



Booz Allen Charts Autonomous AI Threats and Unveils New Counter AI Defense

Sep 02, 2026

New threat report introduces Cyber Weapon Index and unveils Vellox Labs™ Guile, a Counter AI product for autonomous threats

MCLEAN, Va.--(BUSINESS WIRE)--Sep. 2, 2026-- Booz Allen has released a new report, [The Offensive Frontier: AI as the Attacker](#), based on its **Cyber Weapon Index (CWI)**, which tests the capabilities of rapidly advancing AI models and assesses how those capabilities are actively reshaping the offensive cyber threat landscape.

Booz Allen tested 18 advanced U.S. and Chinese AI models and confirmed that a leading frontier model can now autonomously execute end-to-end intrusion, from gaining initial access to taking full control of a network without human guidance. This finding marks a critical shift from AI-assisted hacking to autonomous cyber operations.

Key takeaways and recommendations from the report include:

- **Sophisticated attacks are becoming more accessible:** As the cost, time, and expertise required to launch advanced cyberattacks collapse, capabilities once limited to nation-states and highly sophisticated actors are becoming available to criminal and non-state actors on demand.
- **Critical infrastructure is exposed now.** The report calls for enforceable, sector-specific deadlines requiring operators to demonstrate readiness against AI-enabled attacks - helping ensure the U.S. and its critical organizations can harness AI faster and more effectively than our adversaries.
- **The model is no longer the unit of risk. The system is.** When paired with attack harnesses, tools, memory, and autonomy that guides its actions, even models short of the frontier can cause significant real-world harm.
- **Counter AI turns autonomy into a liability.** The same autonomy that gives AI attackers an advantage creates vulnerabilities defenders can exploit - disrupting how autonomous systems see, trust, and act to slow attacks and regain critical action time. In Booz Allen testing, coordinated Counter AI playbooks reduced autonomous attacker success by more than 95%.

To help organizations defend against these emerging threats, Booz Allen has introduced [Vellox Labs™ Guile](#), a Counter AI product designed to disrupt autonomous attacks by shaping what AI attackers see and trust, ultimately degrading their ability to successfully execute an attack. As autonomous threats advance, Guile adapts with them, learning from real threats and leveraging the latest frontier AI models to evolve its defenses in real time and safeguard critical assets.

Looking Ahead: Countering the Threat

The rise of AI-powered attacks requires defenders to develop new ways to disrupt autonomous attacks and regain time. Booz Allen takes a unified approach to cyber defense, assessing the autonomous threat through our CWI, defining how defenders can take back control through Counter AI, and putting that approach into action through Vellox Labs™ Guile to protect mission-critical operations.

Read Booz Allen's full report here: [The Offensive Frontier: AI as the Attacker](#)

About Booz Allen Hamilton

Booz Allen is an advanced technology company. We build commercial-grade products and solutions for America's most critical defense, civil, and national security priorities. For more information, visit www.boozallen.com. (NYSE: BAH)

BAHPR-CO

View source version on businesswire.com: <https://www.businesswire.com/news/home/20260902152109/en/>

Media Relations: Ashley Howard, Howard_Ashley@bah.com

Investor Relations: investorrelations@bah.com

Source: Booz Allen Hamilton Holding Corporation