Insider Q&A: Artificial intelligence and cybersecurity in military tech

May 29 2023, by Frank Bajak

Josh Lospinoso, CEO and Co-Founder of Shift5, is shown in this April, 2022, photo. Credit: Stephen Voss, Shift5 via AP

Josh Lospinoso's first cybersecurity startup was acquired in 2017 by Raytheon/Forcepoint.. His second, Shift5, works with the U.S. military,

rail operators and airlines including JetBlue. A 2009 West Point grad and Rhodes Scholar, the 36-year-old former Army captain spent more than a decade authoring hacking tools for the National Security Agency and U.S. Cyber Command.

Lospinoso recently told a Senate Armed Services subcommittee how artificial intelligence can help protect military operations. The CEO/programmer discussed the subject with The Associated Press as well how software vulnerabilities in weapons systems are a major threat to the U.S. military. The interview has been edited for clarity and length.

Q: In your testimony, you described two principal threats to AI-enabled technologies: One is theft. That's self-explanatory. The other is data poisoning. Can you explain that?

A: One way to think about data poisoning is as digital disinformation. If adversaries are able to craft the data that AI-enabled technologies see, they can profoundly impact how that technology operates.

Q: Is data poisoning happening?

A: We are not seeing it broadly. But it has occurred. One of the best-known cases happened in 2016. Microsoft released a Twitter chatbot it named Tay that learned from conversations it had online. Malicious users conspired to tweet abusive, offensive language at it. Tay began to generate inflammatory content. Microsoft took it offline.

Q: AI isn't just chatbots. It has long been integral to cybersecurity, right?

A: AI is used in email filters to try to flag and segregate junk mail and phishing lures. Another example is endpoints, like the antivirus program on your laptop—or malware detection software that runs on networks. Of course, offensive hackers also use AI to try defeat those classification

systems. That's called adversarial AI.

Q: Let's talk about military software systems. An alarming 2018 Government Accountability Office report said nearly all newly developed weapons systems had mission critical vulnerabilities. And the Pentagon is thinking about putting AI into such systems? A: There are two issues here. First, we need to adequately secure existing weapons systems. This is a technical debt we have that is going to take a very long time to pay. Then there is a new frontier of securing AI algorithms—novel things that we would install. The GAO report didn't really talk about AI. So forget AI for a second. If these systems just stayed the way that they are, they're still profoundly vulnerable.

We are discussing pushing the envelope and adding AI-enabled capabilities for things like improved maintenance and operational intelligence. All great. But we're building on top of a house of cards. Many systems are decades old, retrofitted with digital technologies. Aircraft, ground vehicles, space assets, submarines. They're now interconnected. We're swapping data in and out. The systems are porous, hard to upgrade, and could be attacked. Once an attacker gains access, it's game over.

Sometimes it's easier to build a new platform than to redesign existing systems' digital components. But there is a role for AI in securing these systems. AI can be used to defend if someone tries to compromise them.

Q: You testified that pausing AI research, as some have urged, would be a bad idea because it would favor China and other competitors. But you also have concerns about the headlong rush to AI products. Why? A: I hate to sound fatalistic, but the so-called "burning-use" case seems to apply. A product rushed to market often catches fire (gets hacked, fails, does unintended damage). And we say, 'Boy, we should have built in security.' I expect the pace of AI development to accelerate, and we

might not pause enough to do this in a secure and responsible way. At least the White House and Congress are discussing these issues.

Q: It seems like a bunch of companies—including in the defense sector—are rushing to announce half-baked AI products. A: Every tech company and many non-tech companies have made almost a jarring pivot toward AI. Economic dislocations are coming. Business models are fundamentally going to change. Dislocations are already happening or are on the horizon—and business leaders are trying to not get caught flat-footed.

Q: What about the use of AI in military decision-making such as targeting? A: I do not, categorically do not, think that artificial intelligence algorithms—the data that we're collecting—are ready for prime time for a lethal weapon system to be making decisions. We are just so far from that.