Background paper

Committee: Committee on Artificial Intelligence (CAI)

Topic A: Promoting the Ethical Development and Application of Artificial Intelligence Technologies for the Public Good

Chairs: Natalia Borjon Zamora and Constanza Olvera Garcia

The ethical development of artificial intelligence over the public good has been lacking since the normalization of AI technologies. According to Tech Target, “AI can influence several ethical issues and risks surrounding data privacy, security, policies and workforces. Generative AI technology can also potentially produce a series of new business risks like misinformation, plagiarism, copyright infringements, and harmful content.”. The problem with AI is that it lacks an impressive human capacity for creativity. Due to these unethical practices, there needs to be action to eradicate the current replacement there has been over human intelligence, as well as the spread of misinformation, private and transparent data practices, and individual control over private information.

AI has been present in our society back in the mid-20th century, even though the use of this technology has been virilizing just in the last 5 years. (What are the most important advances in AI?, Stanford University). The evolution of its use has taken an unfortunate turn for many members of our community. As technology advances, unethical applications progressively increase, which brings great consequences that can destabilize general social well-being. This continued growth demonstrates the urgent need to start implementing tools that can easily eradicate this growing problem. Since the use of these technologies is new for many people, there is not much conscientization about these and the correct use they should have. To give ciphers about the unethical use and application concerns currently going on so far we can state the following. According to Forbes, “Over 75% of consumers are concerned about

misinformation from AI", "As labor shortages become a pressing concern, 25% of companies are turning to AI adoption to address this issue", "77% are concerned that AI will cause job loss in the next year". "ChatGPT had 1 million users within the first five days of being available". This shows how people are using these technologies for their benefit but not for the public good. If continued with inappropriate use of AI, many jobs, privacy, and creativity can be lost in our society.

The most affected countries by the erroneous use of AI are India, China, Germany, Brazil, France, the United States, Spain, the United Kingdom, Japan, and Canada. This is only because there are the ones that have the biggest use of AI technologies. It's important to pay attention to the less developed countries that may not have enough resources to change the role they have taken. Furthermore, it's important to spread information since these societies do not count on knowing how the inappropriate use of AI could and will affect them in the short or long term.

The European Union has currently taken an active role in changing the perspective that society has taken over the incorrect use. Some of the countries that are more involved are Italy, by banning the use of Chat GPT, and Ireland, by seeking input on regulations, however, they are not the only ones that need to be taking action. Countries such as Mexico, Argentina, Peru, Saudi Arabia, and Serbia are also affected, even though because of the resources they count on or the lack of information that people have, there has not been a considerable change or measures. So far, the actions taken have not been big, even though it has been tiring to make the best of it. Some great examples are the Ethical Guidelines, which have been developed by the IEEE's Ethically Aligned Design, which guides responsible AI development, as well as regulatory measures to ensure ethical AI by the European Union.

The EU AI Act: The first regulation on artificial intelligence states, "Unacceptable risk AI systems are systems considered a threat to people and will be banned, Generative AI, like ChatGPT, would have to comply with transparency requirements and Limited risk AI systems should comply with minimal transparency requirements that would allow users to make informed decisions,". Non-governmental organizations such as UNESCO, and the Council of Europe as

well are constantly taking action and searching for new solutions to eradicate the current problem.

It is of utmost importance to begin taking actions that help us build a better society hand in hand with artificial intelligence and not one where values are lost and the integrity of many people is threatened. Therefore, it is important to start global collaboration, in which countries will decide the limits they will allow AI to have, and develop legal frameworks, in which they will obligate transparency, and fairness between people. However governments are the ones required to properly take action, society can also take the initiative to raise awareness in which they will help each other with the understanding of AI for them to have their limits that could lead to the best development.

It is noteworthy to eradicate the misuse of AI technologies. If we don't take action the problem will continue increasing until the point where unethical use of technology is no longer a problem anymore, but if not the hard consequences that society will face. The best way to end these problems is to consciously ourselves, and follow the legal frameworks. So the aftermath of unethical use does not bring such big repercussions to our society. That's why delegates must find a solution to eradicate the problem at all costs.

"Can smart machines outthink us, or are certain elements of human judgment indispensable in deciding some of the most important things in life?"
Michael Sandel, political philosopher, and Anne T. and Robert M. Bass Professor of Government.

Works Cited:

"AI Ethics: What It Is and Why It Matters." *Coursera*, https://www.coursera.org/articles/ai-ethics.

"EU AI Act: first regulation on artificial intelligence | News." *European Parliament*, 8 June 2023, https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

Guo, Mike. "The Ethics of AI In Business and Finance." *StreetFins*, 27 March 2023, https://streetfins.com/the-ethics-of-ai-in-business-and-finance/.

Haan, Katherine. "24 Top AI Statistics & Trends In 2023 – Forbes Advisor." *Forbes*, 25 April 2023, https://www.forbes.com/advisor/business/ai-statistics/.

"Italy became the first Western country to ban ChatGPT. Here's what other countries are doing." *CNBC*, 4 April 2023, https://www.cnbc.com/2023/04/04/italy-has-banned-chatgpt-heres-what-other-countries-are-doing.html.

Lawton, George. "Generative AI Ethics: 8 Biggest Concerns and Risks." *TechTarget*, 1 November 2023, https://www.techtarget.com/searchenterpriseai/tip/Generative-AI-ethics-8-biggest-concerns.

Pazzanese, Christina. "Ethical concerns mount as AI takes a bigger decision-making role." *Harvard Gazette*, 26 October 2020, https://news.harvard.edu/gazette/story/2020/10/ethical-concerns-mount-as-ai-takes-bigger-decision-making-role/.

"SQ2. What are the most important advances in AI?" *One Hundred Year Study on Artificial Intelligence (AI100)*, https://ai100.stanford.edu/gathering-strength-gathering-storms-one-hundred-year-study-artificial-intelligence-ai100-2021-1/sq2.

"What are governments doing to try to regulate AI?" *Euronews*, 9 November 2023, https://www.euronews.com/next/2023/09/11/which-countries-are-trying-to-regulate-artificial-intelligence.

"Which countries are most fearful of AI: New Ipsos survey | World Economic Forum." *The World Economic Forum*, 21 March 2023, https://www.weforum.org/agenda/2023/03/heres-which-countries-are-fearful-of-ai/.

Zara, Shruthy. "Can human intelligence be replaced by artificial intelligence?" *Karpagam Academy of Higher Education*, 30 September 2023, https://kahedu.edu.in/can-human-intelligence-be-replaced-by-artificial-intelligence/.

Background Paper

Committee: Committee on Artificial Intelligence (CAI)

Topic B: Deliberate On The Challenges Of Attributing Cyberattacks To Specific State Or Non-State Actors And The Implications Of Misattribution on International Relations

Chairs: Constanza Olvera García and Natalia Borjón Zamora

In the last years, society has been worried about not having security over its personal information or a state where its confidential information could be leaked to the rest of the world due to cyberattacks. According to the National Cyber Security Center, "An attack, particularly if carried out by a skilled adversary, may consist of repeated stages, which consists of a set of offensive actions against the information system." ("How cyber attacks work - NCSC.GOV.UK") These actions have been increasing over the years, not only because of the constant innovation of technology but also because of the rapid spread and normalization of AI in our society. All of this has an active role in the massive arrival of spam and misinformation. Increasing the activity and connection requests stopped by the firewall, failures of password authentication systems, and connection problems triggering slowness or errors in mobile devices.

Cybersecurity is crucial for states around the world. Countries rely heavily on technology, making them more vulnerable to their information being leaked, as well as misinformation being disseminated. The most recurrent problems over cyber security and misinformation are due to deep fakes. According to the University of Virginia, deep fakes refer to "an artificial image or video that is generated by a machine in which through photoshop, AI formulate people's opinions based on the internet content that is not real." Deep fakes have a strong impact on our society, due to the creation of these videos that tend to defraud with supposed messages provided by important authorities. The objective is to damage, alter, or destroy organizations and people. In addition, they cancel the services they provide, steal data, and use them for spying. Now people

are more focused and spending on technology and that makes them more sensitive to being attacked.

Cyber attacks have a long history, one of the first major incidents happened in the 1970s when a computer worm called "Creeper" spread through connected computers. It left a message saying "I'm the creeper, catch me if you can!". Later, incidents kept happening, such as the Stuxnet, a computer bug targeting Iran's nuclear sites, supposedly made by a country as well as a virus that spread worldwide, asking for money to fix affected computers. In the new days, these actions are even more easily achieved by anyone thanks to AI programs. Another example is, phishing, According to the EasyDMarC phishing statistics, “in 2022, the Netherlands was targeted by the highest phishing attacks, with a staggering 17.7% of all attacks. Russia, Moldova, the USA, and Thailand follow”. Not to mention, Specops Software found that “The United States of America has experienced the most significant cyber-attacks through Identity-Based attacks, totaling 156 between the period of May 2006 and June 2020”. All the activities stated before had been increasing their activity in the past of the time, and if no actions were taken, states would not be the only ones affected by the attacks managed by these technologies.

During the 70’s, people didn't call these events "cyberattacks" like they do now. Over the past, technology has advanced and reached a point in which humans are not the ones running the system, that way technology advances, and our digital systems become more connected. This is a worldwide problem considering that it causes a lot of harm, to businesses, governments, and even regular people in our society, all those becoming at risk to state or non-state actors. The risks of artificial intelligence have become an increasingly recurrent and relevant topic as they are here to stay and will remain present in a thousand positive, but also negative ways in our daily lives.

It's crucial that the solutions to these current issues, as time passes, technology does as well, and not for everyone in a constructive form. The goal is to reach a point in which society no longer has fear over their information being leaked but is also threatened by it. The best solution to eradicate these crescent issues is to implement more cyber security as a society, as well as the states, avoiding more confidential information leaking as well as misinformation circulating. As well as implement open investigation labs that are solely from the governments, that way they are trustworthy. Not to mention, the implementation of more restricted limits over

how far society can use AI. With all stated, delegates should put their best efforts to eradicate these issues and come up with the best solutions that would help their states and others.

"Success in creating AI would be the biggest event in human history. Unfortunately, it might also be the last, unless we learn how to avoid the risks."

Stephen Hawking

Works Cited

"Artificial Intelligence (AI) Cybersecurity." *IBM*, https://www.ibm.com/ai-cybersecurity. Accessed 19 January 2024.

". . - definition of . . by The Free Dictionary." *The Free Dictionary*, https://www.annualreviews.org/doi/full/10.1146/annurev-polisci-051120-104535#_i2. Accessed 19 January 2024.

"How cyber attacks work - NCSC.GOV.UK." *National Cyber Security Centre*, https://www.ncsc.gov.uk/information/how-cyber-attacks-work. Accessed 19 January 2024.

"Phishing Statistics and DMARC." *EasyDMARC*, https://easydmarc.com/blog/phishing-statistics-easydmarc-report-january-june-2022/. Accessed 19 January 2024.

"What the heck is a deepfake? | UVA Information Security." *UVA Information Security*, https://security.virginia.edu/deepfakes. Accessed 19 January 2024.