How AI is shaping the cybersecurity arms race

February 24 2022, by Sagar Samtani

Credit: Pixabay/CC0 Public Domain

The average business receives 10,000 alerts every day from the various software tools it uses to monitor for intruders, malware and other threats. Cybersecurity staff often find themselves inundated with data they need to sort through to manage their cyber defenses.

The stakes are high. Cyberattacks are increasing and affect thousands of organizations and millions of people in the U.S. alone.

These challenges underscore the need for better ways to stem the tide of cyber-breaches. Artificial intelligence is particularly well suited to finding patterns in huge amounts of data. As a researcher who studies AI and cybersecurity, I find that AI is emerging as a much-needed tool in the cybersecurity toolkit.

Helping humans

There are two main ways AI is bolstering cybersecurity. First, AI can help automate many tasks that a human analyst would often handle manually. These include automatically detecting unknown workstations, servers, code repositories and other hardware and software on a network. It can also determine how best to allocate security defenses. These are data-intensive tasks, and AI has the potential to sift through terabytes of data much more efficiently and effectively than a human could ever do.

Second, AI can help detect patterns within large quantities of data that human analysts can't see. For example, AI could detect the key linguistic patterns of hackers posting emerging threats in the dark web and alert analysts.

More specifically, AI-enabled analytics can help discern the jargon and code words hackers develop to refer to their new tools, techniques and procedures. One example is using the name Mirai to mean botnet. Hackers developed the term to hide the botnet topic from law enforcement and cyberthreat intelligence professionals.

AI has already seen some early successes in cybersecurity. Increasingly, companies such as FireEye, Microsoft and Google are developing innovative AI approaches to detect malware, stymie phishing campaigns and monitor the spread of disinformation. One notable success is Microsoft's Cyber Signals program that uses AI to analyze 24 trillion security signals, 40 nation-state groups and 140 hacker groups to produce cyberthreat intelligence for C-level executives.

Federal funding agencies such as the Department of Defense and the National Science Foundation recognize the potential of AI for cybersecurity and have invested tens of millions of dollars to develop advanced AI tools for extracting insights from data generated from the dark web and open-source software platforms such as GitHub, a global software development code repository where hackers, too, can share code.

Downsides of AI

Despite the significant benefits of AI for cybersecurity, cybersecurity professionals have questions and concerns about AI's role. Companies might be thinking about replacing their human analysts with AI systems, but might be worried about how much they can trust automated systems. It's also not clear whether and how the well-documented AI problems of bias, fairness, transparency and ethics will emerge in AI-based cybersecurity systems.

Also, AI is useful not only for cybersecurity professionals trying to turn

the tide against cyberattacks, but also for malicious hackers. Attackers are using methods like reinforcement learning and generative adversarial networks, which generate new content or software based on limited examples, to produce new types of cyberattacks that can evade cyber defenses.

Researchers and cybersecurity professionals are still learning all the ways malicious hackers are using AI.

The road ahead

Looking forward, there is significant room for growth for AI in cybersecurity. In particular, the predictions AI systems make based on the patterns they identify will help analysts respond to emerging threats. AI is an intriguing tool that could help stem the tide of cyberattacks and, with careful cultivation, could become a required tool for the next generation of cybersecurity professionals.

The current pace of innovation in AI, however, indicates that fully automated cyber battles between AI attackers and AI defenders is likely years away.

Provided by The Conversation