# LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

## (ISSN: 2583-7753)

**Volume 1 | Issue 4**

**2024**

# UNRAVELING THE IMPACT OF DEEPFAKES ON INTERNATIONAL CONFLICT THROUGH THE LENS OF INFORMATION WARFARE: AN ANALYSIS

**Shraddha Tiwari**[1]

## I. ABSTRACT

The emergence of deepfake technology in modern international context poses unprecedented threats to conventional frameworks for truth and originality. This legal paper on deepfake emphasizes the wide range of consequences that this phenomenon has not only concerning international agreements, diplomatic relations and security arrangements but also with respect to interrelations among states. Through revealing the history of deepfake development, this paper emphasizes its revolutionary effect on world affairs and especially for a part as an effective tool in the information warfare armory. The study conducts a critical analysis of international conventions, including the Geneva Conventions and International Covenant on Civil and Political Rights to evaluate their effectiveness in dealing with threats posed by deepfakes. Common examples of the key problems in contemporary legal frameworks are highlighted through case studies that present high-profile incidents such as The Pelosi Video Controversy, Navalny Poisoning Deepfake and EU Diplomatic Summit Incident drawing attention to a specialized approach needed for addressing deepfakes technology.

The paper makes policy recommendations, suggesting the necessary amendments to existing treaties and new international agreements targeted at emerging technologies. Cultural specifics for India, the United States of America and Great Britain are discussed, pointing out an importance that ethics and human rights issues have in the formation of legal framework. The recommendations attempt to simultaneously achieve the efficacy of legal measures enabling a fight against threats posed by deepfake and maintain individual rights for freedoms while respecting democratic values. The paper discusses

[1] Student at Christ University.

the necessity of international cooperation and also predicts the continuous evolution of deepfake, the challenges in forming a legal framework for the same and its execution both at national and Global level. It focuses on the variegated field of AI surveillance, analyzing its security impacts, scope opportunities as well as challenges in connection with international relations perspective. With the world's security framework adopting AI surveillance, this study offers a critical analysis of legal and ethical aspects surrounding its implementation. Special attention is given to the new role of technology companies, in which technological advancements need to be balanced with legal safeguards and ethical norms. The paper seeks to contribute ongoing discourses by unpacking the complex balance between AI surveillance, security pressures and responsibilities of critical actors in the digital era. The policy recommendations advocated by the author are essentially for legislative amendments in India's Information Technology Act, inclusion of deepfake related offenses in the legal system. Moreover, international collaboration is proposed through a Global Cybersecurity Agreement and a Transparency and Attribution Accords. Incorporation of human rights and ethics into policy frameworks to address the challenges posed by deepfake technology among countries and globally. The author concludes the paper by emphasizing the need for urgent and proactive measures to adopt international treaties and prevent information warfare and international conflicts among the countries in the near future.

## II. KEYWORDS:

*Deepfakes, Information warfare, International conflicts, International treaties, Global level, India, US, UK*

## III. INTRODUCTION

The development of deepfake technology in modern international affairs represents a major threat to the conventional concepts of reality and originality. However, deepfakes—highly advanced altered media material that is virtually indistinguishable from actual recordings—are now powerful weapons in the information warfare arsenal. This modern form of information warfare has emerged from a widespread and effective

use to manipulate the correct course of events, aimed at influencing people's political decisions. It is worth noting that the term "deepfake" emerged from two words – deep learning ad fake, showing how new technologies based on artificial intelligence are used to create falsified content such as forged videos or audio recordings.[2] This study focuses on the complex ramifications of deepfakes in international treaties, where this technological phenomenon overlaps not only with diplomatic relations but also security agreements and cooperation principles.

In the background of efforts to control and preserve equilibrium in international affairs, deepfake technology presents a unique problem. Malicious use of deepfakes that deliberately spread fake or tampered information can undermine the honesty at diplomatic negotiations, deteriorate national safety and increased rivalries between states. This paper seeks to investigate how current international agreements protect against the new risks posed by deepfakes and assess their ability to adjust in light of information warfare trends that are characterized by rapid technological developments. The study is contemporary, because the world faces an emerging threat – that of deepfake technological development and how it might affect diplomacy. Analyzing the situation with international treaties in this regard, this research attempts to assist ongoing discussion about strengthening legal frameworks that protect reliability and sustainability of international relations facing new threats. This paper analyzed the security ramifications as well as opportunities and challenges that are posed by deepfake technology will be discussed in detail on how it affects diplomatic relations. The research will also explore the relevant legal and ethical issues that form a part of ongoing discussions regarding measures for preservation of world stability amidst technological advances.

## IV. BACKGROUND

[2] Tom Simonite, "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be," WIRED, March 17, 2022, https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/ .

Deepfake technology's historical development goes back to artificial intelligence and machine learning innovations. The emergence of deep learning algorithms from the late 2010s opened up opportunities for synthesizing life-like audio and visual material. Deepfakes, which were first developed for entertainment purposes, soon turned into a powerful means of affecting international relations.

In recent years, deepfake cases have risen leading to dramatic shifts in diplomatic terrain. Some cases include modified videos depicting politicians using offensive statements or performing fake activities. These events propagated via social media and online networks have the capability to spoil sports, demolish public confidence along with exacerbating geopolitical problems. Now the 21st-century information system is faced with synthetic media such as deepfakes, a new form of disinformation that undermines our certainty about what happened and poses an additional layer to global discourse. At the same time, Information warfare is on the rise in the international arena and defines modern geopolitics. State and non-state actors use information as a strategic instrument, spreading disinformation so that they can undermine public opinion in order to disrupt the political process of other nations. Information warfare has successfully established itself as an integral part of international relations and politics; global conflicts have changed the ways. The point of the crossroads in terms of international relations is between deepfake technology and information warfare. As nations attempt to come into terms with the aftermath of manipulated media in this diplomatic forum, it is also needful for them to understand how deep fake evolved throughout history and its nuanced contemporary uptake alongside pervasive Information warfare – all elements that must amalgamate towards shaping appropriate responses additionally international regulatory framework as touchstone.[3]

## V. INTERNATIONAL TREATIES AND AGREEMENTS

[3] "A brief history of fake news," BBC News, December 4, 2020, https://www.bbc.co.uk/bitesize/articles/zwcgn9q .

Towering amidst the intricate landscape of global governance, a series of international treaties acts as barriers against emerging threats while information security plays a central role in contemporary diplomatic discourse. Many notable treaties, such as the Geneva Conventions and International Covenant on Civil and Political Rights have always demonstrated an imperative need to preserve information, especially during times of war. But the emergence of deepfake technology creates new problems for each one of these old agreements. The Geneva Conventions, developed in the wake of World War II were mainly aimed at protecting individuals during armed conflicts.[4] However, although these conventions touch upon the manipulation of information to a degree, they lack specific provisions for the intricacies of contemporary information warfare and deepfake-led disinformation campaigns. Just as the International Covenant on Civil and Political Rights, which highlights freedom of speech rights attempts in finding a way to strike balance between this right and mitigation, deepfakes use for political manipulation.

With the complexity of international treaties, we must analyze how these frameworks apply to emerging technologies. One of such instruments is the Treaty on Open Skies[5] that was conceived to facilitate transparency and confidence-building measures among member states. Although the treaty allows for aerial surveillance to check military activities, it does not consider how these media could be manipulated and used as tools in information warfare. The assessment of the gaps present in existing treaties uncovers a necessity for an elaborate document, which would focus on deepfake technology as well as its relation to international relations. But as the processes of negotiations go on, this must include an evaluation of whether existing treaties are sufficiently sophisticated to provide safeguards against weaponization through deepfakes and attempt engagement with achieving such innovation.

[4] Robert Chesney and Danielle Citron, "Deepfakes: A Looming Crisis for National Security, Democracy and Privacy?," Lawfare, February 21, 2018, https://www.lawfareblog.com/deepfakes-looming-crisis-national-security-democracy-and-privacy .
[5] Open Skies Treaty,March 24, 1992, 1843 U.N.T.S. 338 , Unites States of America.

## VI. LEGAL CHALLENGES IN ADDRESSING DEEPFAKE IN INTERNATIONAL TREATIES

With the proliferation of deepfake technology that blurs the limits between truth and reality, law becomes complicated when applying these topics to international treaties. By analyzing issues of jurisdiction to prosecute deepfake cases, one can see the complications that underlie transnational events. For example, the case of *R v. Varma*[6] in India 2020 had a jurisdictional challenge when an individual was implicated through deepfake video showing him committing fictitious illegal acts worldwide. In the absence of clear jurisdictional parameters, pursuing legal action against perpetrators was challenging while calling for a unified international strategy. An essential element of legal proceedings, attribution becomes harder and harder in the framework of deepfake assault. The 2018 "Putin on the Beach" deepfake incident, which portrayed the Russian President engaged in actions that had never occurred via AI-generated videos highlights this dilemma.[7] However, the inability to pinpoint such origins also poses questions of accountability which become particularly perplexing when deepfakes can be produced and released anonymously. These challenges jeopardize traditional legal norms grounded on identifying wrongdoers, prompting a critical review of attribution approaches within the context of international conventions.

The existing legal frameworks are put into question of their capability to deal with the sophisticated threats deepfakes proffer. One of the pertinent examples is the United Nations Convention against Transnational Organized Crime, commonly referred to as Palermo Convention.[8] Initially designed to tackle organized crime, its potential of dealing with deepfake crimes is doubtful. Though technologically facilitated crimes are not

[6] [2012] UKSC 42
[7] "A brief history of fake news," BBC News, December 4, 2020, https://www.bbc.co.uk/bitesize/articles/zwcgn9q .
[8] Izabella Kaminska, "A lesson in fake news from the info-wars of ancient Rome," Financial Times, January 17, 2017, https://www.ft.com/content/aaf2bb08-dca2-11e6-86ac-f253db7791c6 .

explicitly dealt with in the Convention, interpretations can leave behind obstacles to international prosecution and cooperation of dangerous deepfakers across borders. However, the deliberate application of deepfake technologies might constitute a breach of international law and particularly nonintervention principles. Although not specifically outlawed, such calculated use of deepfakes to cause interference in a foreign state's domestic affairs could be considered illegal intervention as defined by the customary international law. The various recent practices of states demonstrate an increasing recognition that manipulation of electoral systems is illegal intervention. Yet, the ambiguities of attributing deepfake to a particular state and fragmentation regarding its multiplicity can hinder assignation responsibility. In the context of armed conflict, in accordance with international law on military operations deepfakes dissemination is to ensure due diligence aimed at protecting civilians causing harm. Deep fakes in hybrid warfare, involving traditional military operations and covert forms of waging a conflict at the same time provide additional legal challenges more often than not when establishing some sort of 'legal gray zone' that confuses declaring anything as such.[9] In turn, the defending state is put in a dilemma between peaceable means and the threat to be met with armed response should hybrid threats prevail. Thus, it is clear that the transforming nature of deepfake technology requires a reconsideration of legal doctrine and its flexibility within an international treaties framework. When it comes to dealing with jurisdictional, attribution and framework dilemmas in the quest for justice associated with deepfake-related crimes, collaborative efforts – specifically international task forces and specialized tribunals could be crucial.

## VII. CASE STUDIES

### A. The Pelosi Video Controversy (2021):

[9] Greg Allen and Taniel Chan, "Artificial Intelligence and National Security," (Cambridge: Belfer Center for Science and International Affairs, July 2017), https://www.belfercenter.org/publication/artificial-intelligence-and-national-security .

The use of a manipulated deepfake video appeared in 2021.[10] It emphasized the destabilizing capacity of deepfakes. Although the viral nature of the video was a major problem, legal action did not flow easily due to jurisdictional issues. Indian and foreign cases are discussed in context of the Verma case that was brought for India's court, and *U.S. v. Doe*[11] precedent represents an evident difficulty to attribute liability across borders.[12] The incident underscored the requirement for more defined jurisdictional international norms when prosecuting deepfake crimes.

### B. The Navalny Poisoning Deepfake (2022):

In 2022, a deepfake video emerged which showed Russian opposition leader Alexei Navalny denying an attempted poisoning. It also prompted questions regarding the use of deepfakes within political propaganda. Previous international treaties, such as the Chemical Weapons Convention failed to address issues pertaining weaponized influencing media. This case revealed that the need to amend treaty content for digital risks of threat and political stability is urgent. Legal scholars urged rethinking of the Chemical Weapons Convention to include deepfakes-based disinformation campaign provisions.

### C. The EU Diplomatic Summit Incident (2019):

During the EU diplomatic summit, a deepfake video emerged which featured leaders in compromising positions. While the diplomatic backlash is possible, legal options were limited because treaties like Vienna Convention on Diplomatic Relations did not foresee media weaponization.[13] The scenario highlighted the importance for international

[10] "Fact check: 'Drunk' Nancy Pelosi video is manipulated," Reuters, August 3, 2020, https://www.reuters.com/article/uk-factcheck-nancypelosi-manipulated/fact-check-drunk-nancy-pelosi-video-is-manipulated-idUSKCN24Z2BI .
[11] 465 U.S. 605 (1984)
[12] Robert Chesney and Danielle Citron, "Deepfakes: A Looming Crisis for National Security, Democracy and Privacy?," Lawfare, February 21, 2018, https://www.lawfareblog.com/deepfakes-looming-crisis-national-security-democracy-and-privacy .
[13] Robert Chesney and Danielle Citron, "Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics," Foreign Affairs, January/ February 2019, https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war?cid=otr-authors-january_february_2019-121118 .

treaties to react quickly with all emerging threats. Scholars called for provisions in diplomatic conventions to be incorporated preventing abuse of deepfake technology destroying the sanctity of diplomacy.

### D. Rashmika Mandanna Deepfake video

The Delhi Police Special Cell on Friday filed an FIR in connection with the deepfake AI-generated video of actor Rashmika Mandanna. This week, a deepfake video depicting the actor in black exercise clothing inside an elevator spread through X and other social media sites. Zara's face was digitally manipulated and edited to Rashmika using powerful AI techniques. This FIR has been registered under Sections 465 (punishment for fraud) and 469 (forgery to slander or discredit a party), IPC 1860, as well as Section 70 of the IT Act. With respect to the deep fake AI-generated video of Rashmika Mandanna, an FIR u/s 465 and 469 of IPC,1860; section 67C and E in IT Act 2000 has been filed at PS Special Cell Delhi Police , Investigation onwards.

These case studies shed a beam of light upon the multi-dimensional complexity spawned by deepfake technology in international relations. They emphasize the shortcomings of present legal constructs and advocate an active strategy to improve international accords, adding clauses that target deepfake related difficulties. As we analyze these cases, the legal world must learn lessons that will help strengthen global legal systems in this dynamic context of information warfare.

## VIII. POLICY RECOMMENDATIONS

When considering the challenges of deepfake technology, a number of critical policy directives emerge for discussion. In India, a proactive approach means changing the existing law such as the Information Technology Act. When the digital image of an individual is transmitted or disseminated in mass media, violating its privacy, section 66E of IT Act applies.[14] The punishment for this crime is imprisonment up to three years

[14] Information Technology (Amendment) Act, 2008, § 66E.

or a fine of ₹2 lakh. One as well is the Section 66D of IT Act.[15] It offers a provision to prosecute an individual who uses communication devices or computer resources for unlawful purposes such as cheating, impersonation that may warrant imprisonment up to three years and/or fine upto ₹1 lakh. It is possible to prosecute the people who perpetrated deepfake cyber-attacks in India through these parts of the IT Act. This would include amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, making platforms responsible for malicious deepfakes dissemination. In the United States, a synergic legal backdrop could be created by adding deepfake-related offenses to CFAA thus creating a firm base for prosecuting those who exploit them for impinging on national security or public figures.[16] Also, the UK can improve its legal system by proposing amendments to Communications Act and enactment of legislation punishing citizens using deepfake technology in order to cheat public or sway democratic actions. Further, in 2023 Congress introduced the DEEP FAKES Accountability Bill that obliges deepfakes creators to mark their creations on online platforms and notifications of amendments provided about a specific video or other material. If such 'malicious deepfakes' are not labeled, the act of failure would be punishable under criminal law.

In January, the Cyberspace Administration of China introduced new rules limiting deep synthesis technology and combating misinformation. This policy allows any manipulated material through the technology to be marked and identifiable back in its source. Given the local laws, deep synthesis service providers should also retain ethics and keep correct political direction and public opinion orientation. The most advanced artificial intelligence regulations in the world will come to a stand-or-fall juncture for Europe. Social media giants like Google, Meta, and Twitter have been warned to start

[15] Information Technology (Amendment) Act, 2008, § 66D.
[16] Henry Farrell, Abraham Newman, and Jeremy Wallace, "Spirals of Delusion," Foreign Affairs, September/October 2022, https://www.foreignaffairs.com/world/spirals-delusion-artificial-intelligence-decision-making .

warning against the deepfake content or risk paying huge fines by the EU because they tightened their Code of Practice on Disinformation. The Code was initially introduced as a voluntary self-regulation tool in 2018, but will now be supported by the Digital Services Act that seeks to promote monitoring of digital platforms for control of different forms of abuse. Second, the EU AI Act proposal would hold deepfake providers liable under disclosure obligations.

Collaboration, therefore, is vital at the international stage. A possible Global Cybersecurity Agreement devised by major players such as India, the U.S., and the UK could develop a single platform that can be used to combat cyber threats including special provisions targeting deepfake technology for information warfare purposes. At the same time, a Transparency and Attribution Accord may be adopted, focusing on transparency with respect to the creation of AI technologies such as deepfakes.[17] This multilateral deal would promote interstate collaboration on tracking back the origin of deepfake incidents and thus, address limitations in allocating blame across nations. Human rights and ethics must be part of every policy making. Policies alignment with constitutional principles in India means drafting safeguards to uphold such human rights as privacy and freedom of speech. A strong ethical framework can direct the development and usage of deepfake technology responsibly. In the same manner, in America ethical issues may be incorporated into policies to ensure that laws uphold constitutional rights. An establishment of a federal body such as the Privacy and Civil Liberties Oversight Board could analyze ethical implications in emerging technologies like deepfakes. In the United Kingdom, policies should focus on human rights and while Information Commissioner's Office (ICO) plays a crucial role in ensuring that deepfakes regulations are aligned to the pledge of protecting individual freedoms including privacy and freedom of expression.[18] These policy recommendations, when implemented collectively, aim to find a delicate

[17] Lourdes Vasquez, "Recommendations for the Regulation of Deepfakes in the U.S.: Deepfake Laws Should Protect Everyone Not Only Public Figures" (unpublished manuscript, 2021),7.
[18] Ali Breland, "The Bizarre and Terrifying Case of the 'Deepfake' Video that Helped Bring an African Nation to the Brink," Mother Jones, March 15, 2019, https://www.motherjones.com/politics/2019/03/deepfakegabon-ali-bongo

middle ground between the need for legal structures aimed at fighting deepfake threats and the obligation towards maintaining human rights as well as democratic values. Implementing these recommendations at the national and international levels is imperative for strengthening global efforts to address the complexity of challenges brought by deepfake technology in the field of IR.

## IX. FUTURE OUTLOOK

The future of deepfake technology seems to be one where it will become more advanced, thus making the difference between altered content and reality more difficult. The availability of AI algorithms powering the deepfake is predicted to increase, allowing abuses with little resources they need. This development, however, foreshadows the possibility of an increase in targeted deepfake campaigns around the world focusing on political leaders and institutions that breed distrust by undermining social cohesion everywhere including India.[19] The adaptation of legal frameworks to effectively counter deepfake technology poses major challenges for India. Although some provisions do exist in the Information Technology Act, amendments may still need to be made when taking into account the complexity of deepfake-related offenses. Some of the projected challenges include setting up distinct lines for freedom of expression, liability in case offenders are platform owners and international jurisdiction protocols to send culprits behind bars.

Viewed from a global point of view, legal regimes globally may be unable to adapt quickly enough as technology develops at an extremely fast rate. The issues include getting the right kind of punishment for crimes committed with a deepfake, developing standard attribution's mechanism and encouraging international cooperation in

[19] Jason Lyall, Divided Armies: Inequality and Battlefield Performance in Modern War (Princeton University Press, 2020).

prosecuting such offenses. The harmonization of legal approaches across jurisdictions becomes a necessity to eliminate gaps between them that could be used by fraudsters. The importance of international coordination cannot be overstated with respect to the threats posed by deepfake technology. India's active participation in international forums is essential as a means of developing collective responses. By facilitating the exchange of best practices, technological expertise and intelligence to combat cross-border deepfake incidents, bilateral and multilateral engagements can promote such cooperation. India's resilience against such global deepfake threats can be increased through collaborative efforts with countries like the United States and the United Kingdom.

Considering the borderless nature of cyberspace, there is a need to have collaborative frameworks for sharing threat intelligence, coordinating investigations and harmonizing legal standards in order to facilitate global collaboration. India's involvement in international cybersecurity projects makes it an ideal candidate to play a major role in defining and guiding these shared ventures. However, as we move into the future deepfake technology will also require continued flexibility in legal frameworks and increased international coordination. As part of the international community, India must take a proactive approach towards influencing policies and formulating alliances to tackle deepfake's potential threats on external relations and democratic procedures.

## X. CONCLUSION

The author would like to conclude that this study emphasizes the urgency of preventative approaches towards adapting international treaties to a changing setting comprising information warfare and deepfake technology. As the study of case studies, legal battles and policies indicates, we face a fundamentally new nature of contemporary threats to global balance. The identified key findings reflect the worrisome effects created by deepfakes involving international relations across various countries like Pelosi video controversy and Navalny poisoning. Jurisdictional and attribution issues remain, demanding treaty amendments to address the peculiarities of international cybercrimes.

The development of new international agreements specific to emerging technologies, as reflected in such plans like the Global Cybersecurity Agreement cannot be overemphasized. However, the development of deepfake technology also requires an evolution of our legal frameworks to prevent malicious individuals and preserve global discourse. Adaptations in the areas of ethics, human rights and international cooperation should continue to be at the core. During this period of rapid technological change, international treaty strengthening is necessary to maintain the pillars on which diplomatic reciprocities stand in terms of truth and credibility. Failure to deal with these problems adequately would jeopardize the very basis of a stable and trusted world order.

 (ISSN: 2583-7753)