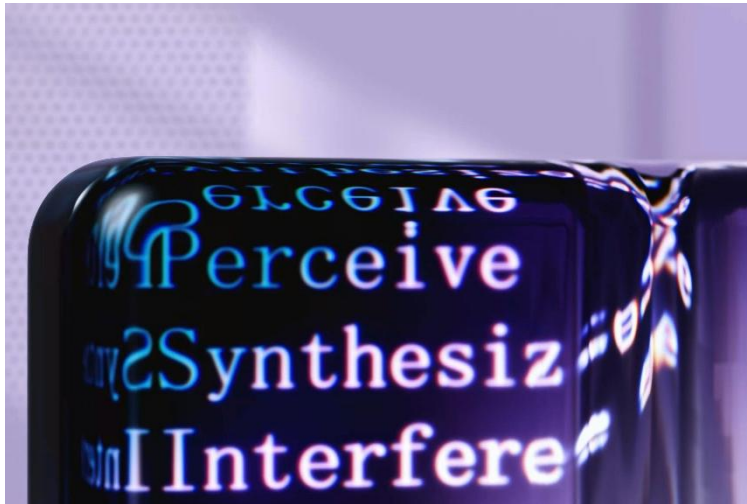


What AI Risks Concern Malaysia?

Rachel Gong and Khoo Wei Yang



KRI's latest report "AI Governance in Malaysia: Risks, Challenges and Pathways Forward" tackles key questions on AI risks, governance challenges and feasible pathways forward. It offers a snapshot of the current landscape, a conceptual framework of AI risks and an assessment of existing gaps and challenges in technology governance. The report also lays out a set of policy recommendations in line with the government's AI ambitions at the national level while recognising international pressures and trends.

Drawing on in-depth interviews and a roundtable with stakeholders and subject matter experts, KRI found three main types of AI risks that are of specific concern in Malaysia.

Risk of being left behind

The first type of AI risk is the risk of being left behind by not adopting AI quickly and widely. The great potential of AI – from raising economic productivity, to expanding scientific inquiry, and to improving human health and living conditions – implies large opportunity costs of not adopting AI.

Views are short opinion pieces by the author(s) to encourage the exchange of ideas on current issues. They may not necessarily represent the official views of KRI. All errors remain the authors' own.

This view was prepared by Dr Rachel Gong and Khoo Wei Yang, researchers from the Khazanah Research Institute (KRI).

Edited versions of this view were previously published by the [Malaymail](#) and [Malaysiakini](#).

Authors' email address:

rachel.gong@krinstitute.org

khoo.weiyang@krinstitute.org

Attribution – Please cite the work as follows: Gong, Rachel and Khoo Wei Yang. What AI Risks Concern Malaysia? Kuala Lumpur: Khazanah Research Institute. License: Creative Commons Attribution CC BY 3.0.

Information on Khazanah Research Institute publications and digital products can be found at www.KRIInstitute.org.

Image by Google Deepmind via [pexels.com](https://www.pexels.com)

If Malaysia cannot scale AI adoption, it risks being left behind other countries that are adopting AI more widely across sectors and industries. Generally, developing countries risk missing out on the benefits of AI if their public and private sectors are slow to adopt AI due to lack of use cases, concerns about high costs or unsuitability of AI models.

Apart from opportunity costs in AI-related benefits, direct economic losses are also a source of concern. Established, traditional firms risk being outpaced by newer, digitally-competent businesses competing in the same market. In the context of global trade, countries that lag in adopting and innovating AI in their industries risk losing global market competitiveness.

Risk of unintended consequences

The second type of AI risk is the risk of unintended harm. Most people have probably heard about how AI can unintentionally perpetuate stereotypes due to biased training data. For example, when asked to generate images of doctors, generative AI tends to show pictures of men, while when asked to generate images of nurses, AI shows pictures of women. This happens when AI models are trained on data that have more images of male doctors than of female doctors, so the models predict that doctors are likely to be men and nurses are likely to be women.

Another form of unintended harm can happen should there be an accidental technical failure. A failure to properly identify objects in a self-driving car could have disastrous consequences, as happened in 2018 when a self-driving Uber car struck and killed someone in the United States.

A third type of unintended harm is structural in nature and takes place on a broad social scale. For example, one of the promises of AI is that it will improve productivity by automating tasks, thus requiring fewer workers. This can result in firms laying off people or not hiring new workers to save costs, especially for jobs involving routine tasks. If not addressed, this in turn could increase unemployment rates or lower wages, resulting in greater social unrest over the long term.

A fourth way in which unintended harm can occur is when people don't have the time or the inclination to factcheck what generative AI tools like ChatGPT tell them. For example, there have been multiple accounts of lawyers in the United States using ChatGPT to write legal case briefs. ChatGPT did so by inventing cases, histories and citations for the briefs which were then submitted in court and subsequently thrown out, causing the lawyers and their clients to lose their cases.

Risk of malicious AI

The third type of AI risk is the risk of malicious use of AI, where AI is intentionally used to cause harm, for example in cyberattacks, to carry out scams and fraud or to be used as a weapon, such as lethal autonomous drones. These represent illegal malicious uses of AI, but AI could also be used in a way that isn't technically illegal but is ethically questionable, for example in the production and distribution of misinformation or deep fakes. This is particularly risky during political election campaigns.

Even where laws exist to combat these malicious uses of AI, enforcement remains a challenge because of how quickly AI works and how hard it is to detect as the source of these harms.

Improve AI readiness to better address AI risks

Addressing these three types of AI risks can be challenging because they cannot be traced to a single source along the AI system pipeline from design to deployment. Not only can the types of harm resulting from AI misuse be varied, but the scale, sophistication and speed at which harm is exacted with the use of AI far surpasses traditional detection and control mechanisms.

For example, widespread integration of surveillance and predictive AI systems in digital spaces such as social media are said to improve personalisation but also lead to the erosion of personal privacy. As digital platforms undercut each other by amassing (sometimes highly sensitive) user data to produce accurate analytics, companies are incentivised to maximise data collection.

None of this is technically illegal. Regulations on data governance have limited impact if there is low public awareness and concern about privacy rights and the power to determine the terms of data sharing and use is concentrated in the hands of a few platforms.

Readying policymakers, industry and the public for the widespread adoption of AI can help society address AI risks. There are at least four ways this can be done. First, establish clear and cohesive AI guidelines and governance frameworks. Second, improve AI capabilities both in terms of work skills and governance competencies. Third, expand public awareness and education on AI benefits and risks. Fourth, increase resources for AI adoption and governance, from financial resources to human capital to infrastructure.

To reap the benefits of AI without falling prey to its risks requires us to improve AI readiness and governance here and now, without speculating about uncertain risks such as AI superintelligence in the future.

References

KRI. 2025. AI Governance in Malaysia: Risks, Challenges and Pathways Forward. Kuala Lumpur, Malaysia: Khazanah Research Institute.