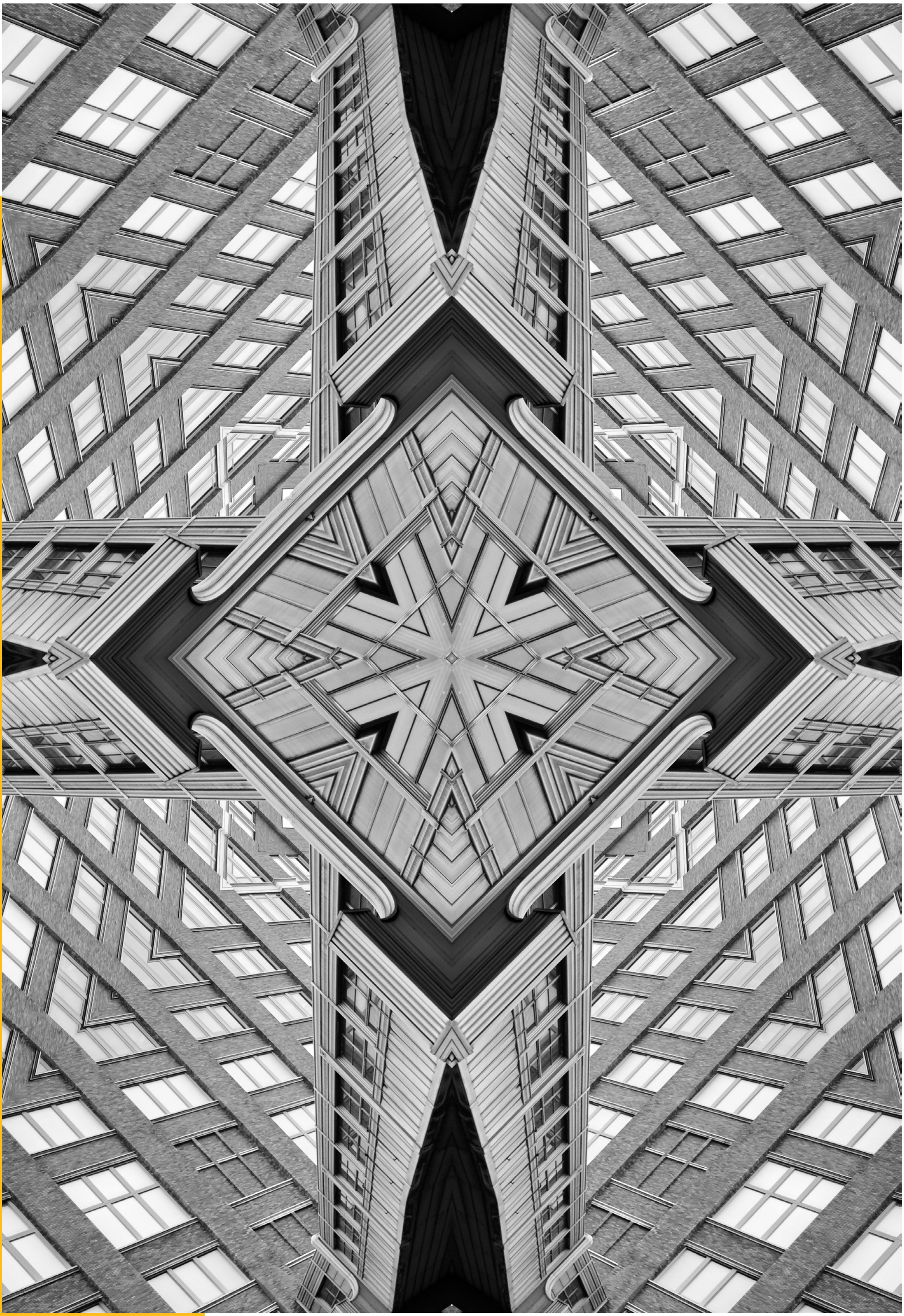
OBSERVER
RESEARCH
FOUNDATION

Occasional Paper



ISSUE NO. 454 NOVEMBER 2024

Elections, Accountability, and Democracy in the Time of A.I.

Rahul Batra

Abstract

This paper assesses how a transformational technology like Artificial Intelligence (AI) can be used by malicious actors to manipulate information and influence election results. It analyses the impact of such activities, and explores ways by which democratic polities can address this challenge. Reviewing cases from India and other countries in South Asia, and the United States, the paper also looks at the required regulatory landscape. It outlines recommendations straddling the strategic, tactical, and technical domains; and underlines the importance of public literacy.

Attribution: Rahul Batra, "Elections, Accountability, and Democracy in the Time of A.I.," *ORF Occasional Paper No. 454*, November 2024, Observer Research Foundation.

Introduction

At the time of writing this paper, more than 80 countries[1]—including seven of the 10 most populated[2]—have either voted or are set to go to the polls. There are three billion registered voters[3] across South Asia, Taiwan, Mexico, the European Union (EU), South Africa, the United Kingdom (UK), and the United States (US). These elections have occurred or are scheduled amid geopolitical conflicts that are causing strained supply chains, inflation, increasing inequality, and societal polarisation.

In this age of rapid technological advancements, where Artificial Intelligence (AI) tools can result in an information overload,[4] a critical question is whether voters are equipped to make a clear, conscious, and informed choice of government.

Indeed, the smartphone revolution of the past decade has enabled instant and endless access to "first and fast" information across online platforms. Led by social media and messaging apps, these digital platforms have overtaken traditional avenues for news and content dissemination such as the television.[5]

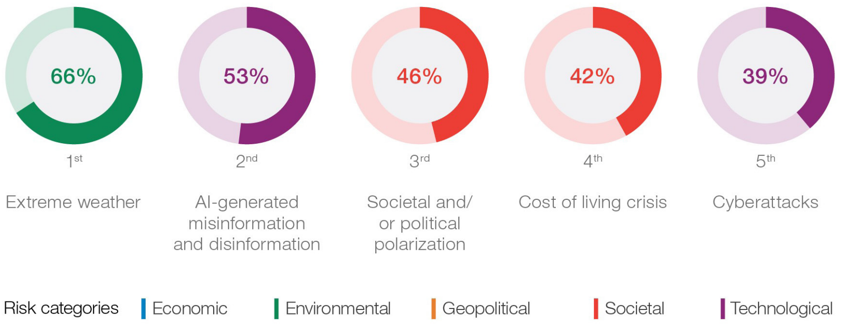
The World Economic Forum's 2024 Global Risks Report[6] placed 'AI-generated misinformation and disinformation' second in a list of the risks most likely to present a material crisis on a global scale in 2024 (see Figure 1). Additionally, 'misinformation and disinformation' was listed as the most severe global risk in the next two years (2024-26).

Both foreign and domestic actors, particularly political adversaries, could exploit people's vulnerability to misinformation to further their agendas. An April 2024 report from the Microsoft Threat Analysis Center (MTAC)[7] emphasised the increased likelihood of election-focused Chinese influence operations through AI-generated or AI-enhanced content, especially targeting voters in democracies such as the US, India, Taiwan, Japan, and North Korea.

Introduction

Figure 1: Current Global Risk Landscape

"Please select up to five risks that you believe are most likely to present a material crisis on a global scale in 2024."



Source:World Economic Forum Global Risks Perception Survey 2023-2024[8]

In October, the Office of the Director of National Intelligence of the US, the Cybersecurity and Infrastructure Security Agency (CISA), and the FBI reported[9] that AI-generated foreign interference and influence operations are likely to target polling day and the post-poll phases of the recently held US elections. With the goal of sowing doubt about the integrity of the election and collecting data for future efforts, foreign actors like Russia,[10] China, and Iran may look to exploit the public perception throughout the multi-stage process. The ways by which they can do this include pushing disinformation or amplifying protests and physical threats over vulnerabilities like voter fraud, ballot stuffing, and partisan officials.

Technology and Democracy: Early Promise and Current Dangers

In July 2024, a "deepfake" parody video[11] created by using a voice-cloning tool[12] to mimic Vice President Kamala Harris went viral on the internet, with the VP claiming incompetence, being the "ultimate diversity hire", and getting nominated as the Democratic candidate for the American elections due to President Joe Biden's declining cognitive health. It garnered 120+ million views just from X owner Elon Musk sharing the video. How many of these millions of viewers would be aware that the video was a deepfake, and how did it influence their opinions about the candidate during the early November election?[a]

Narratives to Liberate and Control

Foreign interference in democratic elections is not new. For example, as part of the Monroe Doctrine,[b] the US government under the Nixon administration helped a military junta in Chile overthrow the democratically elected government in power in 1973.[13] In recent years, social media and other technological innovations such as Big Data and Artificial Intelligence (AI)[14] have exacerbated the issue of election propaganda.[15] Russia's interference in the 2016 US presidential elections[16] is perhaps the most notable example of this.

Tools such as AI were initially projected to add trillions of dollars to the global economy through increased productivity and efficiency.[17] However, the roots of most technologies such as the internet and AI lie in military-led research projects,[18] which aimed to gain an upper hand in warfare against adversarial nations by using information and communication to exercise control. This strategic nature of AI emphasises its geopolitical significance.[19]

Even institutions such as think tanks, banks, and multilateral organisations like the United Nations (UN) are faced with a public crisis around manipulated content, from text to audio and video. Analysts have also raised concerns[20] about mass voice-cloned messages, or robocalls, via WhatsApp. Vulnerable to rapid 'reflexive sharing', such campaigns can drive widespread attention towards AI-generated, misleading content, rather than encouraging critical engagement with it.

[a] Kamala Harris, the Democratic Party nominee, lost the 2024 US General Election by a landslide verdict to Donald Trump, the Republican Party nominee.

[b] Since its inception in 1823 by the then US President James Monroe, the Monroe Doctrine has been a longstanding tenet of US foreign policy, meant to articulate the expansion of American influence in the Western Hemisphere and assert against European imperialism. See: https://history.state.gov/milestones/1801-1829/monroe

Technology and Democracy: Early Promise and Current Dangers

Early Uses of Digital Tools

When digital platforms such as WhatsApp, Facebook, X, and YouTube first grew in reach, they helped mobilise citizens across the world's democracies by enabling them to access campaigns and communications, contribute to fundraising, and give feedback. The generation of large amounts of user data allowed benign political actors to gain an understanding of user behaviour and interests for more personalised and targeted outreach. AI techniques such as Machine Learning (ML) and neural networks enabled a further, unprecedented level of prediction and insight for increased audience engagement.

In more recent years, the advances in AI technologies for language understanding and generation, such as OpenAI's Large Language Models ChatGPT and GPT-4, have resulted in a palpable shift. To be sure, there are many benefits to scaling up the applications of AI, albeit carefully, towards strengthening a democracy. In July 2024, US Rep. Jennifer Wexton, who has lost her voice to a neurological disorder, "regained" that voice from an AI-powered voice-cloning program.[21] Also in the US, candidates managed to deliver more efficient and less-costly campaigns in the run-up to the November polls using AI tools.[22]

Yet, at the same time, as these technologies transition from their use in niche academic pursuits to serve commercial interests, experts have begun to sound alarm bells.[23] Their main concern is machine-profile systems beginning to perform exceedingly well, with almost human-like accuracy and efficiency, in everyday tasks—becoming a growing socio-economic threat to our ability to make decisions and create agency.

Threats to democratic representation, accountability, and trust in the AI era have been well analysed.[24] A May 2024 study[25] suggests that while the immediate implications of persuasive AI-generated propaganda in textual content are yet to become evident, final voter decision is largely premeditated. Thus, there is an increasing risk that marginal groups who are exposed to such manipulation would be able to tilt a verdict. The study also raises concerns about AI-generated audio and visual content being much more persuasive, realistic, and likely to go viral.[26]

AI in the Electoral Process: Observations from South Asia

With more than a billion voters in South Asia having gone to the polls in the first half of 2024 alone, regional trends appear to confirm analysts' warnings.

Bangladesh

The infrastructure of disinformation in Bangladesh[27] has been used to target the political opposition and critics with the goal of institutionally neutralising the space for public debate and dissent. Before the January 2024 general elections in the country, a number of fake videos, allegedly circulated by networks of pro-government content creators, targeted the opposition Bangladesh National Party (BNP)[28] on social media. Consequently, the BNP boycotted the elections, citing the lack of a "free and fair" process under the ruling Awami League government. Simultaneously, deepfakes emerged of two independent candidates[29] claiming that they had withdrawn from the process, even when they had not.

The US government's attempts to pressure the Sheikh Hasina government to conduct a clean election led to Americans also becoming the subject of misinformation campaigns run by the Bangladeshi government and its affiliates, with pro-government agencies, journalists, and tech enthusiasts generating income at an industrial scale through organised disinformation campaigns built on trolling and ad placements on malicious content websites.[30]

Pakistan

In February 2024, while imprisoned, Pakistan's former Prime Minister Imran Khan claimed victory in the general elections through an AI-generated pre-recorded audio-visual speech.[31] This use of a synthetically crafted message by a national figure to congratulate his supporters on their collective win, despite a "crackdown" on his party, the Pakistan Tehreek-e-Insaf (PTI), was notable. Between December 2023 and July 2024, Imran Khan's AI-generated voice was used in six instances, with each one accompanied by a message clarifying that this was not Imran Khan's real voice. On the one hand, this shows a progressive application of ubiquitous modern-day technology in politics; on the other, it signifies the extent to which misinformation can be planted.

The Pakistani elections serve as a global case study[32] on the importance of context in the success or failure of the use of AI in political messaging. The odds being stacked against Imran Khan and the PTI's participation in the elections allowed for the voice-cloned messages to gain attention and trust. A carefully planned and executed application of the technology also ensured that any effort to plant disinformation or spread misinformation through counter-messaging by the current government and its supporters barely registered.

Sri Lanka

In Sri Lanka, where the presidential elections were held in September, a "shallowfake"[c] video was circulated of Trump purportedly expressing support for Anura Kumara Dissanayake,[33] leader of the National People's Power (NPP) alliance. The video caused a backlash among the party's detractors, who presented the NPP as a platform spreading misinformation to manipulate public opinion for its gain.

In a tumultuous information environment characterised by poor media literacy and high consumption of political content, the issue of synthetically generated misinformation and disinformation at an industrial scale is a grave concern that threatens the legitimacy of Sri Lanka's democratic process.

India

India's elections[34] were spread over seven phases between 19 April and 1 June 2024, with 969 million registered voters, 2,660 registered political parties, and one million polling booths. In this context, AI was a double-edged sword.[35]

[c] In "shallowfake" or "cheapfake" videos, content is manually doctored using easily accessible editing tools, instead of using sophisticated algorithmic technology, as in the case of deepfakes. Though cheapfakes alter the strictly technical nature of AI-induced misinformation and require a simpler setup, they expand the scope and reach of larger issues such as information veracity and public trust. See: https://ggr.hias.hit-u.ac.jp/en/2024/02/26/how-disinformation-erodes-the-worlds-largest-democracy/.

AI enabled stakeholders to conduct cost-efficient large-scale surveys for policy feedback, conduct sentiment analysis on digital media, and use facial and speech recognition for personalisation in political campaigns. It also aided in faster and more efficient vote-counting, alongside enabling the use of video analytics to prevent tampering and fraud.[36] However, concerns around content manipulation and moderation persist.[37]

In the short term, public and private actors may find it challenging to identify and keep up with the exponential advances in sophisticated technologies such as 'deep learning'.[d] As a critical-stage remedy, the Misinformation Combat Alliance (MCA)'s Deepfakes Analysis Unit (DAU), in partnership with Meta, set up a WhatsApp helpline[38] in March 2024 to detect and respond to public queries to differentiate between real and fabricated content across both audio and video formats.

Additionally, there were efforts to reach out to both the Election Commission of India (ECI) and platform companies such as X, Meta, Alphabet, Snap, OpenAI, seeking urgent intervention to protect the sanctity of the general elections. The ECI was called upon[39] to invoke the plenary powers accorded to it by Article 324 of the Constitution of India.[e] Meanwhile, the platform companies operating in India were called upon[40] to address ethical concerns and legal risks to maintain their "safe harbour protection" under Section 79 of India's Information Technology Act, 2000.[f]

[d] "Deep learning" is an advanced form of machine learning, an Artificial Intelligence technique, which relies upon human-brain-like neural networks. Built upon basic mathematical principles like 'cause and effect' logical reasoning, sequential recognition of shapes and patterns (in text, images, or videos,) and making connections to identify and classify given objects—these techniques process data and signals for iterative self-improvement to make predictions and recommendations. See: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-deep-learning

[e] Article 324 of the Constitution of India endows the ECI with absolute power to direct, control, and supervise all electoral processes, ensuring their conduct in a free and fair manner. This includes complete authority to make necessary interventions to address any threats that can undermine the fairness of elections.

[f] Section 79 of India's IT Act, provisions digital platforms operating in India with a "safe harbour"— an exemption from liability for third-party content on their service—provided they adhere to other content moderation requirements of Indian Law covering harmful or illegal instances. See: https://www.barandbench.com/columns/safe-harbour-exemptions-available-to-intermediaries-exception-or-norm-under-digital-india-act

As anticipated, “India’s most important elections”[41] were a hotly contested war of perception[42] that involved AI, social media, memes, fake news, parodies, trolling, and the exchange of allegations.[43] In May 2024, for example, fake videos of Union Home Minister Amit Shah and Uttar Pradesh Chief Minister Yogi Adityanath emerged[44] that showed them making claims about issues[g] that were sensitive to millions of voters and could swing support in crucial constituencies in the final stages of the marathon polls. Notably, these were shallowfake rather than deepfake videos.

Further, across both Bangladesh and India, women candidates were among the first targets of such technology being used to obfuscate the truth. Political advertisements using AI-generated deepfake images and videos for sexual harassment or character assassination can undermine the credibility of women candidates[45] and likely prevent them from entering the political fray altogether.[46]

The three-month Indian election cycle had few instances of deepfake content. According to Professor Mayank Vatsa, whose department at the Indian Institute of Technology Jodhpur has built a deepfake-detection tool called *Itisaar*, massive investments and a substantial workforce are required to train AI models in non-English languages—this gap has an impact on the overall generation of “sophisticated deepfakes”.[47]

Thus far, there has also been no evidence of direct, identifiable AI-generated foreign interference in the Indian electoral process.[48] However, just before the last phase of polling began on 1 June 2024, OpenAI reportedly disrupted anti-BJP activity[49] carried out by Israeli political campaign management firm STOIC. OpenAI confirmed[50] that their generative adversarial network models were being used to generate pro-Indian National Congress English-language articles and comments across social media.

[g] One cited that the ruling Bharatiya Janata Party (BJP) would stop certain social guarantees for minorities; another criticised PM Narendra Modi for not doing enough for families of those who died in a 2019 terrorist attack.

The Imperatives of Resilience, Governance, and Awareness

Breakthroughs in the field of AI, especially Generative AI,[51] are creating a notable impact on content generation. This calls for radical changes in the approach to misinformation through the innovation-regulation balance. As the Arizona Secretary of State's Office has flagged,[52] everything from political robocalls to fake videos of politicians have now become normal. Additionally, with the advances in Generative AI, results that would previously take hours or even weeks are now being achieved within minutes.[53] The most commonly discussed solutions to address the rise in deepfakes are technical or legal.[54] However, it is important to highlight that it is ultimately human intent, and not technicalities, that define the malicious use of any technology, be it AI, cars, or smartphones; AI has not created new forms of crime, only amplified existing ones.

Technical Innovation: Addressing the Problem Before and After Identification

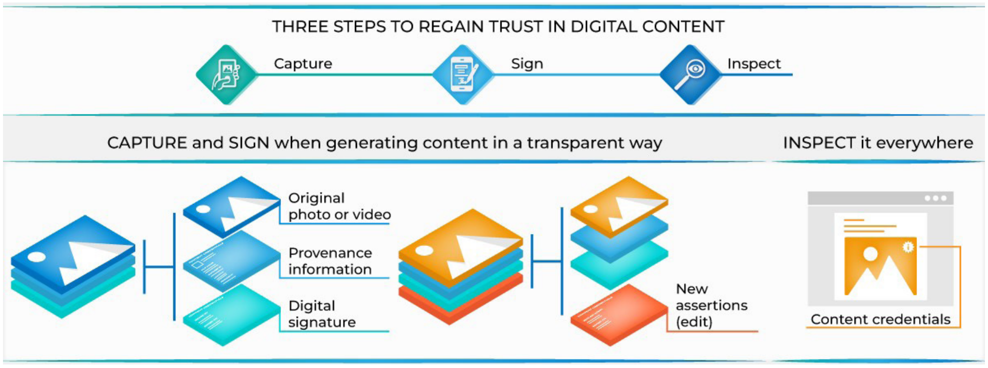
Possible fixes generally involve either debunking (detection tech) or pre-emption (labeling tech).

For debunking, a number of tools and techniques have become available over time that leverage forensic technology to identify misinformation. These include the ability to identify unnatural blinking patterns, distortion in bodily features, inconsistencies across images within a video (especially concerning lighting), incongruities between the speech and mouth movements of the subject, and the absence of biometric patterns specific to world leaders.[55] However, keeping up with the advances in AI, which allow perpetrators to continuously train their systems to close known authenticity gaps and thus bypass detection techniques, remains a massive challenge. In some cases, the Research and Development (R&D) that goes into the detection technology itself contributes to the improvement in deepfake proliferation methods.[56]

For pre-emption, the sector adopts the 'content provenance' approach, which "watermarks" audio, video, and image content digitally using metadata or embedded signals that record details about the content, such as who created it, when, and using what methods (e.g., AI), thus allowing users, platforms, and media organisations to check for authenticity. This approach was first popularised in February 2024 at the Munich Security Conference, where a Microsoft-led consortium of 20 technology companies formed a tech accord to address the threats posed by AI deepfakes in elections.[57]

There is visible momentum around developing and inculcating technical standards such as the Coalition for Content Provenance and Authenticity (C2PA),[h] which certifies the source and history (i.e., the provenance) of media content.[58] The C2PA (technical) standard offers added security and transparency by binding provenance information to a piece of media throughout its journey. From the initial moment when it is created, to every edit that is made, its actions and history can be captured and recorded to create a tamper-evident record that can be inspected and validated by a consumer or a downstream technical process (see Figure 2).

Figure 2: The Core Concept of the C2PA Specification



Source: Antonio Grasso[59]

However, increased tech-sector accountability is not a substitute for the rule of law. Rather than curtailing the scope of innovation-powering

[h] The Coalition for Content Provenance and Authenticity (C2PA) addresses the problem of online misinformation—and focuses on the future of responsible digital media creation, publication and sharing—through the development of technical standards. See: https://c2pa.org/about/

algorithms, what is required is the development of public policies that focus on unraveling disingenuous intent and growing citizen awareness to develop resilience against the persistent threat of disinformation.[60]

The Munich Tech Accord has further emphasised the critical need for new legal frameworks to be developed and implemented around this complex and evolving problem, states the need for "collective inter-governmental leadership" to address the issues.

Regulation: Towards Transparency, Accountability, and Enforcement

Global regulation of an expansive technology paradigm such as AI needs to occur at two levels: international governance frameworks and national policymaking. The geopolitical currents at play make it difficult to achieve consensus on specific goals for any regulation with a clear purpose. At the outset, therefore, a "realist's perspective"[61] suggests the need for: (a) rule diversity in oversight; and (b) regulatory mechanism experimentation that allows for systems to learn and share from each other.

The narrative around AI has steadily shifted over the last decade from its potential to drive unprecedented socio-economic progress to its increasing unpredictability. As possibilities of this technology causing both benefit and harm to humanity emerge, a blurring across its use, intent, and capability has occurred.[62] Given this dualistic nature of AI, national policymakers, especially in the democratic-information sphere, must strike a fine balance between: a risk-based vs. rights-based approach; content censorship and freedom of expression; platform accountability and stifling market innovation/competition.

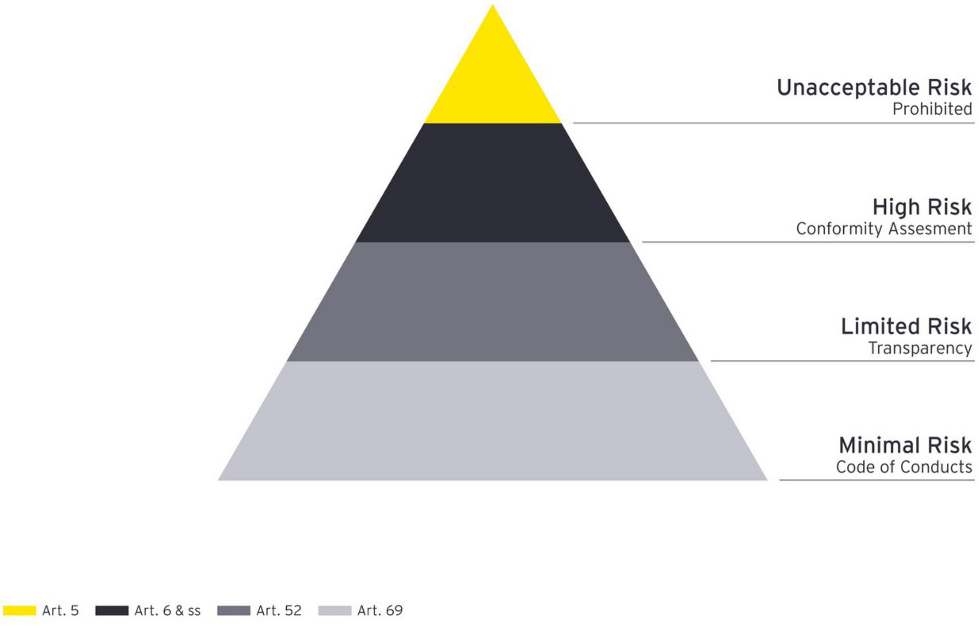
The traditional legal approach to such sectorial regulation of technology entails following a binary logic: a process is either legal or illegal. This is commonly known as the "rights-based approach".[i] A different logic, known

[i] A rights-based approach to legislation prioritises the fundamental (human) rights of the people subjected to such law, over potential risks of impingement owing to any external actors or action in the environment.

as the "risk-based approach", subjects such processes to a layered framework built upon the "proportionality" principle.[j]

On 21 May 2024, the world's first comprehensive AI regulation, the European Union Artificial Intelligence Act (EU AI Act), was adopted by the European Parliament.[63] As its operating principles, "It aims to create an environment where AI technologies respect human dignity, rights, and trust. It also fosters collaboration, innovation, and research in AI among various stakeholders. Moreover, it engages in international dialogue and cooperation on AI issues, acknowledging the need for global alignment on AI governance." The EU AI Act adopted an evolutionary "risk-based approach" (see Figure 3), despite strong arguments in favour of a more definitive "rights-based" one,[64] thus defining a path that avoids stifling innovation in the paradigm-shifting field of AI.

Figure 3: Risk Categories of the EU AI Act



Source: Ernst & Young[65]

[j] A risk-based approach, utilising the principle of proportionality, strives to achieve a balance between the objective of an act, means and methods used to achieve that objective, and the consequences of the act. It follows the maxim that the punishment of an offender should fit the crime.

However, nations and civil society need to remember that fundamental rights are non-negotiable and that they must be respected regardless of the operational risks associated with external factors (e.g., technical environments in which companies function). According to the Institute of Strategic Dialogue, "The (EU) AI Act's requirements will introduce broad democratic protections against AI-driven harms, as well as specific measures to counter the spread of disinformation and misleading content through generative AI and deepfakes."[66]

The prohibitions under Article 5 of the EU AI Act[k] are important safeguards against the introduction and/or exacerbation of societal divisions, marginalisation, or undemocratic concentrations of power through AI. For example, systems using "subliminal techniques to [...] distort behaviour and impair informed decision-making, leading to significant harm" are banned; such a ban is unequivocally beneficial to democratic functioning and the protection of fundamental rights.[l] In addition, all systems involved in the administration of justice and democratic processes, including systems used for influencing electoral outcomes or voting behaviour, will fall under the high-risk category and be subject to its stringent accompanying requirements.

As per the Act, all AI systems that pose a clear threat to the safety, livelihoods, and rights of people will be banned. From social scoring by governments to real-time biometric surveillance in public spaces to toys using voice assistance—they could induce dangerous behaviour. As a punitive measure, the Act also mentions that fines for violations will range from 7.5 million euros (US$8.2 million) or 1.5 percent of a company's turnover to 35 million euros or 7 percent of global turnover, depending on the type of violations. The Act will come into full effect in 2026, with a few exceptions.[67]

While the Act is considered comprehensive in principled intent across its territorial scope, there remain questions around its applicability in multi-stakeholder settings.[68] Beyond normative prescriptions towards compliance, based on its risk-based framework, the legislation needs to address gaps around the responsibilities and liabilities of actors participating within its jurisdiction. The US has taken a light-touch voluntary compliance ("self-regulation") approach,[69] led by the core principle that companies should

[k] See: https://artificialintelligenceact.eu/article/5/

[l] See: https://commission.europa.eu/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en

control industrial development and related governance criteria generally. China, meanwhile, aims to prioritise commercial development[70] alongside maintaining social stability and state control.[71] For their part, the ASEAN has endorsed a business-friendly 'Guide for AI Ethics and Governance'[72] following predictions that AI could add 10-18 percent uplift (of nearly US$1.0 trillion) to their GDP by 2030.

India has made an initial thrust[73] (including an approximately US$1.2 billion state-led investment in March 2024, to be spread over five years) in the field of AI, favouring technical compliance and rapid innovation. Over the past two years, however, it has tried to strike a balance between punitive law enforcement to tackle emerging threats and adopting a more holistic approach to AI regulation.[74]

Besides these prominent national and regional bloc-level programmes, aimed at advancing each actor's own capability and relevance, a global conversation has emerged around "responsible AI".[75] Multi-stakeholder coalitions like the Global Partnership on Artificial Intelligence (GPAI), the UK's AI Alliance, and India's Core-AI are working towards the convergence of governments, big corporations, startups, academia, and civil society organisations to avoid silos on the path to collaborative, consistent, comprehensive, and ethical AI governance.

India's Policy Prerogatives

With a national AI regulatory framework still in the works,[76] Indian policymakers need to work towards striking a balance between driving innovation and regulation in AI. An example could be drawn from the State of California's Governor Gavin Newsom who, in September 2024, blocked a landmark bill aimed at establishing first-in-nation safety measures for large AI models, citing that the proposed bill "can have a chilling effect on the industry."[77] Yet, just days earlier, he had signed unto State Law three stringent bills[78] applicable to AI-generated deepfakes that could deceive voters despite US Federal Laws protecting social media companies and their users against government regulation overreach.

The Imperatives of Resilience, Governance, and Awareness

For its part, the Indian government has relied upon existing legislation,[79] such as under the Information Technology Act, 2000 (IT Act), Indian Penal Code, 1860 (IPC), and Copyright Act, 1957, to offer civil and criminal remedies against AI-generated harms and deepfakes. However, besides utilising a porous Voluntary Code of Ethics since 2019[80] to counter the impact of the internet and social media on electoral integrity, it needs to avoid the kind of reactionary measures that it has resorted to over the past year.

In November 2023, the government issued an advisory to social media platforms in India to take down deepfake content within 24 hours of it being reported.[81] In March 2024, the Ministry of Electronics and Information Technology (MeitY) issued two AI advisories to platforms and intermediaries in India, seeking increased due diligence towards more responsible and ethical use of this technology.[82] The latter set of advisories was particularly contentious because of their initial intent but even more so for the manner in which they were rolled out.[83] The first of the two was issued on 1 March 2024 as a government reaction to a post on X claiming that Google's AI technology was offering a biased response when asked if Prime Minister Narendra Modi was a "fascist".[84]

Keen to avoid any electoral blowback on the eve of the general elections, the government made some ill-conceived and sweeping demands on the digital technology ecosystem in India,[85] at the risk of stifling innovation and adding bureaucratic clutter. Immediate and strong industry pushback led the government to first issue an ad-hoc clarification a few days later, before issuing a formal revision two weeks later.[86] The reactive, non-binding nature of such advisories creates mistrust within the public-private sphere, suggesting that the democratic-information ecosystem in India still has a long way to go in overcoming the very real and rising risk of digital disruption from domestic and foreign actors, especially via mass-reach international platforms.

Experts across forums in New Delhi suggest that Indian policymaking will be well served to tackle these issues through globally validated (democratic governance) principles such as understanding operational and societal risks; transparency; accountability; and the rights of its citizens.[87]

The Imperatives of Resilience, Governance, and Awareness

A consultation meeting with these experts, held in October to discuss the scope of setting up an AI Safety Institute (AISI) in India, is a welcome step by the government.[88]

In its macroscopic effort towards establishing a national AI regulatory regime, India must pay heed to certain strategic, tactical, and technological goals:[89]

a. Strategic:

- Steer away from the "developing nation" trap, which would result in it simply becoming a provider of critical resources for AI innovation to global leaders like the US and China, or being constrained in its capacity to innovate and participate in the global AI economy by being subjected to AI regulations by leaders like the EU.[90]

- Evolve from a risk-based approach built to optimise scarce regulatory resources and administrative ability to prioritise certain harms towards seeking to enforce consciously chosen rules as per the "responsive regulation" approach.

b. Tactical:

- Keep implementation flexible in response to different technological, sectoral, and socio-economic conditions to avoid stifling innovation. This will require risk evaluations and assessments to balance trade-offs and set thresholds through understanding that risk tolerance varies by regulators across sectors.

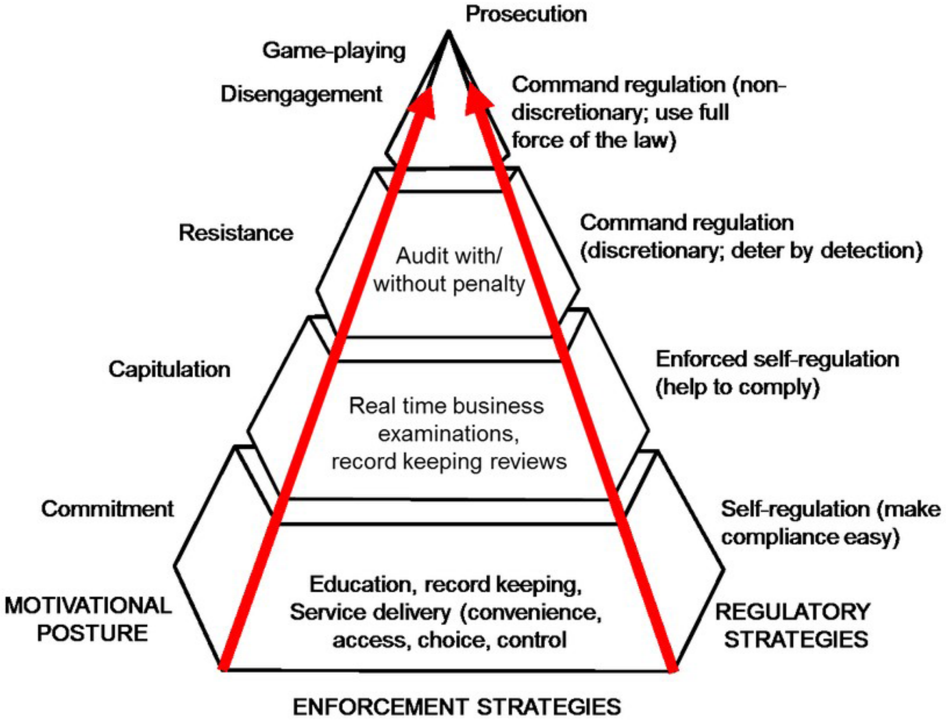
- Define a responsibility and liability framework for actors within the scope of this regulation, based on their role in the ecosystem as a consumer, supplier, or intermediary.

c. Technical:

- Gain an understanding of the complexities of an exponential technology such as AI across nuances like data ownership, proprietary algorithms, computing infrastructure, cultural and contextual biases, and IP regimes in the context of both competition and collaboration.

- Develop iterative, harmonised standards comprising procedural guidance, compliance frameworks, safety evaluation benchmarks, and audit mechanisms, remaining a catalyst for innovation but a deterrent to risk.

Figure 4: The Responsive Regulation Approach


Prosecution
Game-playing
Disengagement
Command regulation (non-discretionary; use full force of the law)
Resistance
Audit with/ without penalty
Command regulation (discretionary; deter by detection)
Capitulation
Enforced self-regulation (help to comply)
Real time business examinations, record keeping reviews
Commitment
Self-regulation (make compliance easy)
MOTIVATIONAL POSTURE
Education, record keeping, Service delivery (convenience, access, choice, control
REGULATORY STRATEGIES
ENFORCEMENT STRATEGIES

Source: European Platform Tackling Undeclared Work[91]

Public Awareness and Literacy

In what is referred to as the "Liar's Dividend",[92] spreaders of misinformation are able to avoid accountability as a result of the increasing scepticism over information online. A recent example of this phenomenon came in the form of US President-elect Trump and far-right social media influencers claiming[93] that the size of the crowd that attended Kamala Harris's early-August Detroit rally was "faked" through the use of AI-manipulated images. In a viral online exchange between the two sides, the Republicans continued to allege a foul projection of popularity on the part of the Democrats, though without any evidence to back their claims.[94] The Democrats presented videos as a counterclaim, with many media reports offering supportive satellite imagery as confirmation.[95]

Simple user-friendly communication—such as the Microsoft primer[96] on "deepfakes" which offers a checklist on fighting deepfakes, a quick test on AI-detection skills, and advice for campaigners and voters—can go a long way in easing citizen anxiety. Additionally, getting popular public personalities to partner with non-partisan media[97] platforms and "gamifying" the problem of tackling deepfakes in the virtual world has helped bring further attention to the issue.

A post-election review in India[98] highlights the need to establish a balance between AI alarmism and idealism through public literacy; understand the nature of a consumer and a generator of online misinformation, and the increasingly blurred line between malign-benign content; overcome the silos between journalists, fact-checkers, and technology solutions; and not underestimate the efficacy of human-led solutions to existing problems.

That universities in India are now offering formal courses to study digital disinformation is a sign that society is slowly but surely catching up.

Conclusion

Technology may not yet be a substitute for conventional forms of campaigning on the ground, door-to-door campaigning and mobilising voters locally. However, evolving paradigms such as AI have the ability to disrupt public discourse and socio-political processes, even challenging the notion of a nation state.[99] Mitigating these threats will require collaboration across a wide variety of stakeholders, such as governments, Big Tech companies, new-age deep-tech startups, media, and civil society organisations, as well as citizens.

In the lead-up to the US elections, a silver lining developed among the dark clouds over the role of AI in the future of the democratic process. Despite all the AI-generated memes and misinformation against Kamala Harris, for instance, she still became the first woman of colour to win the Democratic Party nomination in US history, thus rejuvenating a wide base of supporters in quick time. She was also named "AI Policy Czar",[100] though she will no longer be able to champion this cause as president.

In contrast, President-elect Trump brings an alternate approach and set of priorities to his national and international agenda. His close collaboration with Elon Musk throughout the campaign trail, and his Vice-President pick J.D. Vance having strong ties to Silicon Valley, suggest that technological innovation will remain a central theme in his plans for America's socioeconomic and geopolitical revival.[101]

It remains to be seen whether the Trump administration would implement stronger guardrails on this technology domestically—particularly on matters like safety, bias, and workforce displacement—or if the administration will create an efficiency-and-competition-based policy framework on AI. Either way, the wider democratic world can expect a shift away from the shared-values-based collaboration ensuing under the Biden administration, to an "America first" interest-based transactional future under Trump[102] – for both the global order and AI's role in it.ORF

Rahul Batra *is a geopolitical analyst with extensive experience at the intersection of digital platforms and international affairs.*

Endnotes

[1] Helen Livingstone and Guardian Correspondents, “Elections Tracker 2024: Every Vote and Why it Matters,” *The Guardian*, July 8, 2024, https://www.theguardian.com/world/2024/feb/23/2024-global-elections-tracker-voting-dates-us-india-indonesia-belarus-haiti-pakistan-full-list

[2] Siladitya Ray, “2024 is the Biggest Election Year in History—Here are the Countries Going to the Polls this Year,” *Forbes*, January 3, 2024, https://www.forbes.com/sites/siladityaray/2024/01/03/2024-is-the-biggest-election-year-in-history-here-are-the-countries-going-to-the-polls-this-year/?sh=37d23a6c65f9

[3] Koh Ewe, “The Ultimate Election Year: All the Elections Around the World in 2024,” *Time,* December 28, 2023, https://time.com/6550920/world-elections-2024/

[4] Anulekha Nandi, “The Age of AI and Access to Information Paradox,” Observer Research Foundation, September 2024, https://www.orfonline.org/expert-speak/the-age-of-ai-and-access-to-information-paradox

[5] Anirban Sharma, “Accessing News and Information Online: A Pandora’s Box?,” Observer Research Foundation, September 27, 2024, https://www.orfonline.org/expert-speak/accessing-news-and-information-online-a-pandora-s-box

[6] World Economic Forum, *The Global Risks Report 2024, 19th Edition, Insight Report*, January 2024, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

[7] Clint Watts, “China Tests US Voter Fault Lines and Ramps AI Content to Boost Its Geopolitical Interests,” Microsoft, April 4, 2024, https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/

[8] Saadia Zahidi, “How to Navigate an Era of Disruption, Disinformation, and Division,” World Economic Forum, January 13, 2024, https://www.weforum.org/stories/2024/01/how-to-navigate-an-era-of-disruption-disinformation-and-division/

[9] Lily Hay Newman and Tess Owen, “Russia is Going All Out on Election Day Interference,” *Wired*, November 5, 2024, https://www.wired.com/story/russia-election-disinformation-2024-election-day/

[10] “Deepfake Detection Report: Arizona Election Fraud,” LinkedIn Pulse, November 6, 2024, https://www.linkedin.com/pulse/deepfake-detection-report-arizona-election-fraud-deepmedia-ai-wbdmc/

[11] Mr Reagan (@MrReaganUSA), “Kamala Harris Campaign Ad PARODY,” July 26, 2024, https://x.com/MrReaganUSA/status/1816826660089733492

Endnotes

12 Kat Tenbarge, “Elon Musk Made a Kamala Harris Deepfake Ad Go Viral, Sparking a Debate About Parody and Free Speech,” *NBC News*, August 1, 2024, https://www.nbcnews.com/tech/misinformation/kamala-harris-deepfake-shared-musk-sparks-free-speech-debate-rcna164119

13 John Kirk and Stephen Kimber, “Fifty Years After Chile’s Coup, the Region Still Not Safe from US Meddling,” *Al Jazeera*, 11 September 2023. https://www.aljazeera.com/opinions/2023/9/11/fifty-years-after-chiles-coup-the-region-still-not-safe-from-us-meddling

14 Sarah Kreps, *The Role of Technology in Online Misinformation*, Brookings, June 2020, https://www.brookings.edu/wp-content/uploads/2020/06/The-role-of-technology-in-online-misinformation.pdf

15 Jonathan Haidt, “Why the Past 10 Years of American Life Have Been Uniquely Stupid,” *The Atlantic*, April 11, 2022. https://www.theatlantic.com/magazine/archive/2022/05/social-media-democracy-trust-babel/629369/

16 G. Eady et al., “Exposure to the Russian Internet Research Agency Foreign Influence Campaign on Twitter in the 2016 US Election and Its Relationship to Attitudes and Voting Behavior,” *Nat Commun* 14, no. 62 (2023), https://doi.org/10.1038/s41467-022-35576-9

17 Michael Chui et al., “The Economic Potential of Generative AI: The Next Productivity Frontier,” Mckinsey Digital, June 14, 2023, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#introduction

18 Online Library Learning Center, “A Brief History of the Internet,” https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml

19 Bernard Marr, “The Geopolitics of AI,” *Forbes*, September 18, 2024, https://www.forbes.com/sites/bernardmarr/2024/09/18/the-geopolitics-of-ai/

20 Sanjana H., “Generative AI, and Sri Lanka’s 2024 Presidential Election: Insights from India’s General Election,” June 10, 2024, https://sanjanah.wordpress.com/2024/06/10/generative-ai-and-sri-lankas-2024-presidential-election-insights-from-indias-general-election/

21 Dan Merica, “A Neurological Disorder Stole Her Voice. Jennifer Wexton Takes it Back on the House Floor,” *Associated Press*, July 25, 2024, https://apnews.com/article/jennifer-wexton-ai-voice-clone-progressive-suprenuclear-palsy-speech-6569e27b4095db2b58c36b61e833d0e0

Endnotes

22 John Hewitt Jones, "It's Not All Deepfakes: Responsible AI Can Strengthen Democracy," *Bloomberg Government*, October 29, 2024, https://news.bgov.com/bloomberg-government-news/its-not-all-deepfakes-responsible-ai-can-strengthen-democracy

23 Yoshua Bengio, "AI and Catastrophic Risk," *Journal of Democracy* 34, no. 4 (October 2023): 111–21.

24 Sarah Kreps and Doug Kriner, "How AI Threatens Democracy," *Journal of Democracy* 34, no. 4 (October 2023): 122–31.

25 Dylan Walsh, "The Disinformation Machine: How Susceptible Are We to AI Propaganda?," Human-Centered Artificial Intelligence (HAI), Stanford University, May 1, 2024, https://hai.stanford.edu/news/disinformation-machine-how-susceptible-are-we-ai-propaganda

26 Niharika Palep, "Unmasking Deepfakes: Understanding the What, Why, and How," The Tech Bridge, March 8, 2024. https://the-tech-bridge.org/2024/03/08/unmasking-deepfakes-understanding-the-what-why-and-how/

27 Mubashar Hasan, "Deep Fakes and Disinformation in Bangladesh," *The Diplomat*, December 29, 2023, https://thediplomat.com/2023/12/deep-fakes-and-disinformation-in-bangladesh/

28 "Fake Videos Targeting BNP Resurfacing on Social Media: Reports," *The Daily Star*, December 19, 2023, https://www.thedailystar.net/tech-startup/news/fake-videos-targeting-bnp-resurfacing-social-media-reports-3498361

29 Tohidul Islam Raso, "Fake News of Candidate Withdrawing from Election Circulated on Facebook Using Deepfake Video," dismislab, January 27, 2024, https://en.dismislab.com/deepfake-video-election-gaibandha-1/

30 Nikolina Klatt and Vanessa A. Boese-Schlosser, "Authoritarianism and Disinformation: The Dangerous Link," The Loop, European Consortium for Political Research, June 2023, https://theloop.ecpr.eu/disinformation-in-autocratic-governance/

31 Manjiri Chitre, "Pakistan Election 2024: Imran Khan Takes AI Help to Make Victory Claim," *The Hindustan Times*, February 10, 2024, https://www.hindustantimes.com/world-news/pakistan-election-2024-what-jailed-imran-khan-said-in-ai-generated-video-message-101707525198676.html

32 Thomas Gaulkin, "The Campaign Volunteer Who Used AI to Help Swing Pakistan's Elections: Interview with Jibran Ilyas," *Bulletin of the Atomic Scientists*, September 5, 2024, https://thebulletin.org/premium/2024-09/the-campaign-volunteer-who-used-ai-to-help-swing-pakistans-elections-interview-with-jibran-ilyas/

Endnotes

33 Sanjana H., "Manipulated Media, and Sri Lanka's 2024 Presidential Election," May 14, 2024, https://sanjanah.wordpress.com/2024/05/14/manipulated-media-and-sri-lankas-2024-presidential-election/

34 Bibhudatta Pradhan, "Just How Big is India's 2024 Election? Find Out in Seven Numbers," *Al Jazeera*, March 16, 2024, https://www.aljazeera.com/news/2024/3/16/india-announces-election-2024-seven-numbers-to-unpack-worlds-biggest-vote

35 Sharmila Bhadoria, "Lok Sabha Elections: How AI Will be a Double-Edged Sword to Boost Fake News, Curb Voting Manipulations in Upcoming Polls," *Livemint*, February 25, 2024, https://www.livemint.com/news/india/lok-sabha-elections-2024-how-ai-will-be-a-double-edged-sword-to-boost-fake-news-curb-voting-manipulations-11708705430974.html

36 Kamya Pandey, "Political Parties Discuss Misinformation in Politics at Council for Strategic and Defense Research's Conference," *Medianama*, March 28, 2024, https://www.medianama.com/2024/03/223-navigating-misinformation-in-politics-a-comprehensive-takeaway-csdrs-latest-conference/

37 Yashraj Sharma, "Deepfake Democracy: Behind the AI Trickery Shaping India's 2024 Election," *Al Jazeera*, February 20, 2024, https://www.aljazeera.com/news/2024/2/20/deepfake-democracy-behind-the-ai-trickery-shaping-indias-2024-elections

38 Meta, "MCA's WhatsApp Helpline: Curbing the Spread of AI-Generated Misinformation in India," February 19, 2024, https://about.fb.com/news/2024/02/mcas-whatsapp-helpline-curbing-the-spread-of-ai-generated-misinformation/

39 Software Freedom Law Center, India, "Joint Letter to ECI on Deepfakes and Manipulated Media," https://form.sflc.in/joint-letter-to-eci-on-deepfakes-and-manipulated-media/

40 Software Freedom Law Center, India, "Joint Letter to Platform Companies on Deepfakes and Manipulated Media," https://form.sflc.in/joint-letter-to-platform-companies-on-deepfakes-and-manipulated-media/

41 Sumit Ganguly, "Why this Election is India's Most Important," *Journal for Democracy*, April 2024, https://journalofdemocracy.org/elections/why-this-election-is-indias-most-important/

42 Nilesh Christopher, "'Inflection Point': AI Meme Wars Hit India Election, Test Social Platforms," *Al Jazeera*, March 8, 2024, https://www.aljazeera.com/economy/2024/3/8/ai-meme-wars-hit-india-election-campaign-testing-social-platforms

43 Software Freedom Law Center, India, "Tracking Use of AI by Political Parties in India," https://sflc.in/tracking-use-of-ai-by-political-parties-in-india/

Endnotes

[44] Munsif Vengattil, Saurabh Sharma, and Rishika Sadam, “India Election: Fake Videos of Aides to PM Narendra Modi Trigger Political Showdown,” *RNZ*, May 5, 2024, https://www.rnz.co.nz/news/world/516043/india-election-fake-videos-of-aides-to-pm-narendra-modi-trigger-political-showdown

[45] Catherine Powell and Alexandra Dent, “Artificial Intelligence Enters the Political Arena,” Council on Foreign Relations, May 24, 2023, https://www.cfr.org/blog/artificial-intelligence-enters-political-arena

[46] Shashi Tharoor, “AI And Politics; When Lines Get Blurred,” *Mathrubhumi*, May 16, 2024, https://english.mathrubhumi.com/columns/i-mean-what-i-say/shashi-tharoor-column-on-artificial-intelligence-1.9561156

[47] Karen Rebelo, “Deepfakes Underwhelm as Political Parties Rely on Cheap AI Voice Clones,” *BOOM Fact Check*, May 30, 2024, https://www.boomlive.in/decode/deepfakes-underwhelm-as-political-parties-rely-on-cheap-ai-voice-clones-25483

[48] Jaibal Naduvath, “Flex, Flux and the Foreigner: AI and Election Interference,” Observer Research Foundation, March 19, 2024, https://www.orfonline.org/expert-speak/flex-flux-and-the-foreigner-ai-and-election-interference

[49] OpenAI, *Disrupting Deceptive Uses of AI by Covert Influence Operations*, May 30, 2024, https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/

[50] “OpenAI Says Stalled Attempts by Israel-Based Company to Interfere in Indian Elections,” *The Hindu*, June 1, 2024, https://www.thehindu.com/elections/lok-sabha/openai-says-stalled-attempts-by-israel-based-company-to-interfere-in-indian-elections/article68237334.ece

[51] McKinsey & Company, “What is Generative AI?,” April 2, 2024, https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai

[52] William Pitts, “Arizona Officials Examine Dangers of Artificial Intelligence in Elections,” *12 News*, May 9, 2024, https://www.12news.com/article/news/politics/elections/arizona-officials-examine-dangers-of-artificial-intelligence-in-elections/75-9ebe94c8-5ad1-495d-a8b7-ccbb1544c2d4

[53] Sean Boynton, “Convincing AI Deepfakes of Politicians are Getting Easier, Report Warns,” *Global News*, May 31, 2024, https://globalnews.ca/news/10534195/ai-deepfake-politicians-cloning-tools-report/

[54] “The Rise of Synthetic Propaganda - Gen AI’s Growing Threat to Election Integrity,” *Resolver*, May 3, 2024, https://www.resolver.com/blog/gen-ai-disinformation-threat-2024-elections/

Endnotes

55 Alex Engler, “Fighting Deepfakes When Detection Fails,” Brookings, November 14, 2019, https://www.brookings.edu/articles/fighting-deepfakes-when-detection-fails/

56 James Vincent, “Deepfake Detection Algorithms Will Never be Enough,” *The Verge*, June 27, 2019, https://www.theverge.com/2019/6/27/18715235/deepfake-detection-ai-algorithms-accuracy-will-they-ever-work

57 Brad Smith, “Meeting the Moment: Combating AI Deepfakes in Elections Through Today’s New Tech Accord,” February 16, 2024, https://blogs.microsoft.com/on-the-issues/2024/02/16/ai-deepfakes-elections-munich-tech-accord/

58 Kaushal Rathi and Harry Keir Hughes, “C2PA: An Innovative Approach to Mitigating the Harms of Synthetic Content,” Infosys Knowledge Institute, September 11, 2024, https://www.infosys.com/iki/perspectives/mitigate-harms-synthetic-content.html

59 Antonio Grasso, “Restoring Trust in Online Content and Demystifying Deepfakes with C2PA Credentials,” LinkedIn Pulse, August 2, 2023, https://www.linkedin.com/pulse/restoring-trust-online-content-demystifying-deepfakes-antonio-grasso/

60 Naduvath, “Flex, Flux and the Foreigner”

61 Victor Mayer-Schönberger and Urs Gasser, “A Realist Perspective on AI Regulation,” *Foreign Policy*, September 16, 2024, https://foreignpolicy.com/2024/09/16/realist-perspective-ai-regulation/

62 Trisha Ray, “The Paradox of Innovation and Trust in Artificial Intelligence,” Observer Research Foundation, February 22, 2024, https://www.orfonline.org/expert-speak/the-paradox-of-innovation-and-trust-in-artificial-intelligence

63 European Commission, *AI Act*, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

64 Daniel Leufer Fanny and Estelle Massé, “The EU Should Regulate AI on the Basis of Rights, Not Risks,” *Access Now*, January, 2022, https://www.accessnow.org/eu-regulation-ai-risk-based-approach/

65 Konrad Meier, “The EU AI Act: What It Means for Your Business,” Ernst & Young, March 15, 2024, https://www.ey.com/en_ch/insights/forensic-integrity-services/the-eu-ai-act-what-it-means-for-your-business

66 Terra Rolfe, “The EU AI Act: Insights from the World’s First Comprehensive AI Law,” Institute for Strategic Dialogue, March 20, 2024, https://www.isdglobal.org/digital_dispatches/the-eu-ai-act-insights-from-the-worlds-first-comprehensive-ai-law/

67 Foo Yun Chee and Tassilo Hummel, “Europe Sets Benchmark for Rest of the World with Landmark AI Laws,” *Reuters*, May 22, 2024, https://www.reuters.com/world/europe/eu-countries-back-landmark-artificial-intelligence-rules-2024-05-21/

Endnotes

68 Anulekha Nandi, "The First International AI Treaty: Progress with Caveats," Observer Research Foundation, May 22, 2024, https://www.orfonline.org/expert-speak/the-first-international-ai-treaty-progress-with-caveats

69 Bhaskar Chakravorti, "How Washington Missed the Boat on AI Regulation," *Foreign Policy*, June 10, 2024, https://foreignpolicy.com/2024/06/10/how-washington-missed-the-boat-on-ai-regulation/

70 Johanna Costigan, "China's New Draft AI Law Prioritizes Industry Development," *Forbes*, March 22, 2024, https://www.forbes.com/sites/johannacostigan/2024/03/22/chinas-new-draft-ai-law-prioritizes-industry-development/?sh=6aa771116095

71 Johanna Costigan, "Picking the Rose, Leaving the Thorn: Why China's AI Regulations Are Worth Careful Examination," Asia Society, April 11, 2023, https://asiasociety.org/policy-institute/picking-rose-leaving-thorn-why-chinas-ai-regulations-are-worth-careful-examination

72 "The ASEAN Economic Community Digest: A Business-Friendly ASEAN Guide for AI Ethics and Governance," *The ASEAN Magazine*, May 28, 2024, https://theaseanmagazine.asean.org/article/the-asean-economic-community-digest-a-business-friendly-asean-guide-for-ai-ethics-and-governance/

73 Gayathri Haridas, Sonia Kim Sohee, and Atharva Brahmecha, "The Key Policy Frameworks Governing AI in India," Access Partnership, October 2, 2023, https://accesspartnership.com/the-key-policy-frameworks-governing-ai-in-india/

74 Fatima Tahir, "Striking A Balance in India's Evolving AI Odyssey," 9dashline, June 7, 2024, https://www.9dashline.com/article/striking-a-balance-in-indias-evolving-ai-odyssey

75 Kazim Rizvi, "The Complexity and Impact of AI: Towards a Multi-Stakeholder Approach to AI Governance," Storyboard18, August 5, 2024, https://www.storyboard18.com/digital/the-complexity-and-impact-of-ai-towards-a-multi-stakeholder-approach-to-ai-governance-38543.htm

76 "India Plans to Release the Draft AI Framework by July: MoS IT Rajeev Chandrasekhar," India AI, March 6, 2024, https://indiaai.gov.in/news/india-plans-to-release-the-draft-ai-framework-by-july-mos-it-rajeev-chandrasekhar

77 "California Governor Gavin Newsom Vetoes Bill to Create First-in-Nation AI Safety Measures," *The Hindu*, September 30, 2024, https://www.thehindu.com/sci-tech/technology/california-governor-gavin-newsom-vetoes-bill-to-create-first-in-nation-ai-safety-measures/article68699871.ece

78 Stuart A. Thompson, "California Passes Election 'Deepfake' Laws, Forcing Social Media Companies to Take Action," *The New York Times*, September 17, 2024, https://www.nytimes.com/2024/09/17/technology/california-deepfakes-law-social-media-newsom.html

Endnotes

79 Aaratrika Bhaumik, “Regulating Deepfakes and Generative AI in India | Explained,” *The Hindu*, December 4, 2023, https://www.thehindu.com/news/national/regulating-deepfakes-generative-ai-in-india-explained/article67591640.ece

80 Amber Sinha, “Dispatches on Tech and Democracy: India’s 2024 Elections #5,” *Tech Policy Press*, May 21, 2024, https://www.techpolicy.press/dispatches-on-tech-and-democracy-indias-2024-elections-5/

81 Kamya Pandey, “Take Down Deepfakes Within 24 hours, IT Ministry Tells Social Media Platforms: Report,” *Medianama*, November 7, 2023, https://www.medianama.com/2023/11/223-it-ministry-deepfakes-order-social-media-companies-2/

82 Kamesh Shekhar and Jameela Sahiba, “Comparative Analysis of MeitY AI Advisory,” *The Dialogue*, March 18, 2024, https://thedialogue.co/blog-comparative-analysis-of-meity-ai-advisory/

83 Abhishek Dey and Melissa Cyrill, “India’s Regulation of AI and Large Language Models,” *India Briefing*, March 27, 2024, https://www.india-briefing.com/news/india-regulation-of-ai-and-large-language-models-31680.html/

84 “MeitY Approval Must for Companies to Roll Out AI, Generative AI Models,” *Economic Times*, March 2, 2024, https://economictimes.indiatimes.com/tech/technology/govt-directs-social-media-generative-ai-platforms-to-comply-with-it-rules/articleshow/108162287.cms

85 Nivedita Krishna, “MEITY Directives on AI and Gen AI – A Case of Too Little Too Late?,” *Times of India*, March 4, 2024, https://timesofindia.indiatimes.com/blogs/niveditas-musings-on-tech-policy/meity-directives-on-ai-and-gen-ai-a-case-of-too-little-too-late/#

86 Suraksha P, “Companies Hail Tweaked Advisory Easing AI Model Rollout,” *Economic Times*, March 18, 2024, https://economictimes.indiatimes.com/tech/technology/ai-firms-welcome-revised-ai-advisory-that-removes-requirement-for-govt-permission/articleshow/108567887.cms?from=mdr

87 Mitali Mukherjee, “AI Deepfakes, Bad Laws – and a Big Fat Indian Election,” Reuters Institute for the Study of Journalism, Oxford University, March 19, 2024, https://reutersinstitute.politics.ox.ac.uk/news/ai-deepfakes-bad-laws-and-big-fat-indian-election

88 Aditi Agarwal, “Govt Mulls Setting Up Artificial Intelligence Safety Institute,” *Hindustan Times*, October 13, 2024, https://www.hindustantimes.com/india-news/govt-mulls-setting-up-artificial-intelligence-safety-institute-101728833433153.html

89 Samir Saran, Anulekha Nandi, and Sameer Patil, “‘Moving Horizons’: A Responsive and Risk-Based Regulatory Framework for AI,” *ORF Special Report No. 229*, June 2024, Observer Research Foundation.

Endnotes

90 Benjamin Cedric Larsen, "The Geopolitics of AI and the Rise of Digital Sovereignty," Brookings, December 8, 2022, https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/

91 Colin Williams, "Developing a Holistic Approach for Tackling Undeclared Work: A learning resource from the Seminar of the European Platform Tackling Undeclared Work," 2017, 10.13140/RG.2.2.19277.64488.

92 Roberst Chesney and Danielle Citron, *Deepfakes and the New Disinformation War*, AI Institute, https://alinstitute.org/images/Library/DeepfakesAndDisinformationWar.pdf

93 Bora Erden et al., "Despite Trump's Claims, Footage Shows Large Crowd at Harris's Detroit Rally," *The New York Times*, August 12, 2024, https://www.nytimes.com/interactive/2024/08/12/us/elections/trump-harris-detroit-rally.html

94 Erden et al., "Despite Trump's Claims, Footage Shows Large Crowd at Harris's Detroit Rally"

95 Erden et al., "Despite Trump's Claims, Footage Shows Large Crowd at Harris's Detroit Rally"

96 Microsoft, https://news.microsoft.com/ai-deepfakes-elections/

97 Microsoft, https://unlocked.microsoft.com/the-prompt/

98 Council for Strategic and Defense Research (@CSDR_India), "AI, Disinformation, & the Future of Elections," X post, October 10, 2024, https://x.com/CSDR_India/status/1844347269589475684

99 Cathy Mulligan, "The Impact of AI on Democracy," Robert Bosch Academy, July, 2024, https://www.robertboschacademy.de/en/perspectives/impact-ai-democracy

100 Bhaskar Chakravorti, "If Kamala Harris Was the Czar of Anything, It Would Be AI," *Foreign Policy*, August 19, 2024, https://foreignpolicy.com/2024/08/19/kamala-harris-czar-ai-biden-white-house/

101 Jacob Helberg, "11 Elements of American AI Dominance," The Palantir Foundation, July 26, 2024, https://republic-journal.com/journal/11-elements-of-american-ai-supremacy/

102 Gustaf Kilander, "JD Vance Says US Could Drop Support for NATO if Europe Tries to Regulate Elon Musk's Platforms," *The Independent*, September 17, 2024, https://www.independent.co.uk/news/world/americas/us-politics/jd-vance-elon-musk-x-twitter-donald-trump-b2614525.html

Images used in this paper are from Getty Images/Busà Photography (cover and page 2) and Getty Images/Otto Stadler (back page).

ORF OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org