908-f67f-11e9-a79c-bc9acae3b654

Nuttall, C. (2019c, October 28). Facebook and faking it. *Financial Times*. https://www.ft.com/content/9e3b06a8-f9ab-11e9-98fd-4d6c20050229

Nuttall, C. (2020a, January 8). A brighter future for TVs at CES 2020. *Financial Times*. https://www.ft.com/content/d9a6f1c8-3242-11ea-9703-eea0cae3f0de

Nuttall, C. (2020b, January 21). Big Tech in doing good Davos do-over. *Financial Times*. https://www.ft.com/content/46adbac8-3c79-11ea-a01a-bae547046735

Nuttall, C. (2021, August 11). Samsung's foldable fallacy. *Financial Times*. https://www.ft.com/content/622d96fb-7e53-40a5-96c4-847e4362380c

Nuttall, C. (2022, July 7). China hacked off at spying claims. *Financial Times*. https://www.ft.com/content/30642cea-f529-438a-bede-72d0c4104d1b

Pichai, S. (2020, January 20). Why Google thinks we need to regulate AI. *Financial Times*. https://www.ft.com/content/3467659a-386d-11ea-ac3c-f68c10993b04

Smith, G., Meixler, E., & Vora, P. (2019, October 10). FirstFT: Today's top stories. *Financial Times*. https://www.ft.com/content/9bb887cc-eaa4-11e9-a240-3b065ef5fc55

Steer, G. (2022, September 29). Russia's cyber war that wasn't. *Financial Times*. https://www.ft.com/content/1315165d-3986-4671-972f-c1ce04104560

Thornhill, J. (2019, October 28). New tools are evolving in the fight against deepfakes. *Financial Times*. https://www.ft.com/content/4183b400-f960-11e9-98fd-4d6c20050229

Thornhill, J. (2021, July 29). Deepfakes threaten to inflate the 'liar's dividend.' *Financial Times*. https://www.ft.com/content/6e103e44-acc7-4136-9c37-58543507138a

Thornhill, J. (2023, February 4). Something for the weekend: Understanding AI. *Financial Times*. https://www.ft.com/content/b64d1291-e088-4dc5-a7ed-7bcb91b36a59

Venkataramakrishnan, S. (2019, October 14). Cyber fraud techniques evolve into confidence trick arms race. *Financial Times*. https://www.ft.com/content/005a8c04-e5bc-11e9-9743-db5a370481bc

Venkataramakrishnan, S. (2020a, January 21). Cyber security 2050: Hackers to tap smart cities and deep fakes. *Financial Times*. https://www.ft.com/content/ac865cbc-1c10-11ea-81f0-0c253907d3e0

Venkataramakrishnan, S. (2020b, October 13). After deepfakes, a new frontier of AI trickery: Fake faces. *Financial Times*. https://www.ft.com/content/b50d22ec-db98-4891-86da-af34f06d1cb1

Venkataramakrishnan, S. (2020c, October 13). Amazon gears up for a hard winter. *Financial Times*. https://www.ft.com/content/26b4d8c8-ff0d-48f6-a15e-e33447c4e9ed

Venkataramakrishnan, S. (2021, March 5). Behind the Tom Cruise deepfakes that can evade disinformation tools. *Financial Times*. https://www.ft.com/content/721da1df-a1e5-4e2f-97fe-6de633ed4826

Venkataramakrishnan, S. (2022, February 13). Why cyber threats are a C-suite issue. *Financial Times*. https://www.ft.com/content/c0615b72-5468-4559-9c54-aa2c2c04f9e9

Vincent, M. (2020, September 6). Banks work with fintechs to counter 'deepfake' fraud. *Financial Times*. https://www.ft.com/content/8a5fa5b2-6aac-41cf-aa52-5d0b90c41840

Walker, O. (2020, September 8). Pandemic speeds up push to digital as bank branches close. *Financial Times*. https://www.ft.com/content/9776a4f8-f957-49e3-ac06-3baad9588ee3

Warrell, H. (2020, April 27). UK intelligence urged to step up AI use to counter cyber threats. *Financial Times*. https://www.ft.com/content/1bbeaf4e-db11-4a67-af9e-5b90dc988859

Warrell, H. (2021, February 24). UK spy agency to use AI against cyber attacks and state actors. *Financial Times*. https://www.ft.com/content/2b32d454-1cbe-48e7-a12c-fdc2069b6d5c

Waters, R. (2019a, June 13). Rising tide of online deepfakes bring opportunities as well as risk. *Financial Times*. https://www.ft.com/content/1dd069ba-8df7-11e9-a1c1-51bf8f989972

Waters, R. (2019b, August 17). Tech's Dog Days. *Financial Times*. https://www.ft.com/content/9a68cf74-c085-11e9-b350-db00d509634e

Appendices

Appendix A: List of news media articles

Number	Article Name	Author
#1	Banking crisis blurs central bank focus on inflation	Dodd (2023)
#2	Deepfake ‘news’ videos ramp up misinformation in Venezuela	Daniels and Murgia (2023)
#3	LinkedIn scammers step up sophistication of online attacks	Johnston (2023)
#4	Something for the weekend	Thornhill (2023)
#5	The Vatican and the moral conundrums of AI	Murgia (2023)
#6	Cyber security 2050: hackers to tap smart cities and deep fakes	Venkataramakrishnan (2020a)
#7	UK intelligence urged to step up AI use to counter cyber threats	Warrell (2020)
#8	Russia’s cyber war that wasn’t	Steer (2022)
#9	Ecommerce turns to biometrics to validate shoppers	Minsky (2019)
#10	Deepfakes threaten to inflate the ‘liar’s dividend’	Thornhill (2021)
#11	Rising tide of online deepfakes bring opportunities as well as risk	Waters (2019a)
#12	Finland shows that education is best tool to fight ‘deepfakes’	Nigam (2021)
#13	Lex Midweek Letter: is there any merit to deepfakes?	Moore (2021)
#14	Banks work with fintechs to counter ‘deepfake’ fraud	Vincent (2020)
#15	What breakthroughs will the 2020s bring	Cookson (2020)
#16	Why cyber threats are a C-suite issue	Venkataramakrishnan (2022)

#17	How to counter deepfakery in the eye of the digital deceiver	Mostert and Franks (2020)
#18	Cyber security companies race to combat ‘deepfake’ technology	Murphy (2019)
#19	The new AI tools spreading fake news in politics and business	Murphy (2020)
#20	Why Google thinks we need to regulate AI	Pichai (2020)
#21	Taking apart the smartphone market	Nutall (2019)
#22	We cannot rely on a digital A-Team to fight deepfakes	Kaminska (2020)
#23	Disinformation campaigns are distorting global news	Hall (2019)
#24	Facebook and faking it	Nuttall (2019c)
#25	Call for sharing of deepfake porn to be made illegal in the UK	Criddle (2022)
#26	Who’s been spoofing the FT?	Kew (2020)
#27	‘Deepfake’ videos: to believe or not believe?	Minksy (2021)
#28	Cyber fraud techniques evolve into confidence trick arms race	Venkataramakrishnan (2019)
#29	Facebook accuses telecoms groups of disinformation tactics	Murphy and Reed (2020)
#30	Where do the next generation of investors go from here	Barrett (2021)
#31	Eric Schmidt creates $125mn fund for ‘hard problems’ in AI research	Murgia (2022)
#32	China hacked off at spying claims	Nuttall (2022)
#33	MBAs and rankings must reflect new priorities	Jack (2022)
#34	UK government drops ‘legal but harmful’ clause from new online law	Johnston et al. (2022)

#35	Behind the Tom Cruise deepfakes that can evade disinformation tools	Venkataramakrishnan (2021)
#36	ByteDance staff and investors shocked as founder steps back	Yang et al. (2021)
#37	Samsung's foldable fallacy	Nuttall (2021)
#38	UK spy agency to use AI against cyber attacks and state actors	Warrell (2021)
#39	A brighter future for TVs at CES 2020	Nuttall (2020a)
#40	After deepfakes, a new frontier of AI trickery: fake faces	(Venkataramakrishnan, 2020b)
#41	Amazon gears up for a hard winter	(Venkataramakrishnan, 2020c)
#42	Big Tech in doing good Davos do-over	Nuttall (2020b)
#43	Huge text message campaigns spread coronavirus fake news	Murphy et al. (2020)
#44	James Murdoch makes investment to combat fake news	Nicolaou (2020)
#45	Pandemic speeds up push to digital as bank branches close	Walker (2020)
#46	UK intelligence urged to step up AI use to counter cyber threats	Warrell (2020)
#47	A hacker's paradise: 5G and cyber security	Huber (2019)
#48	Deepfakes: Hollywood's quest to create the perfect digital human	Bradshaw (2019)
#49	Facial recognition: big data is watching you	"Facial Recognition,", (2019)
#50	Fake news is a comfort blanket for moderates	Ganesh (2019)
#51	FirstFT: Today's top stories	(Smith et al., 2019)
#52	Hedge funds holding PG&E bonds score win in bankruptcy proceedings	"Hedge Funds Holding PG&E Bonds Score

		Win in Bankruptcy Proceedings,", (2019)
#53	New tools are evolving in the fight against deepfakes	Thornhill (2019)
#54	Nokia plays generation game	Nuttall (2019b)
#55	Tech's Dog Days: Financial Times	Waters (2019)
#56	apart the smartphone market	Nuttall (2019a)

Appendix B: Coding Tree

Selective Codes (Themes)	**Axial Codes (Subcategory)**	**Example of Open Codes**
Manipulation	Electoral Manipulation	• Faked identities used to support government parties • Using “troll farms” to manipulate election results • Distort the public’s image of politicians • Tool for foreign-nation attacks
	Impersonation	• Supporting propaganda campaigns • Impersonation for financial gain • Decreasing stock prices • Unemployment
	Non-consensual pornography	• Women as primary targets of deepfakes • Content of civil rights campaigners • Fincial gain • Causing psychological distress
Security risks	Scams	• Cryptocurrency scams • Recruitment scam • Deepake employees
	Privacy issue	• Access to personal and financial details • Providing sensitive information
	Misuse and denial	• Excuse to deny wrongdoing • Confirmation bias
	Information apocalypse	• Erosion of trust • Causing liar's dividend
Legal and Regulatory Frameworks	Collaborative efforts	• Need for different levels to work together

		• Deepfake as a threat for whole organisation • Different levels working together to combat deepfakes
	Education and awareness	• Developing digital media literacy • Importance of awareness • Education on deepfakes
	Legal measures	• Opportunity for fraud prevention • Consequences if there are no measures