Converged Cyber AI

A Paradigm Shift in Cybersecurity

leidos

THE ADVANCEMENT OF GENERATIVE AI capabilities presents enormous potential for modernizing government operations but it also introduces new security gaps. While automation allows developers to move from concept to minimum viable product faster than ever, adversaries are developing similar AI-enabled techniques to discover and exploit security vulnerabilities.

To maximize generative AI benefits while minimizing threats, cybersecurity solutions must leverage AI as a first thought, not an afterthought. An AI-centric approach will enhance agencies' abilities to both identify novel attacks and prepare to defend against them. To that end, Leidos is developing innovative converged cyber AI solutions with broad applications across government, from digital modernization to enhancing cyber-physical systems.

Generative AI for government

"The phrase 'transformational technology' is often overused," says Bobby Scharmann, principal investigator for converged cyber AI at Leidos. "But with generative AI, it's really appropriately used — there's broad applicability in virtually every sector of our culture, from music and education and movies to improving the way humans and machines interact with each other."

In the government space, generative AI has the potential to help solve the constant need to do more without an increased budget. Automated processes give human experts more time for deeper analysis and innovation. While fears around being replaced by AI have contributed to an often binary view of AI — that a task is either manual or entirely co-opted by AI — it's more of a spectrum, with augmented decision-making as a sweet spot.

"Every analyst needs ways to help them get through the noise to the important information specifically relevant to them, so that they can make decisions instead of spending 95% of their day sifting through data and searching for what's relevant," says Robert Allen, a research scientist and solutions architect at Leidos.

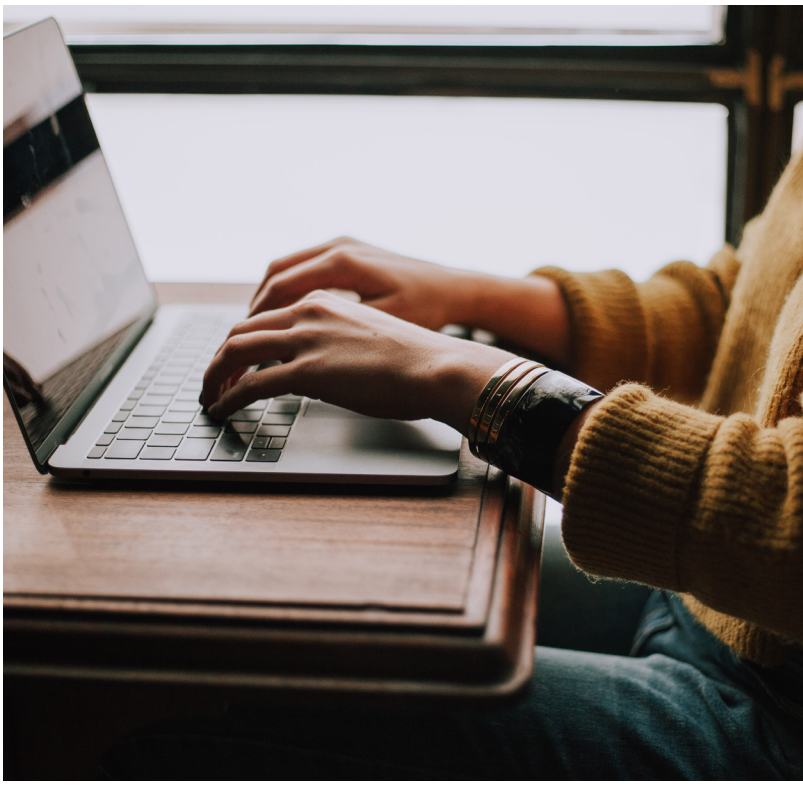
In the software development lifecycle, the augmentative capabilities of generative AI can help developers write new code faster than ever, greatly increasing speed to delivery. However, research has also found that code written with AI assistance tends to be buggier and less secure than traditional methods.

"It's an important consideration that while you're potentially putting out more systems faster, they are inherently less secure in some areas," Scharmann says, "unless you have a security-first mindset throughout the development process."

A cybersecurity paradigm shift

For Leidos, this mindset represents a paradigm shift. Since the cybersecurity field was established decades ago, solutions have largely been increasingly advanced versions of the same rule-based or signature-based methods. Though they've grown more complex and layered over time, there are still gaps that can be exploited, which then must be filled with new heuristic updates.

Generative AI, and its ability to evolve and adapt in ways rule-based methods can't, offers game-changing possibilities, but government leaders are understandably proceeding with caution. Industry partnerships offer reassurance and guidance as agencies move into uncharted territory.



Rule-based firewalls and other protections are familiar and predictable, "but what we need to combat an evolving AI-driven attack is a defense that evolves over time with AI. However, you don't actually have full control over what the AI-enabled defense is," says Meghan Good, senior vice president for technology integration at Leidos. "And that lack of visibility and explainability feels risky. We're helping customers work through that risk."

Given the sensitivity of government data, systems and infrastructure, technology leaders must take care in adopting new technologies. Leidos offers the benefit of innovative proving grounds and testing capabilities to hone new solutions before deployment. The key to developing cutting-edge converged cyber AI solutions is establishing learning environments that focus on: 1) all layers of security — perimeter, network, endpoints — and 2) offensive and defensive perspectives, or purple-teaming.

"Those two perspectives working together is really what strengthens the capability," Allen says. "You might think that you have a good defensive product, but if you're not actually testing that with an evasion capability, then you can't strengthen it. The whole point is to have a system that's learning from its adversary and improving on both sides over time."

This is where AI can help in proactively discovering evasion techniques and vulnerabilities. Then, leveraging the same techniques, you can reinforce a system's defensive posture. Through adopting a first principles approach to AI, breaking it down to its most fundamental interactions and objectives, Leidos is developing dynamic solutions with broad applicability.

"If a given capability is developed for an enterprise IT system, that doesn't mean that the same underlying principles and underlying models are irrelevant in an embedded low-SWaP environment," Scharmann says. "The deployment environments are different, but the underlying fundamentals and characteristics are often very much transferable."

Getting into an attacker's mindset is difficult, especially when they're leveraging their own AI-driven tools and exploits at the same time. AI offers ways to enhance both offense and defense skills beyond human capabilities.

"Leveraging AI/ML techniques allows you to discover novel and innovative approaches that otherwise might be subject to the imagination of the person codifying your more heuristic-based rules," Scharmann says. "It allows you to branch out beyond just their imagination."

Novel solutions for sophisticated threats

Leidos teams are taking a variety of innovative approaches to converged cyber AI solutions with applications across enterprise IT, cyber-physical systems, Internet of Things devices and more.

Among their latest research and solutions:

Generating training data: High-quality data is essential to training AI models in cyber attack detection, but there isn't always enough data available that is representative of a particular attack type. "Our capability allows us to generate synthetic data that is higher quality than existing state-of-the-art methods out there," Scharmann says.

TabMT, recently highlighted in a paper published by the prestigious Conference on Neural Information Processing Systems (NeurIPS), can take a small sample of data and create unlimited additional tabular data. It can also anonymize and later scrub the input data sample while still adhering closely to it, which is particularly beneficial given the high level of sensitivity and confidentiality required for handling government data.

> "The whole point is to have a system that's in effect learning from its adversary and improving on both sides over time."
>
> —
>
> Robert Allen
>
> Research scientist & solutions architect, Leidos

Understanding networks in context: Current enterprise network audits fall short when it comes to contextualizing risks. Leidos' AI-driven network exploration aims to improve such practices by identifying attack paths to key cyber terrain and the exploits attackers may leverage to traverse them, creating invaluable situational awareness. Identifying the easiest exploitation paths to sensitive network segments or resources highlights the greatest risks to the network and essentially creates a map that can be used in the event of a compromise to identify where an attacker might traverse next to access valuable resources.

"It's like going from a list of, 'we have all of these assets in our environment' to 'we fully understand what the relationships are between them right now and the changes that are happening to them over time,'" Good says.

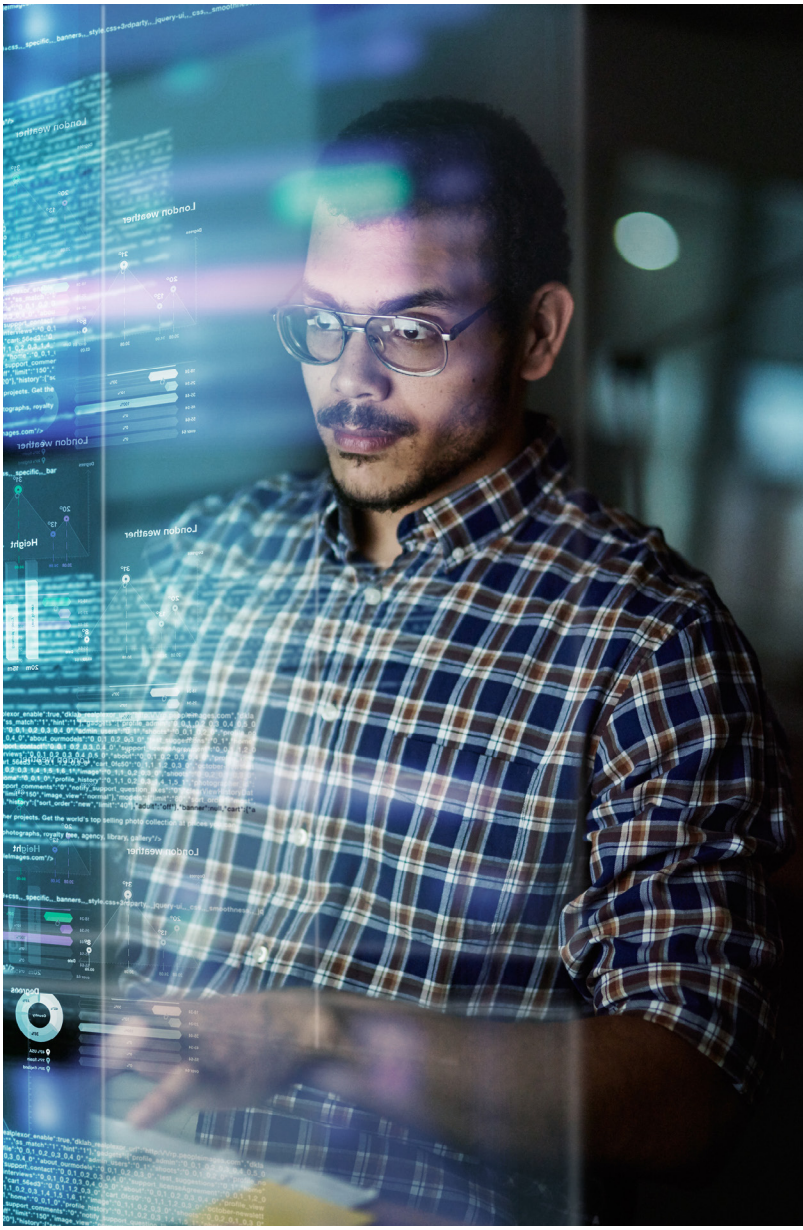
Enhancing existing rule-based systems: Leidos uses AI to discover rule-set gaps and automate defenses against potential attacks. From an offense perspective, it augments human capabilities with thousands of high-confidence, logic-preserving bypass approaches, while from a defensive perspective, it provides automated patching beyond signature-based methods.

"We look at our perimeters differently and take an adversarial, evasive approach through what we currently have deployed, whether that's different layers of firewalls or zero trust network access layers," Good says. "What malicious activity is still making it through from an evasion perspective? And then how do we proactively update our alerting capabilities to better look for these evasive attempts and make sure we're detecting things before they occur in the wild?"

Testing AI solutions in relevant environments: To provide a safe way to do evasion and defensive testing using new products and capabilities, Leidos developed CastleClone, a cyber range solution that enables organizations to create digital twins of their environments and networks. The clones can be used for everything from penetration testing and malware analysis to training employees and new product assessments, all tailored to the organization's unique needs.

CastleClone and digital twins can help ease fears or uncertainties around AI adoption because they offer government leaders a low-risk, custom environment for seeing firsthand how new tools and methods play out.

Building on top of leading commercial AI: To further enhance exploration and development, Leidos also



"We look at our perimeters differently and take an adversarial, evasive approach through what we currently have deployed, whether that's different layers of firewalls or zero trust network access layers."

—

Meghan Good

Senior Vice President, Technology Integration

partners with leading commercial technology providers. Accelerating innovation doesn't mean creating every piece from scratch but rather leveraging the best of existing solutions to create new capabilities. For example, Leidos has teamed up with code intelligence platform Sourcegraph to introduce secure, generative AI-enabled software development tools to government customers.

Good also highlights a partnership with Moveworks, a chatbot solution powered by GPT-class machine learning models with a conversational interface that works across a variety of systems.

"It makes it so you can get to information that was previously in silos," Good says. "A capability like this is able to federate queries and search across and make it so that your data is really actionable."

Keeping pace with evolving threats

As agency leaders continue to explore ways to incorporate generative AI into their cybersecurity solutions, Leidos offers expertise and guidance on how to approach it in a measured and strategic way. While it may be a transformational technology, that transformation doesn't have to happen overnight.

"As part of our trusted AI approach, we start by analyzing and figuring out what we can do to better assist someone, then how we're going to augment them in the future, all before going into more autonomous operations," Good says. "By going through those steps, by using digital twins and proxies, you can understand what the AI is doing and evaluate the risks before deploying it into production."

Cybersecurity will always be a challenge in government, but a commitment to exploring novel technologies and solutions makes that challenge manageable. Staying ahead of adversaries is critical and increasingly complex. Generative AI solutions provide the opportunity to augment capabilities beyond what humans can do alone, enabling faster development and more robust security measures.

"We constantly need to be evolving, because our networks are evolving every day," Good says. "We need a more dynamic way to look at our environments, and that's the capability that we're building."

Learn more about how Leidos can help your agency successfully implement generative AI.