Forum: Special Political Decolonization Committee - GA4

Issue: Limiting the Use of Unchecked AI as a Threat to Democratic Systems

Student Officer: Karolína Hummelová

Position: Chair

Table of contents

INTRODUCTION

Artificial intelligence by definition refers to the capability of computer systems to perform tasks, typically associated with human intelligence. These tasks may consist of aspects and values such as learning, perception, decision-making or even advanced analysis. Not only can Applications and devices equipped with AI see and identify objects, but they can also understand and respond to human language as well as learn from new information and experience. Additionally, such devices can also make detailed recommendations to users and experts and therefore act independently, replacing the need for human intelligence or intervention. From 2024, the most popular type of artificial intelligence is generative AI, which is a technology for creating original text, images or videos.

Nowadays, AI is vastly used in politics for electoral campaigns or the policy making process. It is utilized as a powerful tool thanks to technological advances, access to large amounts of data, machine learning and increased computing power. However, it is feared that these rapid technological improvements may result in a disruption and destabilization of democracies in the future. Alternative widely spread fears refer to the potential threat of disinformation, the corruption of social media, mass surveillance or the manipulation of the public opinion.

KEY TERMS

Artificial Intelligence (AI)

Field of science concerned with building computers and machines that can reason, learn, and act in such a way that would otherwise require human intelligence or that involves data whose scale exceeds what humans can analyze.

Deepfake Technology

Deepfake Technology refers to the type of artificial intelligence used to create convincing fake images, videos and audio recordings.

Algorithmic Bias

Describes systematic and repeatable errors that create unfair outcomes, such as privileging one arbitrary group of users over others.

Surveillance AI

The use of AI to improve surveillance practices and to recognize different elements, including vehicles, objects, humans, or specified events.

Disinformation Campaigns

False information intended to deliberately deceive or mislead individuals. Criminals, terrorist or extremist groups, state-sponsored actors, and conspiracy theorists use disinformation as a tool to spread propaganda, disseminate conspiracy theories, incite distrust and confusion, or even compel violence.

AI Regulatory Frameworks

In April 2021, the European Commission proposed the first EU artificial intelligence law, establishing a risk-based AI classification system. AI systems that can be used in different applications are analyzed and classified according to the risk they pose to users. The different risk levels mean more or less AI compliance requirements.

Microtargeting

The use of online data to tailor advertising messages to individuals, based on the identification of recipients' personal vulnerabilities. Such tactics can be used for promoting a product or a political candidate.

Echo Chambers

Environment or ecosystem in which participants encounter beliefs that amplify or reinforce their preexisting beliefs by communication and repetition inside a closed system and insulated from rebuttal.

Manipulation of Public Opinion

The deliberate use of misleading, deceptive, or persuasive tactics — often powered by AI, media, or propaganda — to influence people's beliefs, attitudes, and behaviors on political, social, or economic issues.

AI ethics

A multidisciplinary field that studies how to optimize the beneficial impact of artificial intelligence (AI) while reducing risks and adverse outcomes.

Digital Rights

Human rights and legal rights that permit individuals to access, use, produce, and publish digital media. They also allow the access and use of computers, other electronic devices, and telecommunications networks. The concept is particularly related to the protection and recognition of existing rights, such as the right to privacy or freedom of expression, in the context of digital technologies, especially the Internet.

GENERAL OVERVIEW

Generative artificial intelligence (AI) threatens to supercharge online disinformation campaigns. At least 47 governments deployed commentators to manipulate online discussions in their favor during the coverage period, double the number from a decade ago. Meanwhile, AI-based tools that can generate text, audio, and imagery have quickly grown more sophisticated and accessible and are now therefore easy to use, spurring a concerning escalation of these disinformation tactics. Over the past year, the new technology was utilized in at least 16 countries to sow doubt, smear opponents, or influence public debate.

AI has allowed governments to enhance and refine their online censorship. The world's most technically advanced authoritarian governments have responded to innovations in AI chatbot technology, attempting to ensure that the applications comply with or strengthen their censorship systems. Legal frameworks in at least 21 countries mandate or incentivize digital platforms to deploy machine learning to remove disfavored political, social, and religious speech. AI, however, has not completely displaced older methods of information control. A record 41 governments blocked websites with content that should be protected under free expression standards within international human rights law. Even in more democratic settings, including the United States and Europe, governments considered or actually imposed restrictions on access to prominent websites and social media platforms, an unproductive approach to concerns about foreign interference, disinformation, and online safety.

To protect internet freedom, democracy's supporters must adapt the lessons learned from past internet governance challenges and apply them to AI. AI can serve as an amplifier of digital repression, making censorship, surveillance, and the creation and spread of disinformation easier, faster, cheaper, and more effective. An overreliance on self-regulation by private companies has left people's rights exposed to a variety of threats in the digital age, and a shrinking of resources in the tech sector could exacerbate the deficiency. To protect the free and open internet, democratic policymakers — working side by side with civil society experts from around the world — should establish strong human rights-based standards for both state and nonstate actors that develop or deploy AI tools.

MAJOR PARTIES AND THEIR VIEWS

United States of America

The U.S. has introduced an AI Bill of Rights to protect citizens from AI misuse. Both entities stress the need for responsible AI development that prioritizes human rights and democratic values. Moreover, the U.S. focuses on voluntary AI safety measures and collaboration between government agencies and tech firms to prevent AI abuse and has passed 15 AI laws focusing on the impact on human jobs, administrative government as well as innovation. In the United States, AI regulation is more fragmented, with various federal and state-level initiatives rather than a unified national policy. The conversation around AI regulation in the U.S. has been driven by concerns over data privacy, cybersecurity, and the potential for AI to perpetuate bias. While there is no overarching federal AI law, the National Institute of Standards and Technology (NIST) has developed a framework to manage AI risks, and the White House has issued guidelines for

the ethical use of AI in government. The approach is heavily influenced by the country's commitment to innovation and maintaining a competitive edge in AI development. This decentralized approach, however, could lead to inconsistencies across states, particularly as some states like California push for more stringent regulations compared to others.

European Union

The European Union is arguably the frontrunner in AI regulation with its proposed AI Act, a comprehensive framework aimed at making Europe a global leader in AI development while ensuring simultaneously the technology is trustworthy and safe. Triggered by concerns over the ethical implications of AI, particularly in areas like facial recognition and predictive policing, the EU's approach categorizes AI systems based on their level of risk. What distinguishes the EU's AI Act is its risk-based approach, which ranges from minimal to high risk, with the latter facing stringent requirements. This framework is being pushed by the European Commission and has been influenced by the EU's General Data Protection Regulation (GDPR) model. The Act is closely tied to the EU's broader cybersecurity strategy, as it mandates that high-risk AI systems undergo rigorous testing for security vulnerabilities. This regulation also positions the EU as a leader in setting global AI standards, influencing other regions to adopt similar frameworks.

Peoples Republic of China

China views AI as a critical component of its national strategy, aiming to become the global leader in AI by 2030. The Chinese government has already implemented several AI regulations, focusing on not only security and ethical use, but also on the promotion of domestic AI industries. The country's regulatory approach is heavily centralized, with the government playing a significant role in both the development and oversight of AI technologies utilizing AI for extensive surveillance and censorship, often prioritizing state control over democratic principles. China's social credit system exemplifies AI's role in monitoring citizen behavior. AI-powered censorship tools in both nations enable governments to track and suppress online dissent, limiting freedom of speech. China has invested heavily in AI-driven governance, integrating smart surveillance into urban management and public security. One of the key drivers for AI regulation in China is national security. The government has implemented regulations that require AI systems, particularly those related to surveillance and data collection, to be secure and free from foreign influence. China's AI strategy is closely linked to its cybersecurity laws, creating a comprehensive framework that supports the country's broader ambitions in digital sovereignty.

Russian Federation

Vladimir Putin has made it clear that Russia's future is with AI. "Russia must become a world leader, not only in the creation, but also in the...penetration of artificial intelligence into all spheres of our lives without exception," the Russian president said at a government-linked AI conference in Moscow in December 2024. Russia has used AI for cyber warfare and disinformation campaigns, particularly in influencing foreign elections. The use of AI for state-controlled media narratives has been a key strategy in shaping public opinion in these countries. These practices highlight the risks of AI being weaponized to erode democratic freedoms and suppress opposing voices. Russia is expanding its artificial intelligence (AI) efforts due to the increasing attention that the nation's government is paying to the development of Al-assisted and Al-facilitated technologies. By its own admission, Moscow's Al development still lags far behind nearest peer competitors like China and the United States, but progress is already evident. Specifically, the Russian government and military are investing heavily in creating the intellectual and physical infrastructure necessary to facilitate Al development across the country, pushing for results in certain civilian and weapons platforms. For now, however, such efforts are at the early stages, facilitated greatly by the government's eagerness to expand the debate, conversation, and cooperation space between the country's growing hi-tech private sector and the expansive military-academic infrastructure. Such efforts merit close attention, given Russia’s willingness to achieve Al-related breakthroughs and its private sector's strong scientific and technical background.

Saudi Arabia

Saudi Arabia’s approach to AI regulation is deeply intertwined with its Vision 2030, a strategic framework aimed at reducing the country’s dependence on oil, diversifying its economy, and developing public service sectors. AI is seen as a key enabler of this transformation, and the Saudi data and ai Data & AI Authority. Saudi Arabia’s National Strategy for Data and AI (NSDAI), launched in 2020, lays out a comprehensive plan to make the country a leader in AI by 2030. The strategy emphasizes ethical AI, data protection, and the development of a robust AI ecosystem. What distinguishes Saudi Arabia’s approach, is its emphasis on AI’s role in achieving national objectives, particularly in areas like smart cities, healthcare, and energy.

India

India is rapidly emerging as a global powerhouse in AI, with a strong focus on leveraging the technology for economic growth and social development. The Indian government has introduced several initiatives to promote the development and deployment of AI, including the National AI Strategy and the National AI Portal. India's approach to AI regulation is characterized by its focus on inclusivity and accessibility, ensuring that AI benefits all segments of society. The government's regulatory efforts are closely linked to its cybersecurity strategy, with a focus on protecting critical infrastructure and ensuring that AI systems are secure and resilient. India is also pushing for regional cooperation on AI regulation, positioning itself as a leader in South Asia.

Tech Companies (Google, Meta, OpenAI)

Emphasize self-regulation and innovation while resisting strict governmental controls. These companies play a crucial role in AI development and deployment but face criticism for prioritizing profits over ethical concerns. AI-driven content recommendation algorithms used by social media giants like Meta (Facebook) and YouTube have been accused of amplifying misinformation and political extremism. OpenAI, the creator of advanced language models, has faced scrutiny over the potential misuse of AI-generated content. While these companies claim to be working on ethical AI principles, their business models rely on data-driven advertising and engagement optimization, which sometimes conflict with efforts to curb AI-driven disinformation.

TIMELINE OF KEY EVENTS

1921: Czech playwright Karel Capek released a science fiction play "Rossum's Universal Robots" (R.U.R.), which introduced the idea of "artificial people" which he named robots. This was the first known use of the word.

1950: Alan Turing published "Computer Machinery and Intelligence" which proposed a test of machine intelligence called "The Imitation Game".

1952: A computer scientist named Arthur Samuel developed a program to play checkers, which is the first to ever learn the game independently.

1955: John McCarthy held a workshop at Dartmouth on "artificial intelligence" which is the first use of the word, and how it came into popular usage.

1956: AI is formally recognized as a field of study at the Dartmouth Conference.

1958: John McCarthy created LISP (acronym for List Processing), the first programming language for AI research, which is still in popular use to this day

1966: ELIZA, created by the MIT computer scientist Joseph Weizenbaum, is widely considered the first chatbot and was intended to simulate therapy by repurposing the answers users gave into questions that prompted further conversation—also known as the Rogerian argument.

1981: The Japanese government allocated $850 million (over $2 billion dollars in today's money) to the Fifth Generation Computer project. Their aim was to create computers that could translate, converse in human language, and express reasoning on a human level

1997: IBM's Deep Blue defeats chess world champion Garry Kasparov, showcasing AI's capabilities in complex decision-making.

1997: Windows released a speech recognition software (developed by Dragon Systems).

2004: NASA uses AI to enhance the capabilities of two rovers sent to Mars to assist in rocky terrain, and make decisions in real-time rather than rely on human assistance to do so.

2006: Companies such as Twitter, Facebook, and Netflix started utilizing AI as a part of their advertising and user experience (UX) algorithms.

2011: IBM Watson wins Jeopardy! against human champions, demonstrating AI's natural language processing abilities.

2011: The release of Apple's virtual assistant Siri and Amazon's Alexa. Both had natural language processing capabilities that could understand a spoken question and respond with an answer.

2015: Elon Musk, Stephen Hawking, and Steve Wozniak (and over 3,000 others) signed an open letter to the worlds' government systems banning the development of (and later, use of) autonomous weapons for purposes of war.

2018: Cambridge Analytica scandal reveals how AI-driven data analytics influence democratic elections.

2020: OpenAI started beta testing GPT-3, a model that uses Deep Learning to create code, poetry, and other such language and writing tasks. While not the first of its kind, it is the first that creates content almost indistinguishable from those created by humans. GPT-3 was trained on 175 billion parameters, which far exceeded the 1.5 billion parameters GPT-2 had been trained on

2021: released DALL-E, a text-to-image model. When users prompt DALL-E using natural language text, the program responds by generating realistic, editable images. The first iteration of DALL-E used a version of OpenAI's GPT-3 model and was trained on 12 billion parameters.

2022: OpenAI released the AI chatbot ChatGPT, which interacted with users in a far more realistic way than previous chatbots thanks to its GPT-3 foundation, which was trained on billions of inputs to improve its natural language processing abilities.

2023: European Union drafts the AI Act, the world's first major attempt to regulate AI.

2024: Global discussions on AI governance intensify as nations recognize its potential threat to democracy.

QUESTIONS TO CONSIDER

How can AI be regulated to prevent the spread of misinformation while protecting free speech?

What measures should be taken to prevent AI-driven election interference?

How can governments ensure transparency in AI decision-making processes?

Should there be international agreements on AI ethics and governance?

How can AI surveillance be controlled to prevent abuses while ensuring public safety?

APPENDIX

Existing AI laws and policies in different countries

for the USA: white house information

The Race to Regulate AI

BIBLIOGRAPHY

https://en.wikipedia.org/wiki/Artificial_intelligence

https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)751478

https://www.ibm.com/think/topics/artificial-intelligence

https://carnegieendowment.org/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai?lang=en

https://cloud.google.com/learn/what-is-artificial-intelligence

https://www.techtarget.com/whatis/definition/deepfake

https://en.wikipedia.org/wiki/Algorithmic_bias

https://www.protex.ai/glossary/artificial-intelligence-for-video-surveillance

https://www.ohiosos.gov/globalassets/about/office-initatives/dec/disinformationoverview.pdf

https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

https://en.wikipedia.org/wiki/Microtargeting

https://en.wikipedia.org/wiki/Echo_chamber_(media)

https://en.wikipedia.org/wiki/Digital_rights

https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence

https://www.coursera.org/articles/history-of-ai

https://www.tableau.com/data-insights/ai/history

https://www.linkedin.com/pulse/10-countries-leading-ai-revolution-whos-setting-rules-betania-allo-n9clc

https://www.rferl.org/a/deepseek-russian-ai-sber-yandex-kandinsky-censorship/33305704.html