INSIGHT 2

# AI COULD EMPOWER NON-STATE ACTORS AND OVERWHELM SECURITY ORGANIZATIONS

In the future, more accessible and versatile AI will have implications for security. Non-state actors — friendly and hostile — will have access to capabilities traditionally held only by states. They might be able to deploy them faster than states, keeping security organizations in a constant race to catch up.

## TODAY

**AI is lowering barriers to entry and reducing the cost of conducting attacks.**[1] For example, AI can help someone with limited programming skills write malicious software.[2] Leading open-source AI models only have marginally less capabilities than what is currently considered the most powerful general-purpose AI, GTP-4 Turbo.[3] Their general-purpose nature makes them equally useful to all types of problems, including harmful activities. It is uncertain who will use AI more effectively and quickly — government bodies among rival nations or non-state actors.[4] However, AI could empower non-state threat actors, corporations, or nations who are not bound by legal or ethical constraints, and willing to apply the technology in ways other states cannot.

# FUTURES

**Many new actors could access large-scale monitoring in the future.** AI's ability to analyze large amounts of open-source data could provide new actors with the ability to track and predict the movement of police and military forces.[5] AI tools can help write malicious computer code, making cyber defence more difficult. Similarly, ChatGPT has been used to create evolving malware, malicious software that can change its original code to evade cyber defences.[6]

**AI can also be used in unconventional attacks, to lower the cost of inflicting physical harm or attacking infrastructure.** For example, AI can facilitate the process of 3D printing dangerous parts like those needed to make nuclear weapons.[7] AI could also be used to automate swarms of low-cost drones to overwhelm air defences,[8] providing an advantage to smaller actors who wish to target urban settings or confront modern militaries. Should AI greatly increase access and automate harm, this could increase pressure on the security sector and change how it keeps citizens safe.

# IMPLICATIONS

- Open-source AI could empower non-state threat actors with new tools and **erode advantages traditionally held by states**, such as surveillance and monitoring[9]
- **There may be constraints of the ability of law enforcement agencies to gather intelligence** as compared to non-state actors
- **More communities could challenge the use of AI** by law enforcement agencies
- Innovative use of AI could **surpass the ability of defence and security organizations to adapt**. Failures in public safety could weaken institutional trust or change public attitudes on appropriate government use of AI[10]
- Private AI firms could become the main players in the cybersecurity and intelligence sectors, including in spaces traditionally seen as within the public domain

## Endnotes


1 Kreps, Sarah and Richard Li. 'Cascading Chaos: Nonstate Actors and AI on the Battlefield'. Brookings, 1 February 2022

2 Scroxton, Alex. Research Team Tricks AI Chatbots into Writing Usable Malicious Code. Computer Weekly, 24 October 2023.

3 Huggingface. LMSys Chatbot Arena Leaderboard - a Hugging Face Space by Lmsys. Accessed 19 February 2024.

4 Hirsh, Michael. How AI Will Revolutionize Warfare. Foreign Policy (blog), 11 April 2023.

5 Homeland Security. Addressing Risks From Non-State Actors` Use of Commercially Available Technologies, 2022.

6 Mascellino, Alessandro. ChatGPT Creates Polymorphic Malware. Infosecurity Magazine, 18 January 2023.

7 Volpe, Tristan. Dual-Use Distinguishability: How 3D-Printing Shapes the Security Dilemma for Nuclear Programs. Carnegie Endowment for International Peace. Accessed 19 February 2024.

8 Ware, Jacob. Terrorist Groups, Artificial Intelligence, and Killer Drones. War on the Rocks, 24 September 2019.

9 Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes. UN Counter-Terrorism Centre (UNCCT) and UN Interregional Crime and Justice Research Institute (UNICRI), 2021.

10 Kreps, Sarah. Democratizing Harm: Artificial Intelligence in The Hands of Nonstate Actors. Brookings, November 2021





PDF: PH4-212/2025E-PDF
ISBN: 978-0-660-76883-0

Aussi disponible en français sous le titre : L'IA pourrait renforcer les acteurs non étatiques et submerger les organisations de sécurité.