COMPLEX TAPESTRY OF AI'S IMPACT ON SOCIETY

Abstract

The paper explores the multifaceted impact of Artificial Intelligence (AI) on society, tracing its origins from Alan Turing's foundational question in 1950 to the recent dominance of large language models like Transformers. It delves into the concept of Emergence in computational data, highlighting the evolution of machine learning and the emergent properties displayed by models like ChatGPT. The paper then dwells into the darker side of AI, focusing on the rise of Deep Fakes and their implications for trust, privacy, and security.

The erosion of trust in the age of AI trickery poses a threat to societal structures, leading to concerns like Reality Apathy and the Liar's dividend. Despite these challenges, the paper argues that a collaborative approach involving governments, tech platforms, and the public to navigate the uncertain road ahead. Legislative measures, technological tools, and education are proposed as strategies to address the risks associated with AI-based manipulation.

The paper concludes by emphasising the need for a dynamic approach, combining public awareness, regulations, fair use clauses, and global collaborations to safely navigate the complexities of the AI landscape.

*Spl. DGP Assam & In Charge, Assam Police Smart Social Media Centre - Nagrik Mitra
**Creative Consultant, Assam Police Smart Social Media Centre- Nagrik Mitra

The father of modern computing and WW2 Hero, Alan Turing presented his seminal paper[1] on Artificial Intelligence in 1950, which laid the foundation for the exploration of machines' ability to think. The paper opens with these words:

I propose to consider the question: 'Can machines think?'

Little did Turing know that his contemplations would set the stage for a technological revolution that not only transformed society positively but also brought forth unforeseen challenges. The year 2023 could well be considered how Tech Researcher Nirit Weiss-Blatt describes[2] it- the Year of AI Panic. Even though AI and Machine learning have been around for a couple of decades, everything started to change in June 2017.

The New World Order Of AI

The world as we know it saw a paradigm shift when a bunch of Google Engineers published[3] 'Attention Is All You Need', an oddly titled paper, proposing a new form of machine learning architecture called Transformer. This paper paved the way for the dominance of large language models and Generative AI took the centre stage replacing the good old fashioned Symbolic AI.

This new flanged set of algorithms also fundamentally changed the AI training models. Earlier, the problem of AI was the knowledge- you feed enough rule-based knowledge to a machine about a subject for it to make intelligent decisions. Today, all you need is an enormous amount of data sets and enough computational power, the lever & fulcrum of the new world order. This is the story of how we discovered the phenomenon of Emergence in computational data. The phenomenon which biologists used to explain complex behaviour arising from simple roots, such as Swarming of birds and Neurons of human brains, is now performing complex machine learning tasks.

To put it simply, a large data set coupled with high computational power will yield machines that are capable of performing tasks with emergent properties. It's a kind of machine learning evolution, a sudden appearance of new behaviour. Large Language Models (LLMs) such as ChatGPT display emergence by suddenly gaining new abilities as they grow. The data set behind ChatGPT, the new messiah of the digital world, is nothing but a large set of words; 300 billion to be precise, all scrapped from the Internet. It's an ever-evolving symphony where the notes of AI weave through the tapestry of constant self-innovation.

In an era marked by the rapid evolution of artificial intelligence, it is essential to avoid succumbing to a doomsday fear psychosis that indiscriminately vilifies all aspects of AI. Acknowledging and addressing the present risks associated with this burgeoning technology is the hour of need.

---

[1] https://academic.oup.com/mind/article/LIX/236/433/986238

[2] https://www.techdirt.com/2023/12/22/2023-the-year-of-ai-panic/?_cf_chl_tk=ozoGzwRu13yHPfndH3IEZHo9dQHMPX24WUv05bsqjkA-1703332390-0-gaNycGzNFHs

[3] https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf

AI Trickery & Deep Fakes

The rapid technological advancement is the cornerstone of human civilization. From rubbing stones to inventing the wheel, technology has played a key role in human society. All previous tech innovations helped us in communicating or propagating our ideas. The Printing Press from the sixteenth century or the Internet of the twentieth century, worked on the same idea. But AI changed that forever. While AI has the potential to revolutionise our lives positively, it also brings forth a side that is exploited by malicious actors to perpetrate crimes that were once unfathomable.

Deep fakes, a form of AI-based manipulation, have become a significant concern for society, with far-reaching implications on trust, privacy, and security. The recent barrage of deep faked audio visuals has sent chills across different sections of the society. These deep faked multimedia, designed to manipulate opinions and perception can have serious consequences. The rise of misinformation, disinformation, and cyber scams is evident, leading to financial losses and reputational damage. According to a recent study[4] by Sumsub, India is among top targets of deepfake identity frauds. From sextortion[5] to deep fake videos[6] & audios[7], scammers are already using AI to elevate their chicanery to dazzling new heights. While governments and other agencies across the globe are responding to this new theatre of crime, it's still a cat & mouse game. As the old adage goes, show me a ten- foot wall and I'll show you an eleven-foot ladder. From the general public to big corporations and celebs, everyone is still figuring out the best practices to deal with AI enabled frauds, copyright infringements and reputational damages.

But, there's more to this AI trickery which meets the eye. Deep fakes blur the line between reality and fabrication, requiring individuals to invest more effort in discerning the truth. The exhaustion of critical thinking poses a serious threat to a society. One of the primary concerns revolving around Deep Fakes is erosion of trust. Seeing is not believing. This erosion of trust has the potential to undermine societal structures, leading to what scholars call Reality Apathy[8]. These fabricated narratives pushed in the online mass media have the potential to influence collective memory of a society, creating collective false memories despite evidence to the contrary, a phenomenon known as Mandela Effect[9]. It was named after the false collective memory of Nelson Mandela's death in prison in the 1980s. In the age of Artificial Intelligence and deep fakes, the lines between reality and illusion become even more blurred.

The existence of convincing deep fake content can also give rise to what Robert Chesney calls the Liar's dividend[10]. Accusations based on recordings and videos can be dismissed by claiming that the source material has been manipulated using AI. This situation will be a formidable challenge for privacy, democracy, and society in general.

---

[4] https://sumsub.com/files/sumsub_identity_fraud_report_2023.pdf?utm_campaign=fraud_report2023-link&utm_medium=automation&utm_source=email&vgo_ee=KqSW6PUPmbMHS3iq%2F3sTkmmijeQMhuEhIm Hc5zhk%2BSpSIMFF%2BWgUqg %3D%3D%3AbToJO54FQ%2FpqiiPzYcXRFo5F3P9SKd76

[5] https://timesofindia.indiatimes.com/city/ghaziabad/retired-ips-officers-deepfake-used-to-blackmail-senior-citizen/articleshow/105603283.cms

[6] https://www.firstpost.com/explainers/what-is-a-deepfake-fraud-how-can-we-stay-safe-from-it-12882832.h

[7] https://economictimes.indiatimes.com/tech/technology/how-voice-deepfakes-are-emerging-as-a-new-threat/articleshow/106161843.cms

[8] https://www.cnas.org/publications/commentary/digital-threats-to-democracy-comfortably-numb

[9] https://en.wikipedia.org/wiki/False_memory#Mandela_effect

[10] https://www.psychologytoday.com/intl/blog/urban-survival/202310/who-thrives-in-a-world-of-deepfakes-and-misinformation

The Road Ahead

Amidst these emerging threats, which will impact not just individuals, but society as a whole, the road ahead is littered with uncertainty. All the stakeholders, including governments, tech platforms and the general public must unite and implement robust measures. Governments are exploring legislative measures to regulate the creation and dissemination of deep fakes. Recent initiatives[11] by the Indian Government in this direction signal a growing awareness of the need to address the challenges posed by AI-based manipulation. The AI Act[12] of the European Parliament which will regulate the use of artificial intelligence in the EU or the Kratt[13] initiative of Estonia, a small Baltic Nation, are some good starting points for India.

Technological efforts should focus on developing tools for flagging AI-based manipulations and detecting and adding Metadata and Encrypted Watermarking to AI Generated Content is already being explored by tech companies and governments around the world. Google's SynthID is one such Tool, which is being developed to provide AI disclosures about any content. In fact, major Tech Platforms have pledged[14] to add Metadata and Watermarks, one of the key promises made to the White House in an effort to curb the harmful and malafide use of AI generated content. However, despite some success stories, integrating AI into governance and public policy is still a distant dream. For the general public, education & awareness emerges as the first line of defence against AI based crimes and manipulation.

We need to incorporate media literacy programs to equip individuals with the skills to critically evaluate the content they encounter. Training programs that keep pace with technological advancements should be at the forefront now.

For law enforcement agencies, the key lies in adaptation, innovation, and collaboration. Harnessing the power of AI not as a weapon but as a shield is essential. Assam Police's AI campaign, particularly its positive engagement in raising awareness about Sharenting, demonstrates the potential of AI as a communication tool. The #ThinkBeforeYouShare initiative of Assam Police serves as notable examples of raising awareness about crimes against children using AI. There are serious concerns[15] about the privacy & safety of Children because of the rising interference of AI in our lives. The emergence of AI based toys, chatbots and social media, has the potential of creating a seismic shift in the social and behavioural development of our children. Today's children are growing up in a society, which is largely augmented with AI, their interaction with the world around them and the reality which they experience has been altered by AI. In a world where reality is just a click away from being reinvented, society must become the guardians of truth, armed with scepticism and a touch of digital Sherlock Holmes.

AI presents unprecedented opportunities for societal advancement. From rapid advancements in the field of medical science to fighting climate change, AI is at the forefront of tech-based interventions in solving global issues. AI systems are now performing top-level scientific research,

---

[11] https://www.livemint.com/news/indias-ai-regulations-will-allow-room-for-innovation-but-with-eye-on-safety-says-top-govt-official- 11701962451156.html

[12] https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[13] https://www.kratid.ee/en/tehisintellekt

[14] https://www.wired.com/story/ai-giants-pledge-external-probes-algorithms-white-house/

[15] https://www.unicef.org/innovation/sites/unicef.org.innovation/files/2018-11/Children%20and%20AI_Short%20Verson%20%283%29.pdf

which will impact millions of lives, positively. The field of clinical genomics has been completely transformed by AI's ability to process large scale data and predictive modelling. But it also comes with its fair share of challenges and risks. Instead of succumbing to panic, as a society, we need to adopt a more dynamic approach to prepare for and mitigate AI threats. With public awareness initiatives, adequate regulations, fair use clauses and multilateral collaborations, we can navigate the AI maze safely. Perhaps, it's time we applied the principles of Turing's idea about machines' ability to think on humans.

Let's take a moment to think before we react, prepare not panic.