THE WALL STREET JOURNAL.

https://www.wsj.com/articles/military-looks-to-ai-to-improve-air-strikes-11571932283

BUSINESS | JOURNAL REPORTS: TECHNOLOGY

Military Looks to AI to Improve Air Strikes

As armed forces work on the weapons, they confront a big problem: AI can be easy to fool

While AI is a young field for armed forces, it is emerging as a future battleground in the technology race between the U.S. and China. PHOTO: JON KRAUSE

By Asa Fitch
Oct. 24, 2019 11:51 am ET

Militaries increasingly are turning to image recognition powered by artificial intelligence to make airstrikes more precise and better track targets.

One big problem with these AI systems: They are often ridiculously easy to fool. For instance, enemies could make an AI miss its target just by making minor alterations to its appearance. Or hackers could play havoc with an AI system as it is learning to recognize images by feeding it incorrect information.

It is a problem that the Pentagon is taking seriously. Even though the armed forces' AI systems are still at a very early stage, military leaders are calling on the academic and business communities to help protect the nascent technology from enemy deception and sabotage.

A future battleground

JOURNAL REPORT

- Read more at WSJ.com/techreport

MORE IN TECHNOLOGY

- Rein In Automation? At What Cost?
- New Disinformation Tactics
- AI in the Classroom
- The Home Wireless Business Heats Up

While AI is a young field for armed forces, it is emerging as a future battleground—not just in actual military actions but also in the technology race between the U.S. and its biggest global rival. China has said it will invest $1 trillion in AI as part of its 2030 plan that aims to make the country a leader in key technology areas. Christopher Ford, the U.S. assistant secretary of state for international security and nonproliferation, said at a recent congressional hearing that Beijing is determined to come out on top in AI, which it sees as the linchpin of the next revolution in military technology.

Yet the advances in AI are raising an age-old problem with new military equipment: Technological advances that make combat more effective also introduce new vulnerabilities.

In the U.S., the Defense Advanced Research Projects Agency, or Darpa, the Pentagon's incubator for cutting-edge technology, is exploring a range of uses for AI, from tools that instantly translate foreign languages to more combat-related applications, such as automatic target recognition.

Researchers at Duke University have demonstrated that disguising even a small part of an image of easily recognizable objects such as planes, bikes, cars and cats prevented them from being properly identified. In a military context, an adversary might try using such methods to fool AI-powered target recognition—which could lead to weapons missing targets or hitting the wrong ones.

Dawn Song, a professor at the University of California, Berkeley, who studies AI, says tricking systems that detect objects in photos is easy because these systems don't learn the same way humans do. While humans may think of stop signs as red and octagonal, featuring large white block letters, computer-vision systems merely process fields of pixels through complex operations to determine whether a stop sign is in the picture. Anyone who knows how those algorithms work can strategically affix stickers to a stop sign that can confuse a computer, making the AI recognize it as something else or not recognize it at all. "It is very easy to fool these systems today," Dr. Song says.

Darpa also is worried AI systems could be compromised early in their development. Because machine learning relies on systems processing troves of information to become smarter, an attacker can introduce errors by contaminating the data used to teach the AI algorithm. When UC Berkeley researchers "poisoned" a sampling of facial-recognition training images by

injecting a handful of mislabeled faces, they successfully caused actress Halle Berry to be misidentified as former Spanish soccer official Manuel Llorente, according to a 2017 paper.

The infiltration risk underscores why basic cybersecurity is even more important in the AI age, says J. Michael McQuade, vice president for research at Carnegie Mellon University.

Problems with AI-powered military equipment could have lasting consequences if commanders lose trust in such tools, says Ben Barry, a senior fellow at the International Institute for Strategic Studies in London, a think tank. “It’s not very good for the morale of the troops if they don’t trust the system,” he says.

First steps

Under a program called Guaranteeing AI Robustness Against Deception, or Gard, Darpa is trying to address some of the pitfalls the latest technological advances introduce. Darpa is so concerned about AI-spoofing techniques that the agency met with companies and academics in February to spell out its concerns and ask for ideas to make AI more accurate.

For now, both the use of AI in military operations and Darpa’s efforts to protect such tools from being fooled are still at an early stage. Darpa hasn’t yet funded any projects under the Gard program, according to a spokeswoman. The agency has said it is primarily interested in efforts that would safeguard against attempts to trick object detection, speech recognition and systems that detect what’s happening in videos.

While some efforts to defend AI systems have shown promise, researchers are still trying to figure out how to make AI tools more resilient. “It’s very much an open challenge, and it goes far beyond the military,” Dr. Song says. “In general, we need to make sure that [AI systems] are resilient against attacks, and I would say security is one of the biggest challenges in deploying AI.”

Mr. Fitch is a Wall Street Journal reporter in San Francisco. He can be reached at asa.fitch@wsj.com.

- **Retirement**
- **Small Business**
- **Technology**
- **Wealth Management**