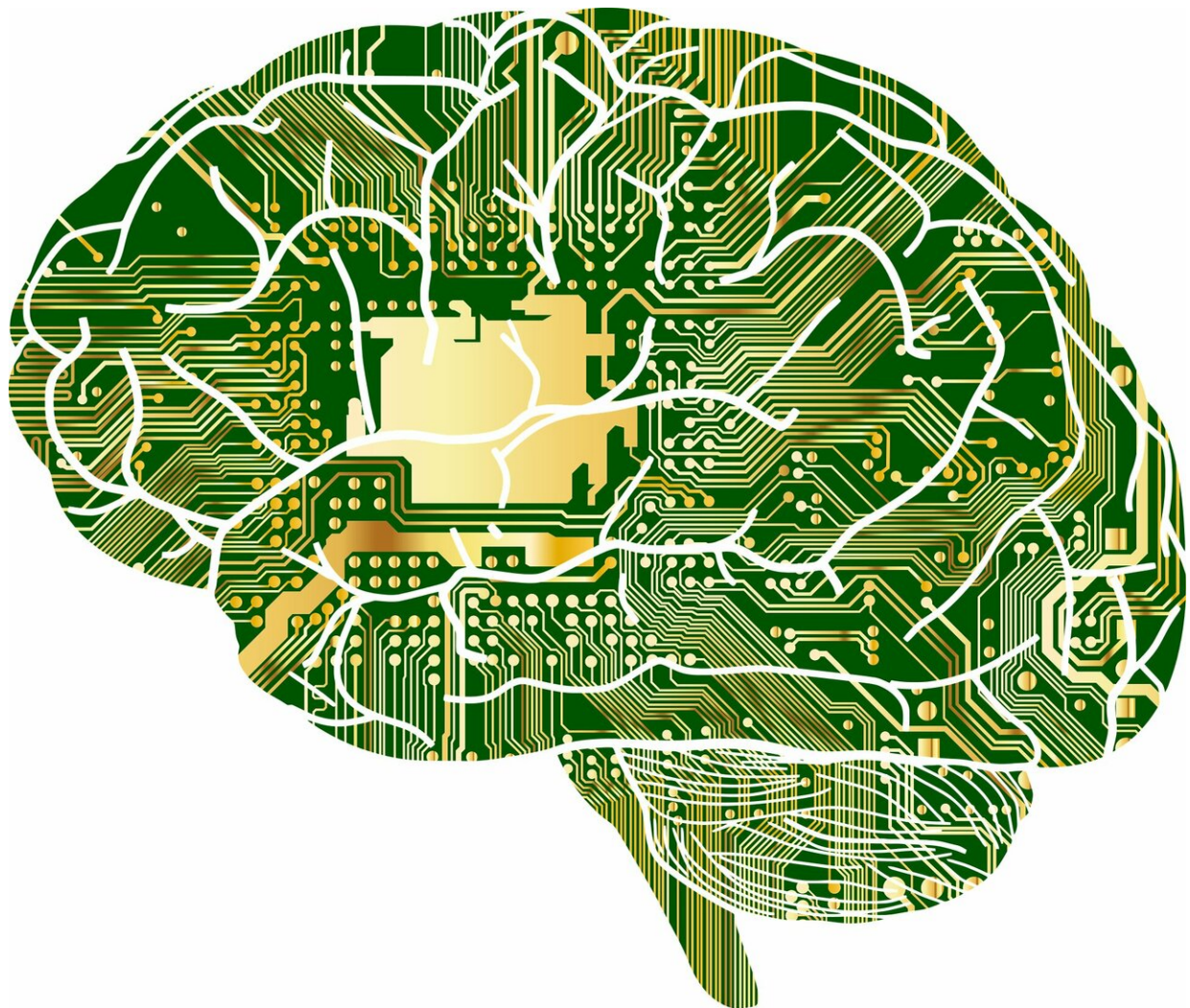


# AI: The real threat may be the way that governments choose to use it

November 2 2023, by Joe Burton

---



Credit: CC0 Public Domain

The significant risks that AI poses to global security are becoming clearer. That's partly why UK prime minister Rishi Sunak is hosting other world leaders at the [AI Safety summit](#) on November 1-2 at the famous second world war code-breaking site Bletchley Park. Yet while the technology of AI is developing at an alarming pace, the real threat may come from governments themselves.

The track record of AI development over the last 20 years provides a range of evidence of [government](#) misuse of the [technology](#) around the world. This includes [excessive surveillance practices](#), the [harnessing of AI for the spread of disinformation](#).

Although recent focus has been on private companies that develop AI products, governments are not the impartial arbiters they might seem to be at this AI summit. Instead, they have played a role that's just as integral to the precise way that AI has developed—and they will continue to.

## **Militarizing AI**

There are continual reports that the leading technological nations are entering into an [AI arms race](#). No one state really started this race. Its development has been complex, and many groups—from inside and outside governments—have played a role.

During the cold war, US [intelligence agencies became interested](#) in the use of artificial intelligence for surveillance, nuclear defense and for the automated interrogation of spies. It is therefore not surprising that in more recent years, the integration of AI into military capabilities has proceeded apace in other countries, such as [the UK](#).

Automated technologies developed for use in the war on terror have fed into the development of powerful AI-based military capabilities,

including [AI-powered drones](#) (unmanned aerial vehicles) that are being deployed in current conflict zones.

Russia's president, Vladimir Putin, has declared that the country that [leads in AI technology will rule the world](#). China has also declared its own [intent to become an AI superpower](#).

## Surveillance states

The other major concern here is the use of AI by governments in surveillance of their own societies. As governments have seen domestic threats to security develop, including from terrorism, they have increasingly deployed AI domestically to enhance the security of the state.

In China, this has been [taken to extreme degrees](#), with the use of facial recognition technologies, social media algorithms, and internet censorship to control and surveil populations, including in Xinjiang where AI forms an [integral part of the oppression of the Uyghur population](#).

But the west's track record isn't great either. In 2013, it was revealed that the US government had developed autonomous tools to collect and sift through huge amounts of data on people's internet usage, ostensibly for counter terrorism. [It was also reported](#) that the UK government had access to these tools. As AI develops, its use in surveillance by governments is [a major concern](#) to privacy campaigners.

Meanwhile, borders are [policed by algorithms](#) and facial recognition technologies, which are increasingly being deployed by domestic police forces. There are also wider concerns about ["predictive policing"](#), the use of algorithms to predict crime hotspots (often in ethnic minority communities) which are then subject to extra policing effort.

These recent and [current trends](#) suggest governments may not be able to resist the temptation to use increasingly sophisticated AI in ways that create concerns around surveillance.

## Governing AI?

Despite the good intentions of the UK government to convene its safety summit and to become a world leader in the safe and responsible use of AI, the technology will require serious and sustained efforts at the international level for any kind of regulation to be effective.

Governance mechanisms are beginning to emerge, with the US and EU recently introducing significant new regulation of AI.

But governing AI at the international level is fraught with difficulties. There will of course be states that sign up to AI regulation and then ignore them in practice.

Western governments are also faced with [arguments that overly strict regulation](#) of AI will allow authoritarian states to fulfill their aspirations to take the lead on the technology. But allowing companies to ["rush to release"](#) new products risk unleashing systems that could have huge unforeseen consequences on society. Just look at how advanced text-generating AI such as ChatGPT could increase misinformation and propaganda.

And not even the developers themselves understand exactly how advanced algorithms work. Puncturing this "black box" of AI technology will require sophisticated and sustained investment [in testing and verification capabilities](#) by national authorities. But the capabilities or the authorities don't exist at the present time.

## The politics of fear

We're used to hearing from the news about [a super-intelligent form of AI threatening human civilization](#). But there are reasons to be wary of such a mindset.

As my own research highlights, [the "securitisation"](#) of AI—that is, presenting technology as an existential threat—could be used as an excuse by governments to grab power, to misuse it themselves, or to take narrow self-interested approaches to AI that don't harness the potential benefits it could confer on all people.

Rishi Sunak's AI summit would be a good opportunity to highlight that governments should keep the politics of fear out of efforts to bring AI under control.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: AI: The real threat may be the way that governments choose to use it (2023, November 2) retrieved 28 April 2024 from <https://techxplore.com/news/2023-11-ai-real-threat.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.