NFSU JOURNAL OF FORENSIC SCIENCE
ISSN: 3049-2408 (Online)
Journal Homepage: https://jfs.nfsu.ac.in/
DOI:10.63633/v3.i3.000030

Weaponizing Public Information: A Review of OSINT-Enabled Deepfake Types and Case Studies

Anouska Dutta[1,*], Hrishikesh Khedekar[2], Dr. T. K. Gundoor[3], Dr. Jovi Jose Salvador D'silva[4], Charudatta Korde[5]

[12345]School of Cybersecurity and Digital Forensics, National Forensic Sciences University, Goa, India

anouska.dutta@nfsu.ac.in (Corresponding Author) *

Abstract

"Deepfake" is a combination of the words "Deep Learning" and "Fake" which means anything manipulated or altered. Deepfakes are fake videos, images or audio recordings created using AI technology that are very realistic. The ease of creating deepfakes has gotten very easy due to the vast amount of personal information found online via social media, news and other public platforms. Open-Source Intelligence (OSINT) methods are used to sift through publicly available data to gain access to the photos, videos, and voice recordings needed to make these highly realistic deep-fakes and employ them in various ways to defraud, disinformation, and thieve identities. This paper takes a closer look at five practical examples of deepfakes which exploit OSINT. They're face-swapped news clips, impersonation clips of business executives, fake witness statements for courtroom evidence, political issue manipulation clips for context and voice cloning clips for phone scams. This study exemplifies the accessibility of public information being misused by cybercriminals to create unprecedented threats and the loss of trust and security in the digital world, using documented real-world examples.

Keywords: *Deepfake, Open-Source Intelligence, Impersonation, Fake Testimonies, Fabrications.*

1. Introduction

The rapid development in the field of computer science and technology has made it possible to quickly collect, analyze, and distribute information, which has brought unprecedented changes in all aspects of human life. However, the ease of access to publicly available information has led to an exponential increase in cybercrimes [1]. Specifically, different threat actors take advantage of weaknesses present in computer systems, networks, and human activity to perform massive cyberattacks with publicly available

information they have gathered in course of time. Open-Source Intelligence (OSINT) is a way of collecting or gathering information from publicly available sources. In the modern era of global interconnectedness, OSINT has come to be an extremely potent and indispensable tool in the context of gathering, processing, and corroborating publicly released information or data collected from numerous digital sources such as social media, news, websites, and multimedia content. It has a very important role in various fields from law enforcement agencies to cybersecurity experts to national security and journalism, allowing analysts to extract actionable insights from huge amounts of data that are freely available and do not require any special permission to use or access. Deepfakes refer to any digitized images, videos, or audiotapes, which are created using deep learning algorithms and artificial intelligence (AI) in order to generate highly realistic but fake content. To put it briefly, deepfakes are artificial media developed through deep learning algorithms and used to alter or produce realistic videos, sounds, or images. These fake forgeries created by AI can convince that someone said or did something that they did, and oftentimes, the fake content can be barely distinguished from reality. This type of deepfakes is commonly referred to as face swap ping [2].

The reason is that the perilous confluence of the OSINT method and deepfake technology creates a sharp turning point in cybersecurity. The publicly accessible information, including social media photographs, recordings of interviews, and contextual data, are now being used by malicious actors to generate hyper-realistic synthetic media which can be used to perpetrate unprecedented fraud, impersonation, and disinformation. The danger of this intersection is especially high due to the combination of two easily available resources: the rich and unregulated amount of data on the Internet and democratized AI tools, which make it possible to become a non-technical actor and engage in sophisticated attacks.

The reliability and authenticity of such information have become even more significant since the volume and velocity of online data continue to grow. OSINT is likewise vulnerable to manipulation and fake information, yet it provides an unlimited variety of possibilities of situational awareness and collection of real-time intelligence. The increased production of content and the development of artificial intelligence are putting a strain on the ability of an analyst to differentiate between real and fake content, and it has become very easy to develop believable digital content. This paper specifically examines the convergence of OSINT and deepfakes, analyzing how publicly accessible data enables and amplifies deepfake attacks. The impact of deepfakes, their numerous uses made possible by OSINT techniques, and the various kinds of deepfake assaults that exploit publicly accessible data are all examined in this study.

2. Literature Review

The literature review is organized into four thematic areas as shown in Table 1. The first four themes chronicle the maturation of deepfake technologies from simple manipulation through sophisticated, AI-driven attacks; the facilitation of such attacks through OSINT; and specific methods for implementing

deepfakes, such as face swap ping and voice cloning. Also highlighted is the need for key research gaps: while previous research has pointed to the potential weaponization of deepfakes and the vulnerabilities created for organizations, there has been no attempt to create a systematic taxonomy of deepfakes enabled by OSINT, which this paper addresses.

Table 1. Literature Review Summary: Deepfake Technologies, OSINT Enablement, and Emerging Threats

Topic / Theme	Examples
Deepfake Evolution & Technologies	Technologies Documented evolution from simple The use of manipulation to more complex deep learning models [3]. The majority of modern deepfakes are based on the Generative Adversarial Networks (GANs) - two competing neural networks for realistic content generation [4]. Variational Autoencoders These (VAEs) were designed for synthesis [5]. Four major deepfake appli cations identified: face swapping, face reenactment, A variety of facial attribute editing and talking face generation [6].
OSINT Role in Deepfake Creation	OSINT OSINT techniques involves the analysis of large amounts of public data, which are There is a wide range of threats that exploit to harvest training data from social. Media, interviews, live streams [7]. Generative AI creates The use of publicly available digital information to create deepfakes [8]. The number of deepfake scam attempts rose by 3,000% in 2023; projected global [9].
Face Swapping & Bio metric Bypass	95%+ of deepfakes online are created by DeepFaceLab. In the case of face swapping, there was no liveness check, which helped to contribute to this. A 704% surge in attacks on remote ID verification by deepfake technology in 2023 [10]. High-resolution images are built by attackers compiling data from press conferences, social media, public appearances and feed into AI models [11].
Voice Cloning & Vishing	Google's Mandiant Red Team demonstrated OSINT data collection techniques for employee impersonation attacks [12]. OpenAI Voice Engine clones' voices from 15-second samples; Google Tacotron/WaveNet produce near-perfect voice replicas [13].

Current studies show that there are important legal and technological gaps in the protection against the use of deepfakes. Existing laws fail to properly establish authenticity of deepfake evidence [14, 15] and detection technologies are not consistent [14]. The ease of creating a deepfake, along with OSINT's capacity to supply authentic contextual information [16] makes highly believable fabrications. While some studies have pointed to the possibility of weaponization for disinformation [17] and vulnerability of organizations [18], there is no universal taxonomy of OSINT-enabled deepfake attacks, which is addressed in this paper. There is indeed a critical gap of knowledge on how public information actually facilitates such attacks specifically. Although previous research has reported on methods of creating deep fake images and outlined their potential dangers, no research has been conducted on their manipulation of the images themselves. There is no systematic categorization of the different ways OSINT methods are used in the various deepfake attack vectors, which is necessary for a comprehensive weaponization for disinformation warfare. To date deep fakes and OSINT have generally been studied as distinct domains, without investigating the risks associated with their intersection. To fill this gap, the study will create a structured taxonomy of the categories of OSINT-enabled deepfakes. The categories are: face swapping in news media, impersonation videos for business, impersonation images of celebrities, fake photos of children on the internet, and fake photos of children in news media. In context, a fabrication that alters the truth, a synthetic testimony that corrupts the judiciary, executives undermining the judiciary. Political conversations, voice phishing attacks and authentication system bypasses. By analyzing real-world This research offers a classification of cases according to the OSINT techniques employed in each type of case and the mapping of the specific techniques used in each case type. growing understanding of how threat actors exploit public data to develop ever-more sophisticated attacks. sophisticated and damaging deepfake attacks.

3. Methodology

In this paper, using a structured literature review and in-depth case study approach, issues at the

intersection points of OSINT techniques and deepfake technology are explored.

3.1. Research Approach

The use of a qualitative research design was chosen to identify the patterns found in the publicly available information that enables the creation and deployment of a deep fake. This research creates a detailed taxonomy for OSINT-enabled deepfakes through the review of real-world incidents and engineering literature.

3.2. Data Collection

The keywords "deepfake", "OSINT", "face swapping", "voice cloning", and "synthetic media" were used

to conduct a systematic literature review from IEEE Xplore, ACM Digital Library, arXiv and Google Scholar for 2014-2024. Among the sources were fundamental research in deep learning [4] and [5] and detailed surveys of deepfakes [3] and [6]; cyber security reports from CrowdStrike [7] and IBM [9] and Google Mandiant [12] as well as technical documentation of tools such as DeepFaceLab [10] and voice generation technologies [13] and verified case studies, including those involving corporate fraud [19] and [21]-[23], entertainment [20], political manipulation [26] and [27], judicial contexts [24] and [25] and vishing attacks [28] and [29]. Special consideration was paid to publications from 2019 to 2024 to reflect the state of the art.

3.3. Analysis and Classification

Patterns were found in data sources used, such as social media, press conferences, and podcasts; data types collected, including voice recordings, facial images, and contextual data; and AI technologies employed, including GANs [4] and voice synthesis [13]. This analysis resulted in a taxonomy of five types: news media face swaps, impersonation videos, synthetic testimonies, contextual fabrications, and voice phishing, with several well-documented examples.

.

3.4. Case Selection

Cases were selected based on: (1) documented evidence from credible sources, (2) clear OSINT usage, (3) measurable impact, (4) occurrence within 2019-2024, and (5) geographic diversity across Asia [20], [23], [27], Europe [21], [26], and North America [22], [24], [28]. This ensures the taxonomy reflects actual threat patterns across corporate [21], [23], [28], [29], political [26], [27], judicial [24], [25], and social media [20] domains.

4. Deepfake Technology: OSINT-Enabled Threats

4.1. Impersonating

Produce a realistic fake video or voice recording of someone, primarily to trick into entering into an unauthorized transaction or some fraudulent activity. The role of OSINT is very important in that it allows video attackers to collect voice samples from podcasts, interviews, public speeches, and high resolution images from social media profiles and press conferences [11].

4.2. Disinformation & Defamation

The dissemination of false statements or damaging of reputations through the creation of audio or video recordings of public figures or people. The malicious actors then use OSINT methods to compile “real” information on actual videos, times, and persons involved, which results in convincing fake video footage of people saying or doing something they never actually said or did. Media manipulation can influence

election results, incite violence and tarnish reputations [7].

4.3. Terrorism

These terrorist groups use deepfake technology in order to enhance psychological operations and propaganda. Extremists analyze publicly available footage of political leaders, military operations, and even news broadcasts to produce hostage videos, doctor political speeches, or forge military operations that never happened. Realistic but untrue content instills fear, disseminates extremist ideologies, and discredits governments [7].

4.4. Social Engineering and Phishing Attacks

Attackers deceive people into taking an action based on fake deepfake content. OSINT reconnaissance yields highly detailed information about the organizational structure, communication patterns, relationships among employees, and operational procedures. Victims are deceived and either release funds or compromise passwords or provide unauthorized access to secure networks, resulting in severe personal, career, and financial consequences [18].

4.5. Extortion and Blackmail

The act of threatening victims that they will publish allegedly deepfake videos or pictures that are convincing, unless they pay ransom. OSINT helps perpetrators by availing facial images, voice records, and personal information about victims' social circles from publicly available domains. This deepfake extortion causes catastrophic psychological suffering and reputational harm, even when the material is completely fabricated [8].

4.6. Privacy Invasion and Identity Theft

The creators of deep fakes are able to infringe the privacy of individuals by overlaying their faces on adult or inappropriate movies. The availability of facial photographs and personal information in OSINT has everything the malicious actors need to recreate people in the form of realistic films or audio files. Besides contravening the will and dignity of the victim, these activities lead to cyber bullying, online harassment, psycho logical trauma, and permanent reputational losses [1].

These offenses prove that deepfakes can be very dangerous to the truth, privacy, and trust. In this regard therefore, they are putting an increasing threat to the digital forensics and information security communities across the globe.

5. Discussion on Types of Deepfake Using OSINT

5.1. Face Swaps in News Media

Swap faces Deepfakes provide OSINT to attack hyped newscast or viral content and swap the face of the original subject with that of a high-profile figure. Malicious actors get access to high-resolution images, videos of the target through publicly available sources like interviews, social media, and press conferences. This allows them to pro duce multifaceted, lifelike, and believable fake videotapes that are distributed to influence the opinion of people, harm the reputations of people, or spread false news. Real-world cases illustrate the destructive efficiency of face-swap-type attacks. In Hong Kong, a finance worker of a multinational company was duped into transferring $25 million to hackers using deepfake to impersonate the voice of the company's CFO and other employees in a faked video conference [19]. In India, actress Rashmika Mandanna's face was superimposed onto a video of British-Indian influencer Zara Patel, creating a deepfake that went viral across WhatsApp and Telegram, created by a 23 year-old fan to increase followers on his fan page from 90,000 to 1.08 lakh within two weeks [20].

5.2. Impersonation Videos

Impersonation videos are fake videos in which the personality, tone and style of a person have been artificially imitated to depict the person in action or saying something that he or she did not say. Attackers use OSINT to obtain as much information as pos sible about their targets as openly available, such as press conferences, interviews, YouTube channels, social media posts, and public appearances, in order to extract high resolution images, voice samples, facial expressions, and typical gestures. This publicly accessible information is then utilized to train AI models that form realistic computer versions of the target person. In February 2024, a finance employee at British engineering firm Arup was tricked into transferring $25 million during a video conference featuring synthetically altered AI-generated likenesses of the company's CFO and senior executives, constructed using publicly available YouTube footage [21]. Similarly, a smitten deepfake video of Elon Musk speaking to a cryptocurrency scam convinced an 82-year-old retiree to invest $690,000, with victims reporting the deepfake "looked and sounded just like Elon Musk," which demonstrates the sophistication of modern impersonation attacks [22]. In India, scammers used deepfake manipulated videos of Infosys founder N.R. Nara yana Murthy to defraud a 79-year-old woman in Bengaluru of ₹35 lakhs by luring her onto a bogus trading site, with similar videos featuring Murthy and Mukesh Ambani conning two additional victims out of ₹95 lakhs [23].

5.3. Synthetic Testimonies

The increase of deepfakes is a major test in terms of admissibility and credibility for digital evidence in courtrooms. Synthetic testimonies are created videos or audio recordings of a person making a false statement, confession, or witness statement. Deep fakes, created using OSINT to investigate actual events, e.g., protests, accidents, or crimes, can be made to fit the real background, location, or timeline.

The testimony will then appear real, yet completely untrue, and can be utilized to sway court cases, drive conspiracy theories, or sway emotions. A number of high-profile cases illustrate the dangers of synthetic testimony. The voice of a high school principal went viral making racist and antisemitic remarks; forensic analysis showed the recording was a deepfake created by the school's athletic director, requiring two forensic analysts to resolve the nature of the recording [24]. In the UK, in one child custody battle, fabricated audio of one parent making threats was introduced; in the United States, a principal's life and reputation were all destroyed until forensic evidence revealed the true origins of the audio [25]. These cases illustrate how OSINT-gathered contextual information about events, locations, and timelines can be used to craft plausible, false testimonies that undermine judicial integrity.

5.4. Contextual Fabrications

Contextual fabrications are deepfakes that are produced to look as if they were recorded in a particular location or during an actual event. Attackers use various OSINT techniques to learn the visual and environmental aspects of actual locations or previous events, like buildings, weather, or crowd behavior and then recreate those environments in imitated videos. This added background context makes the deepfake look more real, genuine and believable and thus it becomes difficult to identify the truth, especially when these kinds of content spread during breaking news or in politically sensitive situations. The most notable contextual fabrication occurred in 2022 when a deepfake video showing Ukrainian President Volodymyr Zelenskyy urging troops to surrender was placed on a hacked Ukrainian news website and broadcast on Ukraine 24 TV channel's news ticker, making it appear as legitimate Ukrainian media [26]. During India's 2024 general election, a deepfake video showed KT Rama Rao, a Telangana state leader, calling on people to vote for the opposition Congress party, which was widely shared on WhatsApp groups, while another deepfake showed Congress MP Manish Tewari making incendiary speeches in Haryanvi, a language he does not speak. More than 50 million AI-generated voice clone calls were made in the two months leading up to India's election [27].

5.5. Vishing

Voice phishing, or "vishing," refers to the technique of using AI-generated voice deepfakes to mimic any targeted individual over a phone call or voicemail. OSINT is utilized to obtain such voice samples, let’s say, from interviews conducted online, pod casts, or recorded speeches, which are then cloned using voice synthesis software. The attacker may then pose as someone trusted such as a boss or family member or someone among the knowns, to manipulate the targeted person into providing sensitive information, transferring money, or granting access to secure systems. This method is particularly risky in corporate or governmental environments where individuals deal with large amounts of data for many users. The sophistication of vishing attacks has evolved significantly with documented cases worldwide.

In 2024, a multinational firm's CEO received a call from what sounded like the company's UK-based managing director, with matching voice, identical tone, and perfect accent, urgently requesting that he transfer US$243,000 [28]. Rob Greig, Arup's Chief Information Officer, maintained that their $25 million attack used psychology and sophisticated deepfake technology to gain the confidence of employees, noting that with open-source software, one could create a moderately convincing deepfake video in around 45 minutes with limited technical ability [21].

6. Conclusion

This paper methodically discussed the dangerous intersection of Open-Source Intelligence and deepfake technology and how the information that is in the open has turned out to be a significant weakness in the digital ecosystem. Through systematic analysis of reported cases and technical literature, we have built a five-category taxonomy of OSINT-enabled deepfakes: face swaps in news media, executive impersonation videos, synthetic testimonies, contextual fabrications and voice phishing attacks. The severity of this threat is confirmed by real-life events. The Arup fraud, the at tempts of election interference in India and Ukraine, the creation of fake courtroom evidence, and advanced vishing campaigns proves that threat actors collectively collect visual and audio information on social media accounts, press conferences, podcasts and speeches by the population and create artificially real synthetic media. Democratizing 9 AI has enabled these advanced attacks to be available to non-technical attackers in these cases DeepFaceLab currently detects over 95% of online deepfakes, and voice cloning systems need only 15-second audio samples to create believable fakes. The existing countermeasures are not adequate since AI development is faster than detection technologies, and the current legal regulations do not provide a system to validate digital evidence. This study adds a formal insight into how OSINT methods support every type of deepfake attack, which can be used in the creation of custom defensive mechanisms. With the constantly increasing amount of publicly available data, a solution to the OSINT-powered deepfakes is imperative to maintaining trust, safety, and authenticity of digital communications.

References

[1] M. S. Rahman, "The Art of Open Source Intelligence (OSINT): Addressing Cybercrime, Opportunities, and Challenges," School of Computer Science and Technology, Xi'an Univ. of Posts & Telecommunications, Xi'an, China. [Online]. Available: https://pa pers.ssrn.com/sol3/papers.cfm?abstract_id=5281845

[2] M. S. Raghava, S. P. Tejashwini, K. Sree, A. Sneha, and R. Naveen, "AI Deep Fake Detec tion," International Journal of Novel Research and Development (IJNRD), vol. 8, no. 10, Oct. 2023. [Online]. Available: https://www.ijnrd.org/papers/IJNRD2310407.pdf

[3] T. T. Nguyen, Q. V. H. Nguyen, D. T. Nguyen, D. T. Nguyen, T. Huynh-The, S. Nahavandi, T. T. Nguyen, Q.-V. Pham, and C. M. Nguyen, "Deep learning for deepfakes creation and detection: A survey," Computer Vision and Image Understanding, vol. 223, p. 103525, Oct. 2022. [Online]. Available:

https://doi.org/10.1016/j.cviu.2022.103525

[4] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Cour ville, and Y. Bengio, "Generative adversarial nets," in Advances in Neural Information Pro cessing Systems 27 (NIPS 2014), Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, and K. Q. Weinberger, Eds. Montreal, Canada, 2014, pp. 2672–2680.

[5] D. P. Kingma and M. Welling, "Auto-encoding variational bayes," in Proc. 2nd International Conference on Learning Representations (ICLR), Banff, Canada, Apr. 2014. [Online]. Available: https://arxiv.org/abs/1312.6114

[6] G. Pei, J. Zhang, M. Hu, Z. Zhang, C. Wang, Y. Wu, G. Zhai, J. Yang, C. Shen, and D. Tao, "Deepfake generation and detection: A benchmark and survey," arXiv preprint arXiv:2403.17881, May 2024. [Online]. Available: https://arxiv.org/abs/2403.17881

[7] CrowdStrike, "2024 CrowdStrike Global Threat Report," Sunnyvale, CA, USA, 2024. [Online]. Available: https://www.crowdstrike.com/global-threat-report/

[8] A. S. Tham and S. Browne, "Deepfake scams have robbed companies of millions. Experts warn it could get worse," CNBC, May 2024. [Online]. Available: https://www.cnbc.com/2024/05/28/deepfake-scams-have-looted-millions-experts-warn-it could-get-worse.html

[9] IBM, "How a new wave of deepfake-driven cyber crime targets businesses," IBM Think Insights, Apr. 2025. [Online]. Available: https://www.ibm.com/think/insights/new-wave deepfake-cybercrime

[10] D. P. Kingma and M. Welling, "Auto-encoding variational bayes," in Proc. 2nd International Conference on Learning Representations (ICLR), Banff, Canada, Apr. 2014. [Online]. Available: https://arxiv.org/abs/1312.6114

[11] M. Shah, S. Pandey, D. Wang, and R. Singh, "Deepfake Media Generation and Detection in the Generative AI Era: A Survey and Outlook," arXiv preprint arXiv:2411.19537, Nov. 2024. [Online]. Available: https://arxiv.org/html/2411.19537v1

[12] Google Cloud Security, "AI-Powered Voice Spoofing for Next-Gen Vishing Attacks," Man diant Blog, July 2024. [Online]. Available: https://cloud.google.com/blog/topics/threat-in telligence/ai-powered-voice-spoofing-vishing-attacks

[13] "What Is Voice Cloning? Quick Guide to Spotting Voice Cloning Scams," SoSafe, May 2025. [Online]. Available: https://sosafe-awareness.com/glossary/voice-cloning/

[14] M. R. Grossman and Hon. P. W. Grimm, "Courts at the Crossroads: Confronting AI Generated Evidence in the Age of Deepfakes," Columbia Science & Technology Law Re view, May 2025. [Online]. Available: https://complexdiscovery.com/courts-at-the-cross roads-confronting-ai-generated-evidence-in-the-age-of-deepfakes/

[15] "Synthetic Media Creates New Authenticity Concerns for Legal Evidence," National Law Review, 2025. [Online]. Available: https://natlawreview.com/article/synthetic-media-cre ates-new-authenticity-concerns-legal-evidence

[16] "Deepfakes in the Courtroom: Problems and Solutions," Illinois State Bar Association, Mar. 2025. [Online]. Available: https://www.isba.org/sections/ai/newsletter/2025/03/deep fakesinthecourtroomproblemsandsolutions

[17] R. Chesney and D. K. Citron, "Deepfakes and the new disinformation war: The coming age of post-truth geopolitics," Foreign Affairs, vol. 98, no. 1, pp. 147–155, Jan./Feb. 2019.

[18] A. Alotaibi, M. Alruwaili, A. Alarifi, and M. Alosaimi, "Deepfake-driven social engineer ing: Threats, detection techniques, and defensive strategies in corporate environments," Journal of Cybersecurity and Privacy, vol. 5, no. 2, pp. 283–312, Apr. 2025. [Online]. Avail able: https://doi.org/10.3390/jcp5020018

[19] "7 Alarming Deepfake Attacks Examples You Need to Know 2025," Breacher, June 2025. [Online]. Available: https://breacher.ai/blog/deepfake-attack-examples/

[20] "Did it to get Instagram followers: How man behind Rashmika Mandanna deepfake was caught," Business Today, Jan. 2024. [Online]. Available: https://www.businesstoday.in/in dia/story/did-it-to-get-instagram-followers-how-man-behind-rashmika-mandanna-deep fake-was-caught-414295-2024-01-21

[21] World Economic Forum, "Cybercrime: Lessons learned from a $25m deepfake attack," Feb. 2025. [Online]. Available: https://www.weforum.org/stories/2025/02/deepfake-ai-cyber crime-arup/

[22] A. Hern, "Deepfake scams are on the rise – here's how to spot them," The Guardian, Oct. 2024. [Online]. Available: https://www.theguardian.com/technology/2024/oct/deepfake scams

[23] "Deepfakes in India: Rising Scams, Political Manipulation, and Legal Gaps," Outlook Busi ness, Aug. 2025. [Online]. Available: https://www.outlookbusiness.com/start-up/game-of shadows-indias-deepfake-dilemma

[24] "Maryland teacher arrested after principal allegedly framed with AI-generated racist rant," NBC News, Apr. 26, 2024. [Online]. Available: https://www.nbcnews.com/news/us news/teacher-arrested-ai-generated-racist-rant-maryland-school-principal-rcna149345

[25] D. W. Linna Jr. et al., "Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases," University of Chicago Legal Forum, Aug. 2024. stract_id=4943841 [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4943841

[26] S. Wakefield, "Ukraine deepfake video of Zelenskyy telling citizens to surrender is quickly debunked," CNBC, Mar. 2022. [Online]. Available: https://www.cnbc.com/2022/03/16/deepfake-video-of-zelenskyy-surrendering-de bunked.html

[27] "Deepfake democracy: Behind the AI trickery shaping India's 2024 election," Al Jazeera, Feb. 2024. [Online]. Available: https://www.aljazeera.com/news/2024/2/20/deepfake-democracy-behind-the-ai-trickery-shaping-indias-2024-elections

[28] "How a Deepfake Voice Almost Tricked a CEO," Web Asha Technologies, June 2025. [Online]. Available: https://www.webasha.com/blog/how-a-deepfake-voice-almost-tricked a-ceo