



EDITORIAL

Artificial Intelligence (AI) in the Year of Elections

Key Points of the Article/Editorial

Background

- The year 2024 has been billed by Time magazine as the "ultimate election year" the largest ever global exercise in democracy, with close to half the world's population engaging in elections.
- Since 2023 was the year of Artificial Intelligence (AI) frenzy, there is a worry that AI will turbocharge 2024 election-related misconduct. Think: Deepfakes, disinformation, robocalls and other dastardly forms of digital voter manipulation.
- It is no surprise, therefore, that governments around the world have leapt into action. From the regulation-loving Europeans and the regulation-allergic Americans to India's minister of state for electronics and IT, Rajeev Chandrashekhar- rules to tackle AI-created disinformation are being rushed out.

Ways that can Widen the Problems of AI

- (I) Through disinformation surge-
- The case of Bangladesh Nationalist Party leader, Tarique Rahman, whose manipulated video showed him suggesting a toning down of support for Gaza's bombing victims a surefire way to lose votes in a Muslim-majority country.
- There are at least 83 elections being held this year. Ironically, the volume of disinformation worldwide could surge overall precisely because of the pressure to catch disinformation coming from a few powerful governments.
- (ii) The growing might of the already mighty-
- The piling up of AI regulations could lead to a second paradoxical outcome reinforcing AI industry concentration. To get a sense of that concentration, consider this: Just three companies, OpenAI, Anthropic and Inflection, cornered two-thirds of all the investments made in generative AI last year and all that money came from just three other companies, Microsoft, Google and Amazon.
- The EU regulations as well as the Executive Order from the White House have seemingly sensible requirements of AI products, such as "watermarking" to clearly label AI-created content or requiring results of "red-teaming" exercises simulated attacks by adversaries to detect safety and security vulnerabilities in AI models.
- However, watermarking requirements are problematic since the watermarks aren't fool-proof and smaller companies reliant on external sources cannot verify such sourced content. Redteaming exercises are expensive once you account for the staffing and process complexities along with legal and documentation costs. Such regulations will only serve to lock in the power



8818810183 | 8818810184 ©

www.prayasiasacademy.com prayasiasacademy101@gmail.com prayasiasacademy

of the already powerful by creating a barrier to entry or making it infeasible for scrappy start-ups.

• Concentration in the AI industry hands power to a few companies, possibly locking in ethical lapses to which they may be blind, allowing risks to proliferate without oversight or competitive forces and biases, and black box systems gaining control of consequential decisions.

(iii) The perils of earnest guidelines-

- With these concerns about ethics, risk, and transparency in AI development, many regulators and civil society groups have been at work putting frameworks and guidelines in place. But these guidelines themselves could be problematic.
- Some believe AI's risks are existential, while others believe that such dire warnings are distracting us from more immediate higher-likelihood risks. Members of Prime Minister Narendra Modi's Economic Advisory Council themselves have argued that even the idea of risk management is risky in the case of AI.
- They argue that AI is non-linear, evolving and unpredictable a "complex adaptive system" and applying blunt instruments of pre-set risk frameworks would be foolhardy.
- A landmark law in New York that requires employers to use automated employment decision tools to audit them for race and gender bias was found to be toothless by a recent Cornell study. In the meantime, companies, such as IBM and OpenAI, have been volunteering their own transparency mechanisms. But we should be wary of foxes drafting reports on the state of the henhouse.

What Needs to be **Done?**

- (i) Democracy has many demons to battle even before we get to the AI demon. Already, political candidates have been jailed in several parts of the world, bomb threats have gone out, cellphone networks have been shut down, candidates have warned of bedlam if they lose or are taken off the ballot, and vote-buying and ballot-stuffing are still part of the toolkit. So, reform in that aspect is a first priority and then the threat of AI should be looked after.
- (ii) We should certainly take the electoral risks of AI seriously, but also keep in mind the risks presented by rushed efforts to manage those risks. There has been a scramble among regulators to reign in AI in advance of elections, setting up 2024 to be a year of the AI freak-out after 2023's AI frenzy. It is better that these well-intended regulators understand the unintended consequences of rushed regulations.
- (iii) AI regulators ought to think several steps ahead and formulate rules that anticipate the greater risks tomorrow. Voters in elections beyond 2024 will be grateful for such foresight.
- Therefore, the threats posed by artificial intelligence during elections are significant and multifaceted. From the potential for misinformation and deep-fake manipulation to the risks of biased algorithms influencing voter decisions, there are numerous challenges to address. It's imperative for governments, tech companies, and civil society to collaborate on robust regulations, transparent AI systems, and comprehensive cyber-security measures to safeguard the integrity and fairness of democratic processes in the face of advancing technology.