ASP AI Imperative 2030 'Cloud of War' Highlights Need for Defensive AI: Reveals Critical Infrastructure Cyber Threat

AI-powered threats to critical infrastructure demand AI-powered defenses, as monthly downloads of automated cyberweapons catch up to conventional malware.

WASHINGTON, DC, DC, UNITED STATES, October 22, 2025 /EINPresswire.com/ -- The American Security Project (ASP) AI Imperative 2030 initiative today released Cloud of War: The AI Cyber Threat to U.S. Critical Infrastructure, detailing how state-sponsored attackers are deploying AI agents to attack U.S. critical infrastructure and how American infrastructure operators and policymakers must respond by investing in defensive AI. The report finds that downloads of automated cyberweapons are rapidly catching up to shares of all conventional malware, posing an urgent and significant threat to U.S. national security. “AI-powered threats to critical infrastructure must be met with strong AI-powered defenses,” said Courtney Manning, Director of AI Imperative 2030 and lead researcher on the report. “Cloud computing and AI have changed the game forever, and state-sponsored threat actors know it. With thousands of autonomous attack agents freely available to the public and cyber-adversaries like China’s Ministry of State Security paying handsomely for each successful penetration of U.S. infrastructure, it is urgent that Congress and federal agencies accelerate adoption of defensive AI and provide critical resources for CISA and other frontline defenders.”

> “AI-powered threats to critical infrastructure must be met with strong AI-powered defenses. Cloud computing and AI have changed the game forever.”
>
> *Courtney Manning*

The report warns that state-sponsored threat actor motivations are shifting from espionage to destructive cyberattacks on critical infrastructure, increasingly targeting perimeter devices to commandeer sensitive financial, energy, healthcare, and defense networks in the United States. Agentic AI tools capable of operating autonomously once inside a network are already modifying system settings and evading detection in ways that overwhelm traditional defenses. Evaluating over 678,000 python-based packages, the researchers found a sharp rise in downloads of free, open-source offensive digital agents that can be leveraged by cybercriminals to penetrate U.S. networks. Often marketed as tools for developers to test the security of their software and network systems, these agents are increasingly tasked for malicious use.

According to the report, downloads of Python-based automated penetration toolkits totaled more than 21.4 million over the past six months, with monthly downloads increasing nearly 50 percent from March to September 2025 alone. By converting “vibe-coded” commands into executable code deployed through offsite cloud servers, these autonomous agents allow unskilled users to run continuous cyberattacks at scale with minimal risk of detection.

AI Imperative 2030 elevates research, ideas and policies critical to winning the AI competition with China

The report recommends the immediate reauthorization of the Cybersecurity Information Sharing Act of 2015, long-term modernization and reinvestment in CISA, and the establishment of federal incentives for continuous threat monitoring and other best practices among private sector infrastructure operators. While moderate investments can give infrastructure defenders the upper hand, ASP warns that ignoring the emerging threat posed by state-sponsored AI cyber weapons risks putting the United States' infrastructure at risk of critical failure by adversaries already deploying these tools at scale.

Report Link: https://ai.americansecurityproject.org/research/cloud-of-war-chinas-ai-cyber-threat-to-u-s-critical-infrastructure

Tais Davis
ASP AI Imperative 2030
+1 202-347-3115
email us here