Intelligence agencies have used AI since the cold war—but now face new security challenges

May 4 2023, by Dafydd Townley

Credit: Pixabay/CC0 Public Domain

Recent publicity around the artificial intelligence chatbot ChatGPT has led to a great deal of public concern about its growth and potential. Italy

recently banned the latest version, citing concerns about privacy because of its ability to use information without permission.

But intelligence agencies, including the CIA, in charge of foreign intelligence for the US, and its sister organization the National Security Agency (NSA), have been using earlier forms of AI since the start of the cold war.

Machine translation of foreign language documents laid the foundation for modern-day natural language processing (NLP) techniques. NLP helps machines understand human language, enabling them to carry out simple tasks, such as spell checks.

Towards the end of the cold war, AI-driven systems were made to reproduce the decision-making of human experts for image analysis to help identify possible targets for terrorists, by analyzing information over time and using this to make predictions.

In the 21st century, organizations working in international security around the globe are using AI to help them find, as former US director of national intelligence Dan Coats said in 2017, "innovative ways to exploit and establish relevance and ensure the veracity" of the information they deal with.

Coats said budgetary constraints, human limitations and increasing levels of information were making it impossible for intelligence agencies to produce analysis fast enough for policy makers.

The Directorate of National Intelligence, which oversees US intelligence operations, issued the AIM Initiative in 2019. This is a strategy designed to add to intelligence using machines, enabling agencies like the CIA to process huge amounts data quicker than before and allow human intelligence officers to deal with other tasks.

Machines work faster than humans

Politicians are under increasing pressure to make quicker informed decisions than their predecessors because information is available faster than ever before. As intelligence scholar Amy Zegart pointed out, John F. Kennedy had 13 days to decide on a course of action on the Cuban Missile Crisis in 1962. George W. Bush had 13 hours to formulate a response to the 9/11 terrorist attacks in 2001. The decisions of tomorrow might need to be made in 13 minutes.

AI already helps intelligence agencies process and analyze vast amounts of data from a wide range of sources, and it does so far quicker and efficiently than humans can. AI can identify patterns in the data as well as detect any anomalies that might be hard for human intelligence officers to detect.

Intelligence agencies are also able to use AI to spot any potential threats to the technology that is used to communicate across the internet, respond to cyber-attacks, and identify unusual behavior on networks. It can act against possible malware and contribute to a more secure digital environment.

AI brings security threats

AI creates both opportunities and challenges for intelligence agencies. While it can help protect networks from cyber-attacks, it can also be used by hostile individuals or agencies to attack vulnerabilities, install malware, steal information or disrupt and deny use of digital systems.

AI cyber-attacks have become a "critical threat", according to Alberto Domingo, technical director of cyberspace at Nato Allied Command Transformation, who called for international regulation to slow down the

number of attacks that are "increasing exponentially".

AI that analyses surveillance data can also reflect human biases. Research into facial recognition programs has shown they are often worse at identifying women and people with darker skin tones because they have predominately been trained using data on white men. This has led to police being banned from using facial recognition in cities including Boston and San Francisco.

Such is the concern about AI-driven surveillance that researchers have designed counter-surveillance software aimed at fooling AI analysis of sounds, using a combination of predictive learning and data analysis.

Truth or lie?

Online misinformation (incorrect information) and disinformation (deliberately false information) represent another major AI-related concern for intelligence agencies.

AI can generate false but believable "deepfake" images, videos and audio recordings, as well as text in the case of ChatGPT. Gordon Crovits of online misinformation research company Newsguard has said that ChatGPT could evolve into "the most powerful tool for spreading misinformation that has ever been on the internet".

Some intelligence agencies are tasked with stopping the spread of online falsehoods from affecting democratic processes. But it is almost impossible to identify AI-generated mis- or disinformation before it goes viral. And once fake stories are widely believed, they are very difficult to counter.

Agencies are also at increased risk themselves of mistaking false information for the real thing, as the AI tools used to analyze online data

may not be able to tell the difference.

Privacy concerns

The vast amount of data collected from surveillance activities that AI analyses is also creating concerns about privacy and civil liberties.

The World Economic Forum has declared that AI must place privacy before efficiency when used by governments in surveillance programs, while some scholars and others are calling for regulation to limit AI's impact on society.

Governments must ensure that agencies that use AI to conduct surveillance are doing so within the law. Such oversight would require clear guidelines being set, regulations to be enforced, and transgressors to be punished. Early indications are that governments have been slow to keep up, even in the United States.

The vulnerabilities of AI mean that, despite the technological advances of the post-cold war world, there is still a need for human agents and intelligence officers.

As Zegart states, what AI will do is undertake most time-consuming menial analysis roles that humans currently do. While AI will allow intelligence agencies to understand what the objects are in a photograph, for example, human intelligence officers will be able to say why those are objects are there.

This should lead to greater efficiency within intelligence agencies. But to overcome the fears of many citizens, legislation may need to catch up with the way the AI world works.

Commons license. Read the original article.

Provided by The Conversation

Citation: Intelligence agencies have used AI since the cold war—but now face new security challenges (2023, May 4) retrieved 23 April 2024 from https://techxplore.com/news/2023-05-intelligence-agencies-ai-cold-warbut.html