Dear Select Committee on Adopting Artificial Intelligence,

My name is Niharika Bandam, an international student at The Australian National University, where I am pursuing a postgraduate degree in Applied Accounting and Financial Management. I would like to convey my concerns about the potential risks posed by unregulated advancements in Artificial Intelligence (AI). As an international student in Australia, I already encounter numerous scam calls each week, a situation that could be exacerbated exponentially with the incorporation of AI technology.

The risks associated with unchecked AI development are manifold and could have many unforeseen consequences, including empowering terrorists to create bioweapons and disrupting critical systems. For instance, a paper published by Collaborations Pharmaceuticals in 2022 highlighted how an AI designed to discover new drugs created 40,000 lethal molecules in less than six hours, many of which were identical to existing chemical weapons. Dr Fabio Urbina, the lead author of the paper, warned about the ease with which someone with basic python code and machine learning skills could recreate this scenario.

Studies also indicate the potential misuse of Large Language Models (LLMs) in the manufacturing of bioweapons. A notable example is the case of college students utilising a chatbot to learn how to create pandemic pathogens from synthetic DNA. Furthermore, fears have been raised by Dario Amodei, CEO of Anthropic, and Matt Clifford, the UK Prime Minister's joint Representative for the AI Safety Summit, about the potential for AI to enable large-scale biological attacks within the next couple of years.

In light of these risks, President Biden issued an Executive Order in October 2023 with the aim of securing safe, trustworthy AI. This order includes measures for screening risky DNA sequences and establishing robust oversight mechanisms. However, it is alarming to note that currently, approximately 20% of DNA orders go without any screening. Moreover, there is no evidence of Australia following the US's lead or exploring alternative measures to achieve the same outcomes, despite Biden's order being almost six months old.

Australia already has regulations in place for the importation of synthetic DNA, which could be adjusted to meet the screening standards promoted by the US. I would urge the Senate Inquiry to seek evidence from the Department of Health, the Office of the Gene Technology Regulator, the Department of Home Affairs, and the Department of Industry to better understand the biosecurity risks posed by AI and the actions being taken to mitigate these risks.

Beyond the potential for biological threats, the increasing capabilities of AI pose significant cybersecurity risks. For example, Google discovered that ChatGPT could pass an interview for a high-paying engineering position, demonstrating the potential for AI-enhanced cyberattacks. This risk is further compounded by the ability of AI to create convincing scam texts and deep fake voices, making it increasingly difficult for individuals and small businesses to stay safe online.

A recent KPMG report estimates that cyber attacks already cost Australia $29 billion per year, with small businesses being the primary target. The report also detailed 153 cyber incidents in critical infrastructure in 2023 alone. With the projected increase in the capabilities of cyber criminals due to AI, the potential for more significant attacks on our critical infrastructure is a realistic concern.

AI advancements, such as ChatGPT, Auto-GPT, and text-davinci-003, demonstrate their potential in various areas of cyber offensive. These include researching vulnerabilities in targets, targeted phishing attacks, malware generation and modification, and evasion of antivirus software. In light of these risks, it is imperative that we improve safety measures and enhance safety controls in AI systems.

To conclude, it seems we are at a crossroads. Either we risk making all our remote services highly vulnerable or we enter a “cyber arms race”, where each of us needs an army of AI bots for protection. I believe that the government should take immediate action to prevent this from happening.

Thank you for your time and consideration of these critical issues.

Regards,

Niharika Bandam