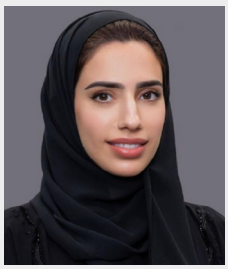
أكاديمية أنور قرقاش الدبلوماسية
ANWAR GARGASH DIPLOMATIC ACADEMY

دبلوماسية الابتكار
INNOVATIVE DIPLOMACY ID

AGDA Insight | MAY 2026

Digital Diplomacy: The Case of Deepfakes in Foreign Policy and Implications for the UAE

Shamma Mohammed Aldabal



Shamma Mohammed Aldabal

is Continuing Education Manager at the Anwar Gargash Diplomatic Academy (AGDA), overseeing executive programmes and professional certificates. With expertise in international affairs and human rights, she develops and delivers training on human rights, international organisations and intercultural communication. Previously, Shamma served as Instructor at Zayed University and Senior Researcher in the Human Rights Sector at the Community Development Authority. She holds an MSc in Human Rights from University College Dublin.

Executive Summary

- Social media platforms facilitate direct communication between governments and civil society, bypassing traditional media. This shift allows different actors to influence foreign audiences and achieve diplomatic goals more rapidly.
- Digital platforms have redefined diplomacy, making it more accessible and transparent. This integration of digitization in diplomacy, known as digital diplomacy, involves using digital platforms and tools to implement foreign policy objectives, and is becoming a common practice.
- However, this opens channels of misuse, particularly in relation to the use of artificial intelligence (AI) content in disinformation campaigns, which could impose threats on international relations.
- This Insight discusses the challenges posed by the technological advances in AI within the context of international relations and diplomacy. Specifically, it examines how the misuse of AI-generated synthetic media, or deepfakes, can undermine trust and credibility, increase security risks and escalate geopolitical tensions.
- The rapid technological advancements of today outpace national regulations and accountability measures, highlighting the urgent need for international governance on ethical use and accountability in the employment of AI-generated audio-visuals. However, creating this global framework could be challenging due to the lack of regulatory consensus among nations because of conflicting national interests, especially on issues like privacy and security.
- The Insight also investigates the potential implications of deepfakes for the United Arab Emirates› (UAE) diplomatic efforts, as well as the significance of this issue for the UAE›s foreign policy. In its National Strategy for Artificial Intelligence 2031, the UAE pledged to become one of the global AI leaders.
- The current risks and challenges that deepfakes pose to the UAE's diplomatic efforts are not different from those posed to the rest of the world. Deepfakes have short- and long-term effects on the country's reputation and credibility, especially given its role as an important mediator in the region and beyond. Nonetheless, the current gaps in global AI governance create an opportunity for the UAE to play a leading role in the standardisation of ethical guidelines in AI-generated content.
- The Insight concludes with recommendations that emphasise the need for technological advancements in AI detection tools and a push towards the application of regulatory frameworks to address existing challenges. Specifically, the Insight recommends:
  - » **implementing a national regulatory framework** that is concerned with disinformation campaigns, and creating intervention and prevention tools to effectively tackle the spread of false information across different age groups;
  - » **employing a collaborative approach** for addressing the challenges and opportunities of AI within diplomacy. This could be accomplished by developing a cross-sectoral framework and operationalising partnerships to implement international standards on media authentication and deepfake detection tools; and
  - » **establishing a centre with a cyber diplomacy mandate** that focuses on developing diplomatic frameworks on AI and crisis management protocols for responding to disinformation campaigns.

The Issue

The development of communication tools in public diplomacy has significantly changed in the past decade. Traditionally, the way governments have approached public diplomacy is through a government-to-public approach (G2P), which involves engaging with the international public to promote national and foreign policy objectives.[1] Recently, however, public diplomacy strategies have become more focused on people-to-people (P2P) interactions, where individuals from both the government and private sectors influence public attitudes and opinions towards a government's foreign policy decisions.[2] This strategy was used in several crises throughout recent years, ranging from the US presidential elections to the Gulf crisis of 2017. During the Gulf crisis, the Twitter platform (now known as X) was used as a medium to shape public discourse, as well as domestic and global perspectives on the situation.[3] For instance, a study suggested that during the crisis, Twitter was used in an unconventional manner, with ministers using the platform to issue official statements, announce the breaking of ties and highlight the rise of political tensions.[4] Additionally, there is a growing body of literature studying the effects of social media platforms, specifically Twitter, on US electoral outcomes. One study provided empirical evidence that social media affects US electoral outcomes and indicated that Twitter led to a reduced vote share for the Republican Party in the 2016 and 2020 presidential elections.[5] Both examples show the increasing use and influence of digital platforms within public discourse, which are now becoming a faster and cost-effective replacement for traditional methods.

The use of digital platforms has changed the way diplomacy is practiced, allowing it to become more direct, public and accessible, and this is seen as the norm today rather than an innovative practice. The unprecedented speed and wide reach of information collection and sharing today has allowed governments to spread messages and establish political plans beyond the scope of conventional channels.[6] Indeed, digital technologies are seen as 'influence amplifiers', as they help increase the diplomatic power of governments and international organisations.[7]

However, alongside the benefits of digital diplomacy lies the dark side of artificial intelligence (AI) and the role that it plays within diplomatic practices. As digital diplomacy in this context refers to the broad scheme of using online tools and techniques in diplomacy to enforce foreign policy objectives, AI naturally falls within that scope given its role in analysing, supporting or influencing decision-making in the diplomatic field. Nevertheless, AI poses a challenge due to the use of deepfakes as an instrument to destabilise international relations. AI is often misused by generating synthetic media of altered videos, photos, text, or audio, and these techniques are often used as tools within disinformation campaigns for malicious purposes. In the World Economic Forum's Global Risks Report 2024, the Global Risks Perception Survey 2023-2024 showed that 'misinformation and disinformation' is the most severe global risk that could arise in the following two years.[8]

The misuse of generative AI is an issue that is quite complex due to the different factions under which it falls. On the one hand, there are constant technological advancements, while on the other there are national and international regulatory institutions that find it difficult to keep up, all of which fall under constant geopolitical shifts and diplomatic tensions. Using AI to generate synthetic media has had and will continue to have consequences on international relations over the years, highlighting the dire need for regulation and accountability.

A Means to an End: The Use of Deepfakes in Conflict, Violence and Information Warfare

Truth is widely understood to be 'one of the first casualties of war', and it is also well understood that propaganda is a tool used in conflict settings.[9] Specifically, the weaponisation of information and the control of certain narratives is a strategic tool used in conflict. Today, this tool is being actively employed by malicious groups, non-state actors and civil society. The accessibility of generative AI tools has made the creation of high-quality audio-visuals, or deepfakes, a common commodity. As a result, different groups in society have been given influential power through the use of deepfakes as part of disinformation campaigns. Today, we see several examples of the implications of these campaigns, but the full extent of their consequences is difficult to predict with the constant advancement of AI technology.

The weaponisation of deepfakes in conflict:

The modern warfare environment has witnessed significant changes as a result of artificial intelligence, and deepfakes, which are used as a strategic tool in armed conflict settings, are some of the most disruptive technologies.[10] Accessible deepfake technology is allowing different actors to create 'realistic digital forgeries' and 'weaponized deepfakes', which threaten security and democratic entities.[11] Specifically, generative AI technology can allow malicious groups to produce convincing fake videos that have the potential to escalate conflict and harm diplomatic efforts, possibly hindering the potential for conflict resolution.[12] For instance, shortly after the Russian invasion of Ukraine, a notable attempt to use a deepfake in an armed conflict was made, with a video of President Zelensky asking Ukrainian soldiers and citizens to surrender.[13] The Ukrainian government, on the other hand, produced an 'educational deepfake' showing President Vladimir Putin describing Russia's war on Ukraine while walking around Mariupol, a Ukrainian city.[14] Additionally, deepfakes impede individuals' ability to form impartial opinions on the progress of war, and detection tools commonly used to target deepfakes are often not at the disposal of average users and their application is unsuitable for war contexts.[15] Furthermore, a study found that, during the Russia-Ukraine conflict, the 'lack of deepfake literacy' in its dataset prompted much misunderstanding of what characterises an actual deepfake, and that trying to increase awareness of deepfakes might have the opposite effect, potentially reducing trust in authentic video content.[16] In 2018, Gabonese president Ali Bongo suffered a health problem with limited government statements being provided to the public about his condition.[17] On December 31st of the same year, the president released a public video statement, but some people in Gabon doubted both the video's legitimacy and the president's ability to govern the country, while others reportedly attempted to prove that it was a deepfake.[18] Although the video was never officially confirmed as a deepfake, the misinformation surrounding it played a role in spurring unrest, contributing to the attempted coup that followed.[19] Incorporating certain AI tools, namely machine learning and autonomous systems, can also accelerate warfare situations, leaving less time for decision-making, and using deepfakes in particular can create high tension in little time.[20]

In addition to their role in fuelling conflict, deepfakes are likely to be used by anti-government extremists to instigate violence, and the anonymity involved in such types of extremism makes them even more dangerous.[21] Deepfakes can also be weaponised within conflicts and used as tools to target civil society, military operations and governments. They have particularly been used in grey zone warfare, including cyberattacks, information warfare and political coercion.[22] When it comes to the use of deepfakes in information warfare, this usually takes place in the context of disinformation campaigns, which spread falsified audio visuals to mislead a population. The proliferation of deepfakes during the war in Ukraine, for example, led the country's defence intelligence office to issue a warning about Russia's dissemination of deepfakes as part of its information warfare.[23] Information warfare involves hindering counterpart communication, done nowadays through cyber operations, as well as psychological warfare, in which information is manipulated for deception, and which has been increasing due to the introduction of audio and video manipulation.[24] Specifically, deepfakes can serve non-state actors including terrorist and mutinous groups, giving them the opportunity to promote extremism and violence.[25] Moreover, deepfake technology makes participation in large-scale information warfare less costly, and when used together with other technologies and social trends, deepfakes are most threatening, disseminating disinformation faster in the digital space and further lowering the already diminishing trust in democratic entities.[26] For example, in May 2023, a report was disseminated on Twitter claiming that an explosion had taken place at the Pentagon, giving people the impression that it was released by a trusted news agency and perpetuating a temporary drop in the S&P 500 index of about 30 points.[27]

Pixels and Politics: The Deepfake Dilemma in Global Diplomacy

Deepfakes are a multifaceted challenge to the diplomacy and international relations sphere; they are being used as catalysts to erode trust between states and discredit political leaders, and lead to the escalation of diplomatic crises when used amid high geopolitical tensions.[28] Deepfakes can also create a climate of mistrust when they are widespread across the media, causing scepticism even toward an authentic, direct line of communication.[29] Moreover, efforts to address the impact of deepfakes on the credibility of and trust in states, governments and diplomats are at risk due to the constant advancement of generative AI technology that could surpass existing deepfake detection tools.

Credibility – mistrust in a world of disinformation:

While the spread of disinformation has existed throughout history in global conflicts for various purposes, such as justifying wars and uprisings, spreading confusion and discrediting leaders, these efforts will now carry significantly more power due to the use of deepfakes.[30] In fact, deepfakes are often used by insurgent actors to target certain governments in an attempt to change the public's perception of them and erode trust.[31]

Spreading uncertainty about the truth has also become a strategic goal of 'state-sponsored propaganda', with malicious actors intentionally introducing disorienting and conflicting ideas into digital discourse.[32] As people become more uncertain about what they are exposed to in the media, suspicion even towards journalism can be exacerbated.[33] Because of this 'truth decay', the public's trust in major sources of information, such as the media and accurate political discourse, is undermined.[34] Real news could also be claimed by public figures to be deepfake content, a phenomenon referred to as 'the liar's dividend'.[35] Additionally, the rise in deepfakes may not only lead to official news agencies being delegitimised, but may also prompt viewers to choose to believe misinformation that aligns with their existing preconceptions.[36] Moreover, eliminating trust in news and photo/video content eliminates the trust shared within society, and people become unable to act on real perceptions of the world around them.[37] Furthermore, discussions based on factual information can become more difficult when users lack the ability to distinguish AI content and the content is subsequently disseminated, spreading misinformation and affecting communities.[38] The spread of fake news is also a time-sensitive issue, as the quick spread of information today sometimes makes it difficult for official channels to keep up and debunk false information. The misinformation impact of deepfakes may also be amplified when political microtargeting techniques are used, wherein targeted political advertisements are created for specific audiences.[39]

Accountability – can we keep up?

Technology is in a state of constant influx and advancement, and despite many national efforts to enforce AI-related laws, challenges remain. One major challenge is the fragmentation of AI governance on a global scale; the disparities in regulations across different jurisdictions allow malicious actors to exploit gaps and operate from countries with limited to no AI guidelines.[40] For instance, an organisation that is not allowed to spread AI content in the EU could be run from a country with more relaxed AI regulation whilst still being able to target EU audiences on online platforms.[41] Given the cross-boundary nature of the digital space and the ability of deepfakes to permeate physical and legal boundaries, the use of AI-generated synthetic media needs to be standardised. Governments are responsible for keeping up with the fast-paced advancements in technology and mitigating the consequences. Specifically, the continued advancement of deepfake technology requires the implementation of adaptive policy solutions to limit harm and protect individual rights, while also mitigating 'broader societal issues related to trust and truth'.[42]

Current regulatory challenges:

The increased speed of content dissemination as a result of online platforms like social media has posed challenges in mitigating the spread of disinformation. Regulating political deepfakes is especially challenging, particularly in the legal context.[43] With regard to using deepfakes for malicious purposes, legal prosecution requires proving intent with reasonable evidence, although there are cases, for instance, where deepfakes are used for art and satire, which are subjective.[44]

Furthermore, one of the main regulatory challenges involved in addressing the deepfake dilemma lies in the disparities in governments' priorities when it comes to synthetic media, leading to non-uniformity with regards to regulation, and regulations that contradict or overlap make regulatory compliance especially challenging for global technology companies based in multiple jurisdictions.[45]

Although the US Congress has passed the National Defence Authorization Act (NDAA), which mandates the Director of National Intelligence to report instances of deepfake use by foreign governments, the introduction of this act does not take into consideration the repercussions of deepfake use within the country.[46] In fact, there is no federal legislation in the United States to mitigate the threats that deepfake technology could impose within the country, and only five states have introduced legislations focused on emerging deepfake technologies.[47] Moreover, the regulation of websites and applications in the US is left to the creators who set their own usage guidelines, but when multiple online platforms have different guidelines, it leads to non-uniform regulations.[48] Additionally, while some existing laws prohibit the deliberate dissemination of harmful misinformation in the country, their reach is constrained,

particularly on an international level.[49] Identifying actors involved in the creation of deepfakes is difficult, and the perpetrators could be located beyond national borders.[50]

Relying only on national efforts could result in divided international regulations, and the need to implement transnational AI regulations is beginning to be acknowledged by international organisations.[51] Although governments' preparedness for a future driven by AI technology has already began, the elevated level of certain AI threats will likely need to be met by coordinated global efforts and the introduction of penalties for violating international standards.[52]

False Faces and Real Consequences: Implications for the UAE's Diplomatic Efforts

The Gulf is emerging as a 'global technology hub', and the UAE in particular has invested $148 billion in AI both nationally and internationally since 2024, as well as partnered with internationally leading technology companies.[53] As outlined in the UAE National Strategy for Artificial Intelligence 2031, however, it is important to ensure the presence of a legal environment capable of supporting innovation and, more specifically, AI implementation; innovations in AI often involve quick regulatory developments and may have negative consequences on a societal level.[54]

In the UAE, the repercussions of disseminating deepfakes depend on the intention behind the dissemination, as opposed to the act of creating the deepfake itself. The UAE Penal Code law, among other laws, provides clear penalties for engaging in fraud, defamation and cybercrimes, without any explicit mention of deepfakes. For example, Federal Decree-Law No. (34) of 2021 criminalises cyber-related deception.[55] However, there is no law that specifically focuses on the dissemination of deepfakes or their misuse. Although there is an AI Ethics Guideline issued by the UAE government which pushes for responsible and transparent AI use, there is no legal requirement for people to disclose that a piece of content has been AI-generated.

From a diplomatic standpoint, deepfakes pose an immediate and long-term risk to the UAE's reputation and credibility, both of which are important pillars of its diplomatic efforts, especially given its role as a mediator in dialogue and de-escalation in the region and beyond. These effects on the existing narrative of the government or leadership can damage any current or future efforts made by the UAE to play this intermediary role. Although the UAE's image today is one of credibility and trust, deepfakes can have a direct effect on the country's regional and international efforts by influencing perceptions of its narrative and stance on certain geopolitical issues. This could impact not only its general reputation but also its bilateral relations, especially with countries that do not have the infrastructure for content verification. This, in turn, could influence decision-making, spark tension and mistrust or disrupt bilateral diplomatic efforts.

To address the lingering challenge of deepfake use, the foreign policy community could lead an international dialogue on establishing standards with regard to the use of reliable communication on both a country-to-country and an individual level, aimed at developing secure communication spaces and creating a medium for countering disinformation, as well as facilitating the sharing of best practices in mitigating deceptive AI tools.[56] However, when holding discussions on global regulatory frameworks, it is important to establish ways to detect misinformation on a G2G level to ensure that relations are intact and tensions are not heightened.

Current gaps in technology platforms provide a clear opportunity for the UAE to lead on this issue; it could be a key player in regional and international governance and significantly contribute to developing standards on digital content use and deepfake detection and regulation, among other ethical issues. Moreover, the UAE could use bilateral or multilateral platforms to push for international cooperation to combat cross-border threats resulting from deepfakes, in addition to initiating cross-sector dialogue with multiple actors to ensure uniformity in public policy decisions.

Conclusion and Policy Recommendations

The diplomatic landscape has witnessed a shift in the tools used to influence public discourse and foreign policy. Whether through engagement by the government with the public, or engagement between people, the pace and efficiency of direct communication through digitisation has replaced traditional tools of media influence. However,

this shift has presented an opportunity for malicious actors to influence political discourse by perpetuating false information or news on digital platforms via AI-generated content such as deepfakes. To incite violence or unrest, such actors have repeatedly created disinformation campaigns on these platforms, posing a continuous challenge for diplomatic efforts and institutions as they rigorously try to enforce countermeasures.

This dilemma carries a range of concerns surrounding aspects such as mistrust in governmental and media institutions, the role of deepfakes in conflict and the lack of a unified international framework to address disinformation campaigns. Concerns about accountability and legality are also present and have been discussed and debated relentlessly. Additionally, governments face regulatory challenges in liability and the prosecution of malicious actors who, due to the constant advancements in anti-detection tools, are difficult to apprehend.

The UAE has actively engaged in and shaped the digital diplomacy landscape. However, it faces similar challenges as those faced by other governments regarding the impact of deepfakes on public and diplomatic discourse. Nevertheless, highlighting the existing gaps and promoting best practices will create opportunities for more efficient countermeasures. This Insight provides the following recommendations that the UAE and other governments can consider to better mitigate the risks posed by deepfakes:

1. Implementing a comprehensive regulatory framework. A national regulatory framework on the use and misuse of synthetic media could be an appropriate strategy, especially if the internet or social media platforms more specifically are unable to prevent the spread of misinformation. To counter the challenges associated with AI and deepfake technology, a 'multifaceted approach' needs to be implemented, spanning not only technology-focused efforts but also regulatory and diplomatic ones.[57] In this context, governments, technology companies and research institutions could work together to implement such measures.[58]

2. Pursuing cross-sector/cross-country partnerships. Enhancing engagement with different sectors and countries to discuss the opportunities and risks of AI within international relations and diplomacy is another key strategy. As with other issues that have both a direct and indirect impact on international politics, AI should be the focus of credible and reputable governments, playing a mediating role by providing a platform to discuss common challenges. Additionally, partnerships between governments and the private sector through collaborative research and other approaches are crucial in developing detection tools targeting synthetic media use.

3. Developing a cyber diplomacy mandate. Establishing a centre that acts as an advisory body for developing regulatory and legal frameworks, analysing risks associated with technology and diplomacy, streamlining content verification in real-time, investing in research and development (R&D), and supporting deepfake crisis management protocols could be influential. The mandate could also include awareness-raising and training initiatives for diplomats and government officials on diplomatic digital literacy, content verification and the development of a centralised platform to counter disinformation campaigns.

Endnotes

1. Snow, N., & Taylor, P.M.(Eds.). (2008). Routledge handbook of public diplomacy. Routledge.
2. Ibid
3. Frey, C. (2024). Digital diplomacy: The impact of technology on modern diplomacy and foreign policy: Current realities and future prospects. Romanian Journal of European Affairs, 24(1), 107–126. http://dx.doi.org/10.2139/ssrn.4864962
4. Al-Mansouri, T., Al-Mohannadi, H., & Feroun, M. (2021). Digital diplomacy during the first 100 days: How GCC ministries of foreign affairs and ministers tweeted the blockade. QScience Connect, 2021(2). https://doi.org/10.5339/connect.2021.spt.1
5. Fujiwara, T., Müller, K., & Schwarz, C. (2024). The effect of social media on elections: Evidence from the United States. Journal of the European Economic Association, 22(3), 1495–1539. https://doi.org/10.1093/jeea/jvad058
6. Adesina, O. S. (2017). Foreign policy in an era of digital diplomacy. Cogent Social Sciences, 3(1). https://doi.org/10.1080/23311886.2017.1297175
7. Bjola, C., & Zaiotti, R. (Eds.). (2021). Digital diplomacy and international organisations: Autonomy, legitimacy and contestation (1st ed.). Routledge. https://doi.org/10.4324/9781003032724
8. World Economic Forum. (2024). The Global Risks Report 2024 (19th ed.). https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
9. Kleemann, A. (2023). Deepfakes—when we can no longer believe our eyes and ears: Media manipulation in conflict. Challenges and responses (SWP Comment 2023/C52). Stiftung Wissenschaft und Politik (SWP). https://doi.org/10.18449/2023C52
10. Akkuş, B. (2025). Deepfakes and the Geneva Conventions: Does deceptive AI-generated misinformation directed at an enemy during armed conflict violate international humanitarian law? A critical discussion. Laws, 14(83). https://doi.org/10.3390/laws14060083
11. Schroeder, R., Tan, K., Nadaf, A., & Neyazi, T. (2024). Does trust in government moderate perceptions towards deepfakes? Comparative perspectives from Asia on the risks of AI and misinformation for democracy. Government Information Quarterly, 41(4). https://doi.org/10.1016/j.giq.2024.101980
12. Salvi, A. (2024). The attack of the clones: deepfakes and the evolving landscape of disinformation. In Kovalčíková, N. (Ed.), Hacking minds and machines: Foreign interference in the digital era (pp. 32-40). European Union Institute forSecurityStudies.https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_184.pdf
13. Ibid.
14. Kuźnicka-Błaszkowska, D., & Kostyuk, N. (2025). Emerging need to regulate deepfakes in international law: The Russo–Ukrainian war as an example. Journal of Cybersecurity, 11(1). https://doi.org/10.1093/cybsec/tyaf008
15. Ibid.
16. Twomey, J., Ching, D., Aylett, M.P., Quayle, M., Linehan, C., & Murphy, G. (2023). Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine. PLOS ONE, 18(10), 15–16. https://doi.org/10.1371/journal.pone.0291668
17. Grossman, D. (2020). How a sick president, a suspect video and a midnight broadcast helped spark an attempted coup in Gabon. The Washington Post. https://www.washingtonpost.com/politics/2020/02/13/how-sick-president-suspect-video-helped-sparked-an-attempted-coup-gabon/
18. Ibid
19. Ibid.
20. Boulanin, V., Saalman, L., Topychkanov, P., Su, F., & Carlsson, M. P. (2020). Artificial intelligence, strategic stability and nuclear risk. Stockholm International Peace Research Institute. http://www.jstor.org/stable/resrep25355
21. Busch, E., & Ware, J. (2023). The weaponization of deepfakes: Digital deception on the far-right. International Centre for Counter-Terrorism. https://doi.org/10.19165/2023.2.07

22. Cooke, D., Edwards, A., Day, A., Nair, D., Barkoff, S., & Kelly, K. (2024). Crossing the deepfake rubicon: The maturing synthetic media threat landscape. Center for Strategic & International Studies. https://www.csis.org/analysis/crossing-deepfake-rubicon

23. Salvi, A. (2024). The attack of the clones: deepfakes and the evolving landscape of disinformation. In Kovalčíková, N. (Ed.), Hacking minds and machines: Foreign interference in the digital era (pp. 32-40). European Union Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_184.pdf

24. Ayaegbumam, I., & Fidelis, N. (2024). The intersection of artificial intelligence, deepfake, and the politics of international diplomacy. Ianna Journal of Interdisciplinary Studies, 6(2), 53 – 71. https://doi.org/10.5281/zenodo.11393419

25. Chesney, R., & Citron, D. (2018). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. Foreign Affairs. https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war

26. Smith, H., & Mansted, K. (2020). Weaponised deep fakes: National security and democracy (Report No. 28/2020). Australian Strategic Policy Institute. https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2020-04/Weaponised%20deep%20fakes.pdf?VersionId=lgwT9eN66cRbWTovhN74WI2z4zO4zJ5H

27. Kleemann, A. (2023). Deepfakes - when we can no longer believe our eyes and ears: Media manipulation in conflict. Challenges and responses (SWP Comment 2023/C52). Stiftung Wissenschaft und Politik (SWP). https://doi.org/10.18449/2023C52

28. Salih, M. H. B., Bukhari, S. S., Liaqat, I., Majeed, A., Noman, M., & Siddiqui, A. A. (2025). Deepfake diplomacy and international relations: Assessing the impact of AI-generated media on global trust, diplomatic engagement, and conflict escalation. Advance Social Science Archive Journal, 4(1), 2731–2737. https://doi.org/10.5281/zenodo.16903863

29. Ibid

30. Byman, D.L., Gao, C., Meserole, C., & Subrahmanian, V.S. (2023). Deepfakes and international conflict. Foreign Policy at Brookings. https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf

31. Williams, R., & Otto, L. (2022).Artificial intelligence as a tool of public diplomacy: Communication between the United States and Iran. The Thinker, 90(1). https://doi.org/10.36615/thethinker.v90i1.1171

32. Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. Social Media + Society, 6(1). https://doi.org/10.1177/205630512090340

33. Weikmann, T., Greber, H., & Nikolaou, A. (2025). After deception: How falling for a deepfake affects the way we see, hear, and experience media. The International Journal of Press/Politics, 30(1), 187–210. https://doi.org/10.1177/19401612241233539

34. Momeni, M. (2025). Artificial intelligence and political deepfakes: Shaping citizen perceptions through misinformation. Journal of Creative Communications, 20(1), 41–56. https://doi.org/10.1177/09732586241277335

35. Schiff, K.J., Bueno, N.S, & Schiff, D.S. (2024). The liar's dividend: Can politicians claim misinformation to evade accountability? American Political Science Review, 119(1), 71-90. doi:10.1017/S0003055423001454

36. Weiner, M. D. (2024). Destined to deceive: The need to regulate deepfakes with a foreseeable harm standard. Michigan Law Review, 122(4), 771-807. https://doi.org/10.36644/mlr.122.4.destined

37. 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

38. Momeni, M. (2025). Artificial intelligence and political deepfakes: Shaping citizen perceptions through misinformation. Journal of Creative Communications, 20(1), 41–56. https://doi.org/10.1177/09732586241277335

39. 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

40. Romanishyn, A., Malytska, O., & Goncharuk, V. (2025). AI-driven disinformation: Policy recommendations for democratic resilience. Frontiers in Artificial Intelligence, 8. https://doi.org/10.3389/frai.2025.1569115

41. Ibid.

42. Birrer, A., & Just, N. (2024). What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape. New Media & Society, 27(12), 6819-6838. DOI: 10.1177/14614448241253138.

43. Ramluckan, T. (2024). Deepfakes: The legal implications. In Proceedings of the International Conference on Cyber Warfare and Security (pp. 282–288). Academic Conferences International Limited.

44. Ibid.

45. He, X., & Fang, L. (2024). Regulatory challenges in synthetic media governance: Policy frameworks for AI-generated content across image, video, and social platforms. Journal of Robotic Process Automation, AI Integration, and Workflow Optimization, 9(12), 36-54. https://helexscience.com/index.php/JRPAAIW/article/view/2024-12-13

46. Quirk, C. (2023). The High Stakes of Deepfakes: The Growing Necessity of Federal Legislation to Regulate This Rapidly Evolving Technology. The Princeton Legal Journal. Accessed on February, 2026. Accessible on: https://legaljournal.princeton.edu/the-high-stakes-of-deepfakes-the-growing-necessity-of-federal-legislation-to-regulate-this-rapidly-evolving-technology/

47. Ibid.

48. Nnamdi, N., Oniyinde, O.A., & Abegunde, B. (2023). An appraisal of the implications of deep fakes: The need for urgent international legislations. American Journal of Leadership and Governance, 8(1), 43-70. DOI: 10.47672/ajlg.1540.

49. Chesney, R., & Citron, D. K. (2018). Disinformation on steroids: The threat of deep fakes. Council on Foreign Relations. http://www.jstor.org/stable/resrep29943

50. Ibid

51. Zaidan, E., & Ibrahim, I.A. (2024). AI governance in a complex and rapidly changing regulatory landscape: A global perspective. Humanities and Social Sciences Communications, 11, Article 1121. https://doi.org/10.1057/s41599-024-03560-x

52. Scott, B., Heumann, S., & Lorenz, P. (2018). Artificial intelligence and foreign policy. Stiftung Neue Verantwortung. https://ssrn.com/abstract=3103961

53. Fitzgerald, K. (2025). AI investment a ‹game changer› for UAE and Gulf, Jihad Azour says. The National. https://www.thenationalnews.com/business/economy/2025/12/08/ai-investment-game-changing-for-uae-and-gulf-says-imf-regional-director/

54. United Arab Emirates Minister of State for Artificial Intelligence, Digital Economy & Remote Work Applications Office. (n.d.). UAE national strategy for artificial intelligence 2031. https://ai.gov.ae/strategy/#objective8

55. Federal Decree-Law No. (34) of 2021. https://uaelegislation.gov.ae/en/legislations/1526/download

56. Scott, B., Heumann, S., & Lorenz, P. (2018). Artificial intelligence and foreign policy. Stiftung Neue Verantwortung. https://ssrn.com/abstract=3103961

57. Ayaegbumam, I., & Fidelis, N. (2024). The intersection of artificial intelligence, deepfake, and the politics of international diplomacy. Ianna Journal of Interdisciplinary Studies, 6(2), 53 – 71. https://doi.org/10.5281/zenodo.11393419

58. Ibid