Impending Expansion of AI Misuse towards Militarization in India

Param Raval
Université de Montréal, Mila - Quebec AI Institute
Montréal, Canada
param005raval@gmail.com

1 Introduction

Facial recognition technology (FRT) has always had the risk of being weaponized by malicious actors in power including private and state institutions. With greater data consolidation capabilities, artificial intelligence synergizes with extended dataveillance [1] to give these actors better tools to achieve objectives potentially harmful to the rights of minorities and political enemies. With an urban population of $\sim$500 million out of a total $\sim$1.45 billion [2], and an emerging base of around 750-800 million active internet users [3], India provides a compelling case study to analyze AI misuse. Being a non-western democracy, it also allows us to critique the existing and proposed frameworks to regulate the state use of surveillance and AI technology for public safety and beyond.

We argue that the recent deterioration of human rights safety in India [4,5], with the government targeting its critics, minorities, and other vulnerable sections, and state and military deployment of FRT in policing points to a larger threat in impending expansion of harmful use of AI systems. Further, we observe that frameworks proposed to assess the threats of and regulate such systems are found lacking when applied in this case. When combined with the weaponization of AI towards swaying public opinion in favor of the government, the situation sets the stage for dangerous advancements in the near future. Based on our observations, we call for a re-evaluation of global regulatory frameworks and to extend this reasoning to other nations with systems vulnerable to AI-driven misuse by harmful actors.

2 Observations and proposal

In recent years, the Indian government has invested significantly in developing AI applications to enhance military defense and public safety measures [6,7] resulting in a slew of announced projects and global partnerships [8-10]. With the rampant increase in deploying AI in the public space, AI has also facilitated authoritarian attacks on dissenting individuals. These include the use of FRT in tracking and persecuting peaceful protesters speaking against government policies [11,13,14]. In the military, FRT has been used to scan crowds for persons of interest in regions of Kashmir where the former has a history human rights violations [12,15]. Furthermore, Indian urban spaces are notoriously well-surveilled with Delhi and Chennai being among the most surveilled cities in the world [16,17]. Despite the governmental opacity in on-going military uses, the on-going state use of AI in civil scenarios paint a bleak picture.

In a purported two-prong approach to AI policing, there are instances of government agencies using automated scripts to generate and spread misinformation and military propaganda on social media that influences public opinion on more stringent policing policies [18-20]. This approach to nurture public acceptance and to use FRT and other dataveillance methods in a civil setting to crackdown on dissent has set the scene for larger and more complex misuse of AI.

Most western democracies have codified laws and neutral regulatory bodies to support the privacy and related rights of all its citizens. Thus, even the academic frameworks usually proposed to guide

2024 Harms and Risks of AI in the Military (HRAIM 2024).

or regulate the states' use of AI assume such policies or bodies being in place [1,25,26,27]. They also usually assume the explicit intent of the state to self-regulate, or of exercisable user privacy rights and autonomy. Similarly, the laws passed in an effort to regulate private development and deployment of AI are again limited by the control to regulate being with the state.

However, in India, with the lack of regulatory bodies in India or the lack of the authority given to them, under similar laws and policies, the state and the military have been granted exceptional exemption from data privacy acts, right to information requests, and policing methods [21-24]. With extensive dataveillance and technological capacities, this risk is even worse now. Moreover, the present, widely-cited guidelines do little to prevent a government from using intelligent systems against its own citizens while being "legal" under the national laws. Hence, such frameworks, while giving a good start, cannot effectively apply to the governing bodies that cannot self-regulate and have demonstrable intent to misuse AI for political gains.

We contend that, even in an academic setting, international attention be drawn towards developing actionable, global regulatory frameworks that cover the assumptions made presently and make them applicable in democracies globally.

- Similar to the recent, developing understanding of data privacy, a concerted effort towards creating **public awareness** is needed not just for AI safety but digital ethics and digital governance practices – education that can both tackle state-spread misinformation and create an urgency to have the state adopt best practices.
- This may lead to international bodies and alliances enforcing governments to release public statements and reports committing to **risk assessment and responsibility** before deploying any large-scale AI system related to domestic defense or policing.
- And following that up with international regulations and treaties akin to the nuclear disarmament and non-proliferation efforts to create mandatory transparency, dismantling potentially harmful systems, and **commitment to crack down on AI-empowered abuses** of human rights of anyone anywhere.

Such efforts, while seemingly excessive, can curtail misuse and overuse of large-scale AI while the former are still nascent.

3 Conclusion

The current trajectory of the Indian state towards unregulated empowerment of AI systems under the guise of public safety has far-reaching consequences for nearly 1.5 billion people especially for vulnerable minorities. Such studies made for other nations will undoubtedly raise this number. While slow moving policymakers worldwide are lagging in matching the recent unfettered growth in AI applications, at least academic frameworks must be evolved rapidly to tackle cases as the one discussed here. We propose to move towards a more cohesive, urgent, and international effort to stymie the budding danger while possible.

References

[1] Fontes, Catarina, et al. 'AI-Powered Public Surveillance Systems: Why We (Might) Need Them and How We Want Them'. Technology in Society, vol. 71, Nov. 2022, p. 102137. DOI.org (Crossref), https://doi.org/10.1016/j.techsoc.2022.102137.

[2] World Development Indicators | DataBank. https://databank.worldbank.org/indicator/SP.POP.TOTL/1ff4a498/Popular-Indicators. Accessed 23 Sept. 2024.

[3] PTI. 'Over 50% Indians Are Active Internet Users Now; Base to Reach 900 Million by 2025: Report'. The Hindu, 3 May 2023. www.thehindu.com, https://www.thehindu.com/news/national/over-50-indians-are-active-internet-users-now-base-to-reach-900-million-by-2025-report/article66809522.ece.

[4] 'Human Rights in India'. Amnesty International, April 2024, https://www.amnesty.org/en/location/asia-and-the-pacific/south-asia/india/report-india/.

[5] Human Rights Watch. 'India: Events of 2022'. Human Rights Watch, Jan. 2023, https://www.hrw.org/world-report/2023/country-chapters/india.

[6] 'Indian Army Ramps up AI, but How Effective Will It Be? – DW – 10/18/2023'. Dw.Com, 18 Oct. 2023, https://www.dw.com/en/indian-army-ramps-up-ai-but-how-effective-will-it-be/a-67134664.

[7] 'Readout of the Inaugural U.S. – India Advanced Domains Defense Dialogue'. U.S. Department of Defense, 25 May 2023, https://www.defense.gov/News/Releases/Release/Article/3408336/readout-of-the-inaugural-us-india-advanced-domains-defense-dialogue/.

[8] 'Early Steps in India's Use of AI for Defence'. IISS, 18 Jan. 2024, https://www.iiss.org/en/online-analysis/online-analysis/2024/01/early-steps-in-indias-use-of-ai-for-defence/.

[9] DRDO & Directorate of Defence R&D, Israel Sign Bilateral Innovation Agreement for Development of Dual Use Technologies. Press Information Bureau, 09 Nov. 2021, https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1770299.

[10] 'Impact of AI in the Indian Army'. INDIAai, 15 Jan. 2024, https://indiaai.gov.in/article/impact-of-ai-in-the-indian-army.

[11] 'Delhi Police Is Now Using Facial Recognition Software to Screen "Habitual Protestors"'. The Wire, 29 Dec. 2021, https://thewire.in/government/delhi-police-is-now-using-facial-recognition-software-to-screen-habitual-protestors.

[12] 'J&K Police Steps up Effort to Get Facial Recognition Technology in Srinagar to Track down Terrorists'. India Today, 21 Oct. 2021, https://www.indiatoday.in/india/story/jammu-kashmir-police-effort-facial-recognition-technology-srinagar-terrorists-1867667-2021-10-21.

[13] 'Cops In India Are Using Artificial Intelligence That Can Identify You In a Crowd'. HuffPost, 16 Aug. 2018, https://www.huffpost.com/archive/in/entry/facial-recognition-ai-is-shaking-up-criminals-in-punjab-but-should-you-worry-too$_a$23502796.

[14] 'How Andhra Pradesh Built India's First Police State Using Aadhaar And A Census'. HuffPost, 23 July 2018, https://www.huffpost.com/archive/in/entry/how-andhra-pradesh-built-indias-first-police-state-using-aadhaar-and-a-census$_a$23487838.

[15] Update of the Situation of Human Rights in Indian-Administered Kashmir and Pakistan-Administered Kashmir from May 2018 to April 2019. Office of the United Nations High Commissioner for Human Rights, 8 July 2019, p. 43, https://www.ohchr.org/sites/default/files/Documents/Countries/IN/KashmirUpdateReport8July2019.pdf.

[16] 'Delhi, Chennai Among Most Surveilled In The World, Ahead Of Chinese Cities'. Forbes India, 25 Aug. 2021, https://www.forbesindia.com/article/news-by-numbers/delhi-chennai-among-most-surveilled-in-the-world-ahead-of-chinese-cities/69995/1.

[17] 'India's among the World's Top Three Surveillance States'. Quartz, 16 Oct. 2019, https://qz.com/india/1728927/indias-among-the-worlds-top-three-surveillance-states.

[18] 'NewsGuard Uncovers Massive India-Aligned Network Using AI and Fake Accounts to Target Country's Foes Operating without Detection for Three Years'. NewsGuard, 4 Sept. 2024, https://www.newsguardtech.com/special-reports/india-ai-fake-accounts-network. Accessed 23 Sept. 2024.

[19] Dutta, Deeplina Banerjee, Suyesha Dutta, Suyesha. 'AI Amplifies Political Reach but Magnifies Disinformation in India Elections'. Asia Pacific Foundation of Canada, 5 June 2024, https://www.asiapacific.ca/publication/indian-election-use-of-ai-political-campaigns-voter-engagement.

[20] P R, Biju and Gayathri O. 'Self-Breeding Fake News: Bots and Artificial Intelligence Perpetuate Social Polarization in India's Conflict Zones'. The International Journal of Information, Diversity, Inclusion (IJIDI), vol. 7, no. 1/2, Apr. 2023. DOI.org (Crossref), https://doi.org/10.33137/ijidi.v7i1/2.39409.

[21] Chadha, Kalyani, and Sachin Arya. 'Challenges to Press Freedom in India'. Oxford Research Encyclopedia of Communication, by Kalyani Chadha and Sachin Arya, Oxford University Press, 2021. DOI.org (Crossref), https://doi.org/10.1093/acrefore/9780190228613.013.974.

[22] Bajoria, Jayshree. 'Stifling Dissent'. Human Rights Watch, May 2016. Human Rights Watch, https://www.hrw.org/report/2016/05/25/stifling-dissent/criminalization-peaceful-expression-india.

[23] 'How India Surveils Its Citizens'. The Morning Context, 4 Sept. 2021, https://themorningcontext.com/chaos/how-india-surveils-its-citizens.

[24] Analysis of the Facial Recognition Technology-Enabled Surveillance Landscape in India • Software Freedom Law Center, India. 16 Jan. 2024, https://sflc.in/analysis-of-the-facial-recognition-technology-enabled-surveillance-landscape-in-india/.

[25] Rashid, Adib Bin, et al. 'Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges'. International Journal of Intelligent Systems, edited by Yu-an Tan, vol. 2023, Nov. 2023, pp. 1–31. DOI.org (Crossref), https://doi.org/10.1155/2023/8676366.

[26] King, Anthony. 'Digital Targeting: Artificial Intelligence, Data, and Military Intelligence'. Journal of Global Security Studies, vol. 9, no. 2, Mar. 2024, p. ogae009. DOI.org (Crossref), https://doi.org/10.1093/jogss/ogae009.

[27] Floridi, Luciano, et al. 'AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations'. Minds and Machines, vol. 28, no. 4, Dec. 2018, pp. 689–707. DOI.org (Crossref), https://doi.org/10.1007/s11023-018-9482-5.