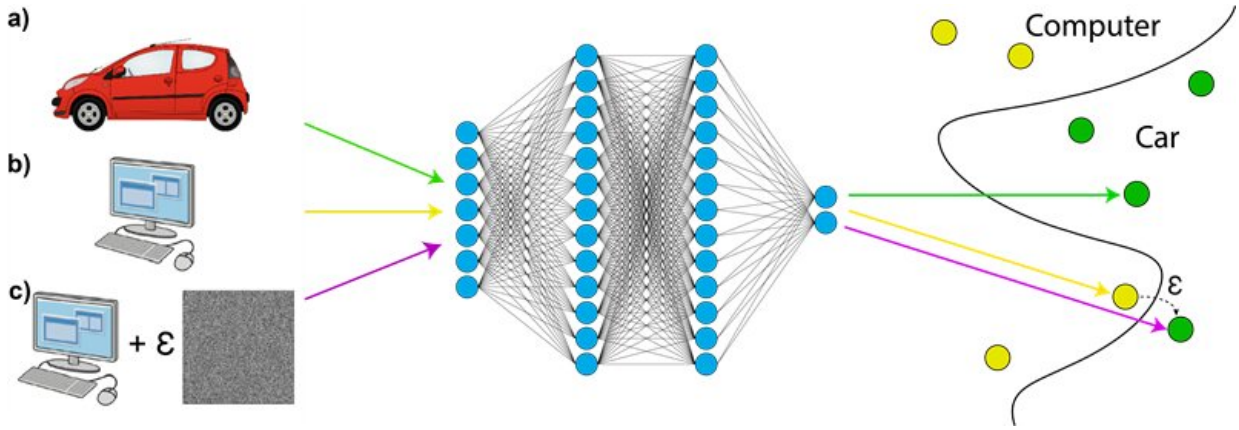
Can quantum computing protect AI from cyber attacks?

May 26 2023, by ALICE TREND and MUHAMMAD USMAN



A car (green line) and a computer (yellow line) are correctly identified by a machine learning algorithm. But when random noise is added to the image, representing a cyber attack, the algorithm makes a mistake and classifies the computer as a car (pink line). Credit: CSIRO

AI algorithms are everywhere. They underpin nearly all autonomous and robotic systems deployed in security applications. This includes facial recognition, biometrics, drones and autonomous vehicles used in combat surveillance and military targeting applications.

Machine learning and AI algorithms are trained to classify and identify image features, like the features of our faces in facial recognition. But the data underpinning these algorithms can be vulnerable to cyber

attacks. Subtle manipulation of image data by removing only a few pixels—invisible to the human eye—can result in incorrect predictions and even pose serious security threats.

Is quantum computing the answer?

Research published May 25 in *Nature Machine Intelligence* by researchers from CSIRO's Data61 and University of Melbourne reveals that advances in quantum technology may hold the key to protecting AI algorithms from cyber attacks.

Dr. Muhammad Usman is lead senior author of the paper and team leader of Quantum Systems at CSIRO's Data61. He described the potential of integrating quantum computing with AI as a game-changing technology.

"The hunt for quantum advantage is heating up," Usman said.

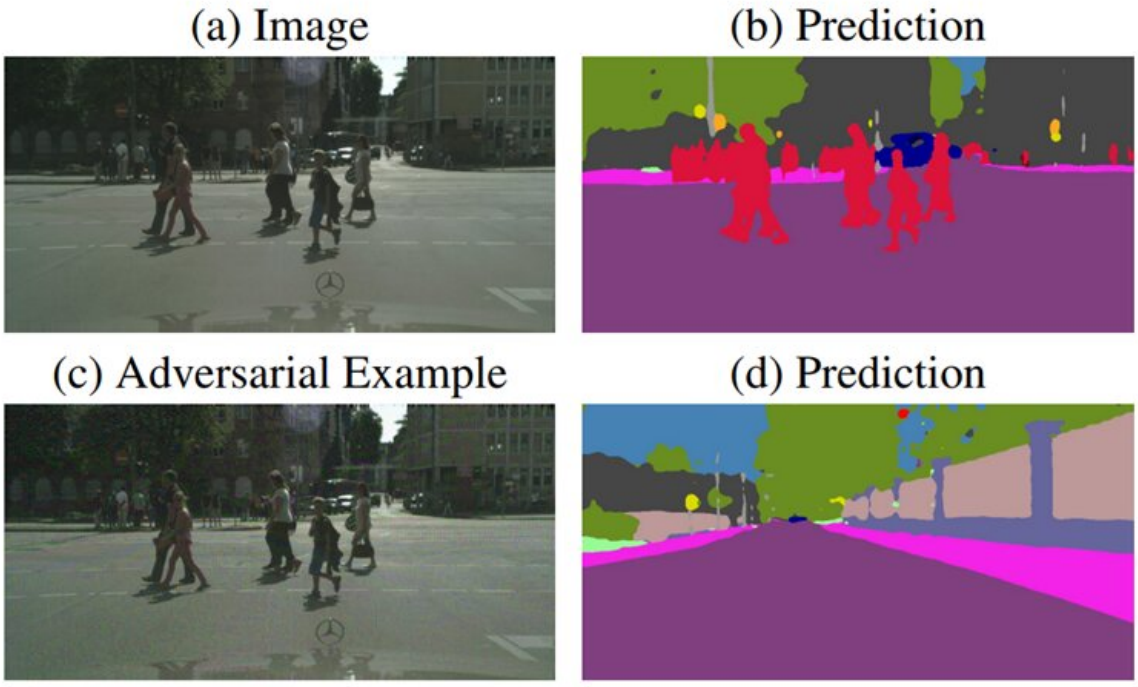
"Quantum machine learning is one of the front-runner applications of quantum computing. By integrating quantum with machine learning we can speed up AI training and enhance robustness against cyber attacks."

What's all the fuss about quantum computing?

Worldwide, interest in quantum is surging. On May 3, 2023, the Australian Government launched the National Quantum Strategy, with a vision for Australia to be recognized as a leader in the global quantum industry by 2030. The Strategy stated that quantum technologies are expected to create an Australian quantum industry worth $6B by 2045.

We have established our ambitious Quantum Future Science Platform to develop these world-leading technologies and launched a new program

that will soon be accepting students to become the next generation of quantum technology specialists.



A machine learning algorithm has been trained to identify people (top left image). The algorithm correctly identifies people (top right image), but if just a few pixels are changed in a cyber attack (bottom left image), the algorithm cannot identify the people (bottom right image). In the case of a driverless car, if a machine learning algorithm predicts there are no people on the road as the result of a cyber attack, there could be serious consequences. Credit: Jan Hendrik Metzen et al, Universal Adversarial Perturbations Against Semantic Image Segmentation, *arXiv* (2017). DOI: 10.48550/arxiv.1704.05712

How it works

Quantum computing is a new field of computing. It stores information as "qubits" rather than as binary "bits." While a single bit can store or process information in the form of 0 and 1 on a conventional computer, a quantum qubit can be placed in a 0 or 1 state or represent both states simultaneously. This is called superposition.

A second special property of quantum mechanics is known as entanglement, which allows qubits to interact with each other at long distances without any physical connection. Einstein famously called it "spooky action at a distance."

Calculations or code-breaking functions that may take a conventional computer thousands of years could take just hours on a quantum computer.

The quantum advantage

As more industries from transport to defense and banking incorporate AI, security will be paramount. Quantum could help ensure AI-powered technologies are resilient to attacks and may provide a competitive advantage for early adopters.

But Usman cautions that quantum computers could also be used to generate very powerful cyber attacks.

"This is a very serious cybersecurity threat. However, rapid advancements in quantum hardware and software and more sophisticated error mitigation strategies are coming. Quantum computers of the near future should enable quantum machine learning algorithms to start demonstrating advantages," Usman said.

"This is a very exciting research direction which could have significant socio-economic and security implications for Australia."

More information: Maxwell T. West et al, Towards quantum enhanced adversarial robustness in machine learning, *Nature Machine Intelligence* (2023). DOI: 10.1038/s42256-023-00661-1