The Future of AI in Cybersecurity

Why Generative AI is NOT the Whole Story

Kevin E. Jackson
CEO & Founder Level 6 Cybersecurity

Generative AI has dominated the headlines for more than a year, mesmerizing technologists and laypeople alike with its ability to create natural language interactions with software tools. While chatbots have been around for a long time, the leap forward in capabilities offered by tools like OpenAI's ChatGPT is significant. The power of Large Language Models (LLMs) feeding on big data collections and cloud-enabled search has impacted everything from software bug detection to how middle school kids write term papers. These advances trigger a laundry list of follow-up questions centered around one theme: how will generative AI affect *my* industry, discipline, or profession?

Cybersecurity is, of course, no exception.

Generative AI software, as the name implies, supports the generation of diverse, new content by learning the characteristics of existing content and relevant data. The source information and generated outputs can be text, video, audio, images, raw data, and more. At the forefront of this technology are the LLMs, such as the model powering OpenAI's ChatGPT (and its competitors from Google, Microsoft, and AWS) that have elevated chatbot functionality to impressive levels of human-like interaction. The disciplines of data analytics and business intelligence have been moving toward the adoption of natural language processing for many years, but these generative AI breakthroughs have made conversations with data-focused tools a reality. Generative AI algorithms have tremendous potential but are limited in scope by, among other things, the availability of source data upon which their new creations can be based.

How will these developments affect cybersecurity?

One school of thought focuses on how generative AI can dramatically accelerate the development of software. This means that both defenders and attackers may be able to create advanced tools faster, leading to a cyber arms race of sorts. This reasoning is based on one of the most important aspects of generative AI tools—its high accessibility.

Just how often are dramatic technological advancements instantly in the hands of nearly every computer and smartphone user in the world?

This rapid accessibility means rapid adoption by all parties, regardless of their motives. But another school of thought focuses on a contrarian view of the future of AI in cybersecurity that is vastly different from, and far older than, generative AI.

Artificial intelligence is not new to cybersecurity. Machine learning (ML) capabilities, a subset of AI, have been key features within security detection and defense technologies for more than a decade. ML-powered tools already help identify dangerous emails, detect insider threat activities, and identify fraudulent financial transactions in many industries. Tools like these leverage the fact that computer systems are perfectly suited for processing vast quantities of data to find correlations, identify trends, and determine hidden relationships.

These capabilities are very different from generative AI. They are based on the creation of analytic models specific to the problem at hand. For example, a machine learning-powered email scanner is based on a model of the characteristics of good versus evil email messages. It is able to learn from both its own results and "this is a phishing email" inputs from users. These models are the "engine" that can generate increasingly useful answers for practitioners and users. The data fed into the models is the "fuel" that makes the engine run.

What is not being touted very much these days — because it is not nearly as sexy as generative AI — is that data modeling technologies as a whole are also rapidly advancing.

Historically, the greatest challenges to such models have been data availability and quality. But parallel advancements in data mining and management technologies that ingest and help assess the enormous volumes of information on the internet have lowered the bar of entry.

This partially explains the rapid rise of generative AI, which requires large amounts of input data but has had a similarly large impact on industry-specific data modeling technologies.

Predictive and descriptive models that anticipate and capture changes in complex environments are now providing actionable guidance to decision makers in the fields of medicine, environmental science, finance, astrophysics, and most recently, cybersecurity. Tools are now available that leverage high-quality, real-world data within analytic models that calculate optimal strategies in every cybersecurity domain.

Kevin E. Jackson | CEO & Founder of Level 6 Cybersecurity

DATA MINING
Ai
ARTIFICIAL INTELLIGENCE
PROBLEM SOLVING
PATTERN RECOGNITION
MACHINE LEARNING

By modeling cybersecurity strategy in a machine learning environment, both performance and cost optimization can be realized. This aspect of AI is just as revolutionary as advanced chatbots (if not more so) but is distinctly less exciting in news headlines. Statisticians and performance managers are fond of the phrase "What you measure, you can improve." Consider an alternative, AI-focused mantra for the next generation of problem solvers: "What you model, you can optimize."

But what happens when we combine these two aspects of AI? The optimization algorithms described above offer what the generative AI tools need most: useful source data. If we marry the high accessibility of generative AI's natural language interactions with source data from advanced analytic models, we come to a significant new paradigm. The combination of generative AI and predictive/descriptive machine learning models will produce powerful new simulations of complex systems that are immediately and easily accessible to the masses, including the practitioners in specific domains such as cybersecurity.

Imagine, as a corporate cybersecurity manager, having casual conversations with an AI that has already calculated the optimal mix of resources and tools that bring your organization the best security for the cost. And that AI is constantly updating both its analytic model and source data to keep you abreast when technologies, threats, or costs change the optimization results.

This science fiction-like scenario is the future of AI in cybersecurity, but it is a very near future. Months to years away, not decades. And this pattern will repeat itself in many other disciplines as the related modeling and generative AI approaches mature.