ASP | AI IMPERATIVE 2030

SPUTNIK REPORT

CLOUD OF WAR:

The AI Cyber Threat to U.S. Critical Infrastructure

www.AmericanSecurityProject.org

October 2025

Cloud of War:

The AI Cyber Threat to U.S. Critical Infrastructure

Agentic AI cyberweapons are rapidly becoming the tool of choice for state-sponsored attackers targeting U.S. critical infrastructure. By autonomously conducting reconnaissance, modifying system settings, and adapting to new environments, these tools exponentially accelerate the pace of cyber combat. If urgent action is not taken to equip infrastructure operators with strong AI defenses, malign actors will remain free to exploit vulnerabilities in U.S. infrastructure to prey on U.S. citizens, intercept sensitive intelligence, and disrupt vital national functions.

With cloud computing broadening America's attack surface and AI shortening cyberattack lifecycles, U.S. critical infrastructure is increasingly vulnerable to cyber threats. Like federal agencies, private sector infrastructure operators sustain the vital systems underpinning U.S. national security and prosperity. Unlike the public sector, however, these operators are falling far behind in the AI race, creating unprecedented cyber risk for the entire cloud-connected ecosystem. *Cloud of War* examines the role of AI agents in infrastructure defense, finding that cybersecurity defenders are well-positioned to prevail—so long as they act quickly.

The Problem

- **Since 2022, AI-assisted cyberattacks have risen nearly 2,200%.**[1] As U.S. critical infrastructure operators increasingly rely on interconnected cloud and cellular networks, penetrations of cloud networks by state-sponsored hackers and other malign actors have increased by over 130%.[2]
- **Free, open-source, autonomous AI agents are rapidly exposing new vulnerabilities in LLMs, operating systems, and cloud networks.** Over the past six months, total downloads of AI hacking toolkits by both attackers and defenders exceeded 21.4 million, with downloads increasing nearly 50% between April and September 2025 alone.
- **U.S. critical infrastructure relies on outdated and insecure operational software and hardware across multiple sectors.** Operators' low profit potential and overregulation on the state and local level reduces their capacity to adopt necessary AI defenses.

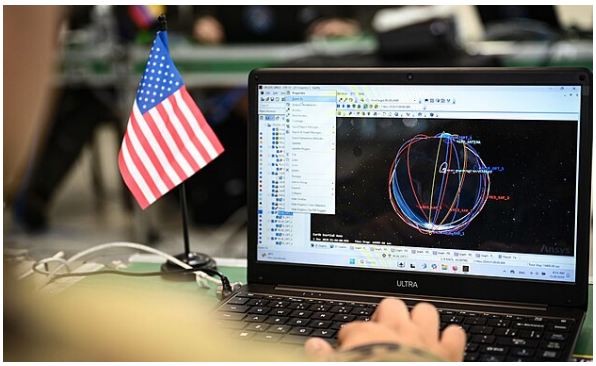
The Solution

- **The United States must restore and strengthen its federal partnerships with private infrastructure operators.** Information-sharing and cyber defense requirements for operators and their enterprise partners must be combined with liability protections for responsible victims of cyberattacks.
- **Continuous threat monitoring and defense in depth are necessary to defend against AI-powered threats.** Infrastructure operators need federal assistance to hire and train AI-aware cybersecurity professionals that can implement and enforce NIST and CISA frameworks up and down critical infrastructure supply chains.
- **Congress must increase funding for public sector and nonprofit applied research on infrastructure cybersecurity solutions**. Open-source alternatives to proprietary operational software are cost-effective but must be thoroughly vetted before adoption.

Introduction

For decades, the global information superhighway was a high-volume firehose of low-value ones and zeroes. With interpersonal communications comprising 90% of global data flows, encryption protected only the most sensitive military, diplomatic, and financial information. Early hackers spent decades chasing needles in the digital haystack, but even state-sponsored cyber criminals opted to physically enter buildings to access targeted systems.

Not anymore.



A National Guard systems operator works through a critical infrastructure cyber scenario. Department of War photo.

As organizations shift more and more operations to the cloud, global data systems don't just carry individual communications; they transmit, and increasingly conduct, the core functions of firms and governments. As America's energy, financial, and healthcare sectors rapidly adopt cloud-based data processing, storage, and system management, critical operations are becoming siloed into programming black boxes, moving out of sight of everyday employees and creating digital vulnerabilities visible only from the back end of cyberspace.

With so many vital security functions now conducted entirely in the digital realm, both the breadth of America's cyber attack surface and the potential impact of a single penetration have magnified exponentially. Adversary nations and other advanced persistent threats (APTs) maintain thousands of cyber experts working around the clock to penetrate U.S. systems. With sophisticated cyber tactics, techniques, and procedures (TTPs) available to anyone with a computer, keys to the nation's power grids, military command systems, and financial markets are bought and sold on dark web marketplaces that are now too entrenched to eliminate.

And just as the U.S. is catching up, artificial intelligence is changing the game again.

AI-powered cyberattack agents enable cyber criminals to execute sophisticated, automated, and personalized attacks at scale. When leveraged against America's outdated and dangerously vulnerable infrastructure systems, these agents are a boon for America's adversaries and competitors. Downloads of free, open-source offensive AI toolkits increased nearly 50 percent over just the last six months, with total downloads exceeding 21 million—rapidly catching up to shares of all written malware online.

With agentic AI algorithms behind the wheel, even the attackers themselves may not know how their own kill switches work or how to stop them.

Preventing persistent cyber threat actors from wreaking havoc on the U.S. homeland requires superior AI-powered defenses spanning America's entire infrastructure ecosystem, not just its public sector. The good news? AI cyberspace is one of the few battlegrounds where—with the right tools and strategies—infrastructure defenders can gain and sustain the upper hand. This report analyzes the scale of the potential AI cyber threat to U.S. critical infrastructure and provides federal-level recommendations to adapt, evolve, and defend against U.S. adversaries in the digital domain.

Critical Infrastructure in Cyberspace

Cloud networks' supermassive economies of scale allow even small, rural infrastructure operators to access large volumes of data and computing power at competitive prices. However, each account, software, and service in a shared network creates additional potential entry points that can be compromised by a persistent threat actor. With artificial intelligence accelerating the pace of cyber offense and defense, weak links in critical infrastructure systems have become exceptionally valuable targets.

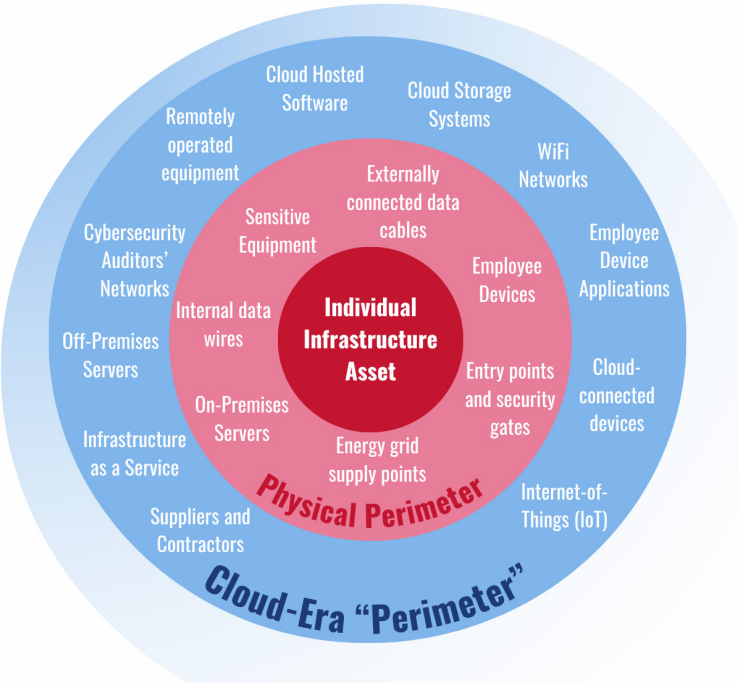
The Cloud: Exponentially Increasing America's Attack Surface

Critical infrastructure provides the functions that are so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on American security, economy, or public health and safety.[3]

For the private sector organizations that build and operate this infrastructure, defending them once required installing fences, walls, locks, and guards around a physical perimeter. As operations gradually moved online, this perimeter mindset led to the development of firewalls, VPNs, and other digital moats aimed at deterring initial cyber penetrations.

Enter cloud computing. While cloud products and services made infrastructure operators more connected, efficient, and streamlined than before, each new addition increased the endpoints and perimeter devices connected to sensitive networks. Today, U.S. critical infrastructure data and operations are split across on-premises servers, public cloud platforms, and third-party supplier ecosystems. This decentralization has drastically expanded not only the number of potential entry points for cyber intrusions, but also the potential repercussions of each penetration as vulnerabilities cascade across cloud-connected supply chains.[4]

U.S. Infrastructure Points of Attack



Initial Access Vectors and Zero-Day Vulnerabilities

Financial motivations drove 90% of all cyberattack attempts in 2024.[5] By contrast, state-sponsored attackers are motivated by espionage 74% of the time—and in 26% of cases, they aim to penetrate and commandeer infrastructure.[6]

To access these systems, hackers utilize three entry methods at roughly similar rates: acquiring or brute-forcing user credentials, exploiting perimeter vulnerabilities, and mass-proliferating phishing emails or other low-skilled spam. Over half of enterprise security breaches involve human error, from accountants downloading suspicious files to administrators misconfiguring network permissions.[7] Manipulating users into granting access to systems or data is called "social engineering," and employees that improperly grant access are termed "insider threats." Weekly cyberattacks on U.S. systems have increased 56% year-over-year, with utilities facing 234% more cyberattacks in 2024 than in 2025.[8]

Case Study #1: 2024 Treasury Department Hacks

China's Ministry of Public Security (MPS) and Ministry of State Security (MSS) fund an extensive network of private firms, contractors, and criminal organizations to hack U.S. data and computing systems. In some cases, the MPS and MSS pay hackers to target specific victims in the United States. In others, hackers target victims and systems speculatively, receiving a generous payout upon each successful intrusion.

In 2024, CISA confirmed that an unidentified threat actor compromised the U.S. Treasury Department's Azure cloud network.[9] After successfully authenticating to an internal virtual private network (VPN) access point using a username and password found in an enterprise data breach, the attacker entered the on-premises network and moved laterally across implicitly trusted connections to the Azure cloud. According to CISA, the incident "fit a well-documented pattern of operations by PRC-linked groups, with a particular focus on abusing trusted third-party services - a method that has become increasingly prominent in recent years."[10]

In March 2025, the Department of Justice charged 12 Chinese state-sponsored contract hackers for the Treasury attacks and others going back to 2013.[11] As of September, however, the defendants remain at large.

The Race to the Perimeter

Once inside, state-sponsored actors and other cyber adversaries can lock up an operator's data for ransom, overwhelm a system with requests until it fails, and exploit "zero-day vulnerabilities," or previously unknown flaws in network architectures, to lurk and laterally move inside connected systems for as long as possible.[12] Zero-days are sold on digital marketplaces for upwards of $20 million,[13] including to firms and governments who purchase these vulnerabilities in order to patch them.[14]

In the past, nearly all security breaches originated in employees' cell phones and browsers. Today, ongoing improvements in threat detection and mitigation by user platform providers mean a majority of successful hackers now exploit perimeter devices and services.[15] This trend poses a novel and alarming threat to U.S. critical infrastructure, as security and networking vulnerabilities allow attackers to compromise and disrupt vital operations in addition to accessing sensitive information and data systems.

Cloud Sprawl and The Rise of Supply Chain Attacks

To defend vital systems, critical infrastructure operators must deploy a wide range of internal and external cybersecurity experts, software, and procedures. Under current best practices, cyberspace is one of the few battlegrounds where defenders can gain a structural advantage over attackers.[16] However, if leveraged improperly, these efforts can create a perimeter paradox: as more security layers are added to a system, each introduces additional potential entry points an attacker can exploit.

For critical infrastructure organizations, the perimeter security paradox—combined with the requirement for duplicative data systems in the case of primary system disruption—can easily create "cloud sprawl": a high-risk environment where defenders lose visibility of their assets across multiple data systems and are exposed to vulnerabilities from connected but unobservable systems. These risks are magnified when third-party cloud-hosted services and infrastructure providers host tens or hundreds of organizations on the same network; according to Verizon, nearly 30% of breaches in 2024 originated in external partner networks, a sharp rise from 15% just one year prior and 8% in 2022.[17]

AI Cyber Offense: A Revolution with No Rollback

With cloud computing exponentially expanding potential entry points to U.S. critical systems, artificial intelligence made it easier than ever to conduct simultaneous identity attacks on the front end and sophisticated zero-days on the back end. Since 2022, AI tools have increased cyber-attacks on cloud systems more than 2,200% year-over-year.[18] ASP research finds that public interest in these tools is rapidly catching up to that of conventionally written and shared malware.

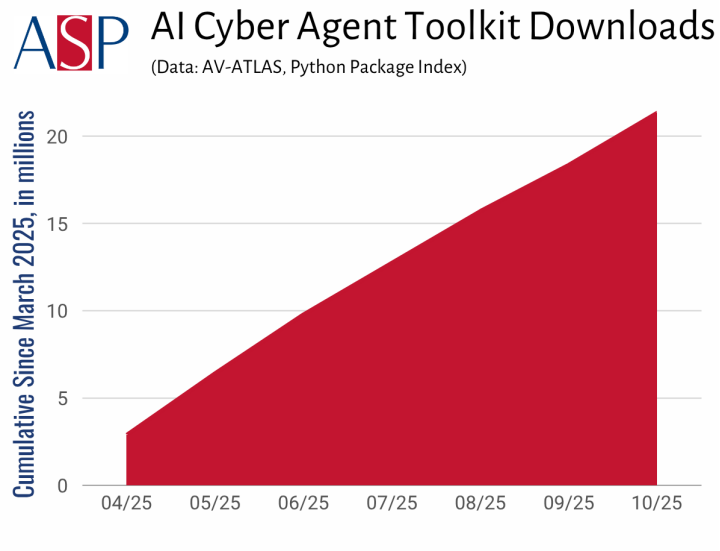
The Explosion of Generative AI Attacks

Generative AI can create highly convincing phishing and other social engineering campaigns in over 35 languages. Despite the average cost of insider threats exceeding $15.4 million per organization,[19] nearly 80% of Americans claim to be "very confident" in their ability to protect their personal information.[20] This false sense of security creates risk even within a centralized, secure perimeter; in a post-cloud environment, thousands of critical infrastructure systems are now only as safe as their weakest link.

Of all the actors leveraging artificial intelligence for cyber harms, the People's Republic of China (PRC) is by far the most prolific and sophisticated. Chinese state-sponsored hacking groups like APT41 and APT31 use large language models like DeepSeek to rapidly develop convincing emails, texts, and phone calls, using voice and video algorithms to impersonate targets ranging from high-profile leaders like U.S. Secretary of State Marco Rubio and House Representative John Moolenaar to low-level employees with access to internal databases and networks.[21] These groups then use AI-accelerated networking and 5G infrastructure to simultaneously blast these scams to millions of user devices at maximum energy and compute efficiency.

The Impending Threat: Agentic AI Agents

However, what comes next is even more dangerous. Agentic AI algorithms autonomously modify system settings, conduct system reconnaissance, and invent new defense evasion activities without the permission—or even the oversight—of the attacker. "AI penetration toolkits" are sold on dark web marketplaces and shared on online software repositories like the Python Package Index, often with step-by-step instructions on how to install and run them. While deploying AI malware requires far more computing power and energy than conventional malware, cloud-hosted compute services like AWS Lambdas allow attackers to anonymously run these toolkits without provisioning servers,[24] further reducing the resources and skills needed for sophisticated cyberattacks.[25]

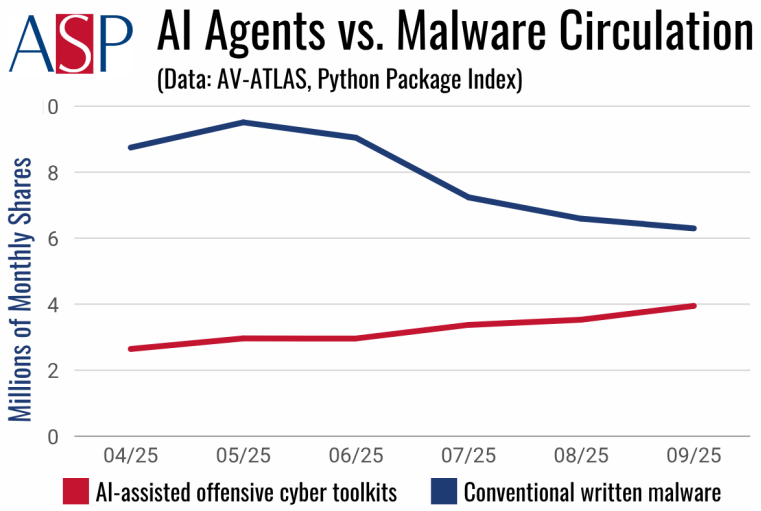


While AI-assisted malware agents are often legally sold as tools to help organizations defend against novel cyber intrusions,[26] it is estimated that 80% of ransomware attacks in 2024 resulted from these tools.[27] One tool, Villager—a model that uses Chinese AI model DeepSeek to translate simple user requests into attack sequences that are then automatically executed[28]—has been downloaded more than 17,000 times since July 2025. In August, Anthropic reported that a cybercriminal had used an agentic AI to target at least 17 organizations in healthcare, emergency services, and other critical infrastructure sectors.[29]

New Findings: AI Agents Are Rapidly Dominating Cyber Operations

An API query of open-source Python repository PyPI finds that total downloads of AI-assisted offensive cyber software exceeded 21.4 million from March to September 2025.[30] These toolkits are often legitimately used by cybersecurity experts to probe for novel vulnerabilities and stress-test software they are tasked with defending. However, a rising number of packages—several hundred as of September 22nd—openly advertise that they can be executed against systems not owned by the downloader to cause real-world harms. These AI malware executables have been downloaded more than 12 million times in the past six months.

While preliminary, these findings are startling—particularly considering this analysis did not include AI penetration agents from other open-source repositories like GitHub or private malware-sharing communities on apps like Discord, Telegram, or Signal. According to industry insiders, these platforms produce an estimated 60% of all offensive AI cyber agents. As a result, these findings are a highly conservative estimate of the rising popularity of AI malware agents compared to traditional malware shared online, with autonomous malware executables likely exceeding 20 million or more downloads over the past six months.



In a stark contrast to the overall decline in traditional malware sharing, the popularity of agentic cyber penetration agents is increasing exponentially. From April to September 2025, monthly downloads of open-source AI-assisted offensive cyber suites rose from 2.6 million to 3.9 million, a 49.3% increase in just six months. According to AV Atlas, a threat intelligence firm that monitors malware shared online, monthly shares of written malware declined from 11 million in March to 6.5 million in August 2025. Consequently, the ratio of offensive AI cyber agent downloads to written malware files shared online increased from .25 to .54 in the six months from March to September, demonstrating that downloads of offensive AI cyber agents may be supplementing or even partially replacing traditional malware sharing mechanisms.

Project description

Pytorch-based executable with over 40 Adversarial EXEmples. AI agent evades Windows Malware detectors.

"Oh, you think darkness is your ally. But you merely adopted the dark; I was born in it, molded by it. I didn't see the light until I was already a man, by then it was nothing to me but BLINDING! The shadows betray you, because they belong to me!" -Bane (Dark Knight)

Examples of project descriptions and disclaimers common to AI-assisted malware and penetration testing toolkits

Features

- Automated Nmap Scanning: Performs detailed scans using Nmap scripts to identify vulnerabilities.
- Exploit Searching: Searches Metasploit for available exploits based on the scan results.
- Automated Exploitation: Attempts to exploit identified vulnerabilities with Metasploit.
- Session Management: Opens, interacts with, and closes sessions automatically.
- Logging and Reporting: Generates detailed logs and reports in Markdown and CSV formats.
- Interactive Console: Provides an interactive console with rich text output for user interactions.

Collection of offensive tools targeting Microsoft Azure networks written in Python packaged with a flexible AI executable. The current list of tools can be found below:

- `./Device_Code/device_code_easy_mode.py`
  - Generates a code to be entered by the target user
  - Can be used for general token generation or during a phishing/social engineering campaign.

Disclaimer

This tool is intended for educational purposes only. Unauthorized use of this tool is prohibited. Always obtain proper authorization before performing any penetration tests or scans on systems.

State-of-the-art AI agent covertly deploys a range of malicious workflows into compromised devices. Please keep in mind that you can mess up and get caught if you don't know what you're doing.

The Imperative for U.S. Infrastructure AI Cyber Defense

As generative AI models like DeepSeek are integrated into offensive agentic tools that conduct attacks at inhuman speed, equally or more capable AI defenses must be rapidly integrated into U.S. critical infrastructure systems. Continuous threat monitoring is no longer a recommendation for critical infrastructure operators; it's a national security imperative.

Improving Defensive Capabilities at Scale

Cybersecurity defenders have long been at the mercy of attackers in cloud-connected cyberspace. While agentic AI tools can be leveraged by attackers and defenders equally, critical infrastructure operators have a singular advantage over their assailants: vastly superior energy and computing power, which can support far more sophisticated and comprehensive threat monitoring. Given the supermassive economies of scale of America's power grids, data centers, and other infrastructure networks, AI-powered cyber defense suites are more cost-effective than traditional monitoring and incident response—and several magnitudes faster. IMB research finds that AI-assisted cyber defenses reduce data breach lifecycles by 80 days on average and save organizations approximately $1.9 million per breach in data loss mitigation, operational downtime, regulatory fines, and other costs.[31]

Case Study #2: T-Mobile and the Fight Against Salt Typhoon

In Spring 2024, it was discovered that China's Ministry of State Security (MSS) had gained access to Washington's most sensitive telecommunications systems, including the phone networks of then-former U.S. President Donald Trump and future Vice President J.D. Vance. Exploiting weak passwords, unpatched bugs, and federal wiretap entry points, MSS-affiliated attackers Salt Typhoon compromised the networks of over 80 U.S. telecom providers, including AT&T, Verizon, and Lumen, and transferred large volumes of American metadata and communications to Beijing.[32] The attack was so sophisticated that the U.S. government was unable to attribute the hacks until nearly a year later.[33]

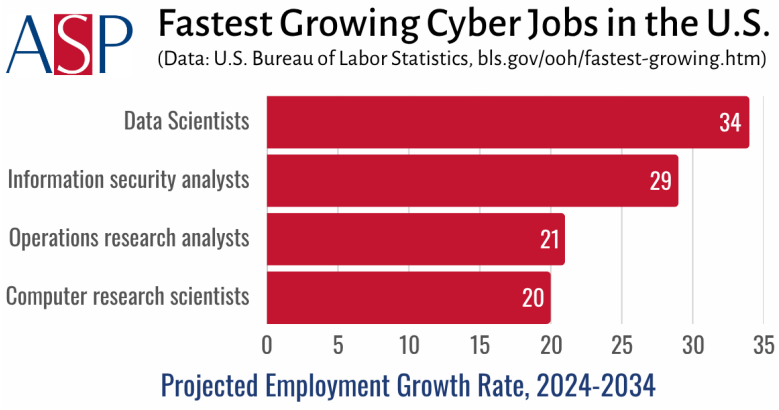
However, while Version and AT&T took months to evict Salt Typhoon from their systems, one firm stood out from the rest: T-Mobile. Around the same time that other telecoms giants experienced their first breaches from Salt Typhoon, the carrier's network engineers identified and prevented similar unauthorized users from penetrating systems storing customer data. Because the attackers were identified at T-Mobile's network gateway, the firm was the first to present a profile of these attackers to federal agencies and other telecommunications firms. This decision provided unprecedented transparency into the likely modus operandi for Salt Typhoon.

A unique combination of security features allowed T-Mobile to succeed where others failed. First, multi-layer architecture ensured that their "edge infrastructure"—the points connecting T-Mobile networks to those of other telecoms firms—was fully isolated from routers storing sensitive customer data.[34] Second, as the firm operates exclusively within the United States on its own 5G network, attackers couldn't exploit common cyber vulnerabilities found in older, remote, or poorly maintained infrastructure. Finally, T-Mobile recently made significant investments in advanced cyber protections, including FIDO2 multifactor authentication and logging protocols. The result was a data protection ecosystem that stood up against the most aggressive state-sponsored telecom breach in U.S. history.

Unfortunately, sector-wide limitations have led critical infrastructure operators to be slow to adopt these tools, posing enormous risks to U.S. national security in the AI era. Some of these limits are structural; for example, operational technology systems, which control equipment spanning from hospitals and power grids to train switches and oil pipelines, often contain proprietary code that is unable to be modernized without taking critical systems offline.[35] One software suite with several persistent and unpatched vulnerabilities, ICONICS SCADA, is embedded in over 70% of Global 500 companies.[36] Other limitations are regulatory; federal oversight investigations have found that overlapping regulations and conflicting parameters in infrastructure sector cybersecurity requirements greatly increase time and labor spent in compliance and approvals processes, reduce available resources for cyber defense operations, and deter operators from initiating complex but necessary software improvements.[37]

Empowering Human Agents

The speed and unpredictability of AI attack agents are rapidly reducing the ability of infrastructure operators to rely on human oversight alone. As these agents improve in scale and sophistication, human expertise and response capacity in cyberspace must be supplemented with continuous AI monitoring both at the perimeter and in the internal networks of critical infrastructure systems.



While some analysts posit that this shift will lead to human cyber experts being "replaced by AI," leading research suggests the opposite: amidst a shortfall of over 660,000 cybersecurity experts in the United States,[38] continuous threat monitoring and other AI tools are making careers in cybersecurity more feasible and lucrative for entry- to mid-career workers.[39] In addition to empowering more individuals to meet labor market demands,[40] job postings are rising for specialists who can train and fine-tune defensive AI systems to adapt to new threats.[41] This AI labor specialization will open additional cybersecurity positions at more advanced levels while strengthening the nation's overall capacity to remediate vulnerabilities in critical infrastructure.

Accelerating Vulnerability Mitigation

The rapid adoption of AI in cyberspace by both attackers and defenders has significantly accelerated the pace of cyber conflict, making continuous monitoring and layered defense a necessity even for operators with strong but conventional cybersecurity capacities. As continuous threat monitoring agents more rapidly expose and eject lurkers from sensitive systems, the average "dwell time" between an attacker entering a system and being detected by a defender has reduced from 16 days in 2023 to just 10 in 2024.[42] Improved detection has accelerated the pace at which cyber criminals must exploit novel vulnerabilities after discovery; penetration-to-attack timelines condensed from 32 days in 2022 to just five days in 2025.[43]

Today, cyber offenders exploit gaps faster than human defenders can write code to patch them. As a result, successful exploitation of zero-day vulnerabilities increased 34% over the last year.[44] However, this figure fails to tell the whole story. With open-source cyber defense toolkits like NVIDIA's NeMo Agent exposing vulnerabilities more efficiently than the majority of offensive agents,[45] organizations can easily detect and disrupt the majority of penetrations—as long as they are aware of the threat and available solutions. Federal mechanisms like the Cybersecurity and Infrastructure Security Agency's Stakeholder Engagement Division and National Risk Management Center are critical for furthering infrastructure operator awareness and adoption of these tools.

Ameliorating Emerging Open Source and AI-Assisted Software Risks

According to Alexei Bulazel, top cyber official at the National Security Council, "the technology that's deployed in critical infrastructure contexts… is not the best-in-class software or hardware."[46] However, while critical infrastructure operational software is often vulnerable and in need of replacement, between 70 to 90 percent of modern solutions rely on open-source code[47]—and as of 2025, between 50 and 60 percent of this code is AI-generated.[48]

Broad adoption of AI-generated code by third party suppliers and internal employees poses new risks to critical infrastructure security. According to Stack Overflow, while 81 percent of surveyed developers "use or plan to use" generative AI to write code, only 32 percent trust AI outputs.[49] This mistrust is justified; analysis by auditor BaxBench finds that half of all working code generated by leading AI models contains critical security vulnerabilities.[50]

As AI-generated code neproliferates across the open-source landscape, agentic AI systems help infrastructure operators scan software for embedded vulnerabilties, mitigate security risks, and maintain comprehensive inventories of connected devices and networks. When combined with System of Trust and NIST Cybersecurity Framework standards, these tools dramatically improve network security—the most adagentic agents align with cybersecurity expert decisionmaking 98% of the time.[51] AI agents can also be combined with generative AI models to reduce hallucinations by over 2700% in the coding process.[52] However, careful consideration must be made that these powerful tools are not hijacked by adversaries; too-broad security permissions combined with limited human oversight can result in catastrophic, system-wide effects if an agent becomes misaligned.

Case Study #3: The Cascading Effects of Volt Typhoon

U.S. critical infrastructure isn't just at risk; it's actively under attack. In February 2024, twelve international government agencies warned of persistent intrusions into America's most sensitive government and infrastructure systems.[53] For at least five years, multiple organizations were compromised across the communications, energy, water, defense, and transportation sectors, and not just to access sensitive data. Investigators concluded "with high confidence" that the attacks enabled lateral access to operational technology systems, granting attackers the ability to disrupt critical operations—in the United States, but also in Canada, Australia, and New Zealand.

The interconnectivity of allied cloud infrastructure would allow this sufficiently sophisticated attacker to disable the infrastructure of nations comprising over a third of the world's GDP with one keystroke. The attackers, code-named Volt Typhoon, were "living off the land"—using network administration tools to obscure unusual activity and limit suspicion of their activities.

According to then-FBI director Christopher Wray, Volt Typhoon is "the defining threat of our generation." In March 2025, lawmakers launched an oversight investigation into the perceived lackluster response by the federal government following the attacks, requesting additional transparency into the federal government's cyber mitigation strategy.[54]

Policy Recommendations

As organizations shift more and more operations to the cloud, global data systems don't just carry individual communications; they transmit, and increasingly conduct, the core functions of firms and governments. Urgent action is needed for policymakers and infrastructure operators to catch up to the AI age.

To Ensure America's Critical Infrastructure is Defended Against AI-Powered Threats:

Congress must urgently reauthorize the Cybersecurity Information Sharing Act (CISA 2015), which expired in September.[55] In 2022, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act, which tasked the Cybersecurity & Information Security Agency (CISA) with designing new regulations to faciliate information sharing between critical infrastructure operators and the federal government.[56] However, these regulations will not go into effect until at least May 2026. In the meantime, CISA 2015 provided critical information-sharing networks that protected operators from state-sponsored attacks and offered liability protections that empowered the private sector to share vital cybersecurity information with the federal government.

Appropriate additional funding and establish a permanent, dedicated funding stream for CISA.[57] America's infrastructure oeprators rely on CISA to modernize their information and operations systems and defend against cyberattacks. Particularly useful is CISA's Joint Cyber Defense Collaborative (JCDC), whose budget was recently cut by $10 million.[58] Rep. Eric Swalwell aims to codify JCDC into law,[59] but each of CISA's other vital programs must be individually justified and restored by Congress.

Treat U.S. Cloud Infrastructure as Critical Infrastructure. In addition to supplying the foundation for global AI leadership, cloud networks provide the backbone of global trade, communication, and military cooperation between the U.S. and its allies. The U.S. currently entrusts oversight and defense of these networks to the private sector, creating national security risks as these networks are connected to America's most sensitive government and military operations. To begin reducing the hundreds of millions of cyberattacks on cloud networks daily, the United States must treat cloud infrastructure as critical infrastructure and afford it the same oversight and protection mechanisms as America's energy, healthcare, and transportation networks.

Incentivise software-as-a-service solutions for infrastructure systems' stored data—but prioritize secure, self-hosted solutions for critical operations. Network segmentation and defense in depth approaches prevent penetrations of a cloud environment from spreading to systems responsible for critical functions. Attackers seeking data for either profit or espionage should not be able to accidentally stumble into parts of the network that allow for disruption and even destruction of these operations. Non-critical, third-party services should be limited at all costs, including automatic add-ons to contracted services.

About the Author

Courtney Manning is the Director of AI Imperative 2030 at the American Security Project, where she leads a team of cross-disciplinary stakeholders investigating the critical geostrategic forces driving the global AI race in the 21st century. Formerly, she led ASP's research portfolios on military recruitment and readiness, strategic competition with China, and emerging technology risks. Before ASP, she worked as a geopolitical risk consultant for the Peruvian government and a special advisor for the Permanent Mission of Afghanistan to the United Nations. Courtney holds an MIA in international security policy and conflict resolution from Columbia University and a BA in international relations from the University of Denver Korbel School.

Endnotes

1 https://www.signicat.com/the-battle-against-ai-driven-identity-fraud; https://www.securitymagazine.com/articles/100067-report-shows-1265-increase-in-phishing-emails-since-chatgpt-launched

2 https://ir.crowdstrike.com/news-releases/news-release-details/2024-crowdstrike-global-threat-report-breakout-breach-under/;

3 https://www.cisa.gov/national-critical-functions-set

4 Duszynski, Jimmy (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023, 2(1), 129–171. https://doi.org/10.60087/jaigs.v2i1.102

5 https://www.verizon.com/business/resources/T163/reports/2025-dbir-data-breach-investigations-report.pdf

6 https://www.verizon.com/business/resources/T163/reports/2025-dbir-data-breach-investigations-report.pdf

7 https://www.verizon.com/business/resources/reports/dbir/

8 https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

9

10

11

12 https://www.securityweek.com/chinas-volt-typhoon-hackers-dwelled-in-us-electric-grid-for-300-days/

13 https://techcrunch.com/2025/08/20/new-zero-day-startup-offers-20-million-for-tools-that-can-hack-any-smartphone/

14 https://www.crowdfense.com/exploit-acquisition-program/

15 https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends

16 https://www.sciencedirect.com/science/article/pii/S2543925123000372

17 https://industrialcyber.co/features/rising-threats-push-industrial-supply-chains-to-adopt-real-time-monitoring-proactive-cybersecurity-practices/

18 Data from U.S. CISA

19 https://cybermagazine.com/top10/top-10-biggest-cyber-threats

20 https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/

21 https://www.securityweek.com/details-emerge-on-chinese-hacking-operation-impersonating-us-lawmaker/

22 GenAI to create ransomware

23 https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global

24 https://codestax.medium.com/how-hackers-are-turning-aws-lambda-into-stealthy-command-control-server-5d7a0ae534a9

25 https://unit42.paloaltonetworks.com/windows-backdoor-for-novel-c2-communication/
26 https://pypi.org/
27 https://cams.mit.edu/wp-content/uploads/Safe-CAMS-MIT-Article-Final-4-7-2025-Working-Paper.pdf

28 https://www.infosecurity-magazine.com/news/chinese-ai-villager-pen-testing/
29 https://www.anthropic.com/news/detecting-countering-misuse-aug-2025
30

31 https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry

32 https://www.nextgov.com/cybersecurity/2024/12/hundreds-organizations-were-notified-potential-salt-typhoon-compromise/401843/?oref=ng-homepage-river;
33 https://home.treasury.gov/news/press-releases/jy2792
34 https://www.cybersecuritydive.com/news/att-verizon-salt-typhoon/736680/
35 https://www.appgate.com/blog/the-rising-threat-to-ot-environments-in-manufacturing-and-critical-infrastructure-and-how-to-defend-them

36 https://cyberscoop.com/iconics-scada-vulnerabilities-2025-palo-alto/

37 https://www.gao.gov/assets/gao-24-107602.pdf; https://homeland.house.gov/2025/04/08/house-homeland-oversight-republicans-urge-omb-to-cut-burdensome-duplicative-cyber-regulations/; https://web.archive.org/web/20240829125901/https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf, page 19.

38 https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study
39 https://al-kindipublishers.org/index.php/jcsts/article/view/10366/9084

40 https://www.gartner.com/en/newsroom/press-releases/2024-03-18-gartner-unveils-top-eight-cybersecurity-predictions-for-2024

41 Unfortunately, as the available labor force for cybersecurity technicians in the united states is short by about 750,000 workers, the labor gap for trained AI technicians is likely going to be the biggest hurdle to this transition. See https://www.afcea.org/signal-media/cyber-edge/cyber-workforce-shortage-myth
42 https://services.google.com/fh/files/misc/m-trends-2024.pdf
43 https://www.linkedin.com/posts/matthewlye_this-has-been-coming-for-years-but-we-have-activity-7377080989099094017-5nVH/; https://services.google.com/fh/files/misc/m-trends-2024.pdf
44 2025 Verizon Data Breach Investigations Report
45 https://developer.nvidia.com/nemo-agent-toolkit
https://arxiv.org/abs/2501.13946

46 https://cyberscoop.com/alexei-bulazel-critical-infrastructure-security-tech-needs-to-be-as-good-as-our-smartphones/

47 https://www.linuxfoundation.org/blog/blog/a-summary-of-census-ii-open-source-software-application-libraries-the-world-depends-on

48 https://www.wearetenet.com/blog/github-copilot-usage-data-statistics

49 https://survey.stackoverflow.co/2025/ai

50 https://baxbench.com/

51 https://www.crowdstrike.com/en-us/blog/agentic-ai-innovation-in-cybersecurity-charlotte-ai-detection-triage/

52

53 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a?utm_source=EA&utm_medium=press_release&utm_campaign=VT_020724

54 https://homeland.house.gov/wp-content/uploads/2025/03/2025-03-17-Green-Garbarino-Brecheen-to-Noem-DHS-re-Volt-and-Salt-Typhoon.pdf

55 https://www.wilmerhale.com/en/insights/client-alerts/20250912-critical-national-security-law-cisa-2015-set-to-expire-at-the-end-of-the-month, https://cyberscoop.com/cisa-2015-expiration-industry-warning-threat-information-sharing/

56 https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

57 https://oversight.house.gov/hearing/salt-typhoon-securing-americas-telecommunications-from-state-sponsored-cyber-attacks/

58 https://www.cisa.gov/news-events/news/securing-core-cloud-identity-infrastructure-addressing-advanced-threats-through-public-private

59 https://www.vitallaw.com/news/bill-to-revamp-cisa-s-cyber-collaborative-clears-committee/cspd01139b4f3b914a401fba3d0e77713df3f4?refURL=https%3A%2F%2Fwww.theregister.com%2F#.

"2024 CrowdStrike Global Threat Report: Cloud Infrastructure Under Attack," CrowdStrike, February 21, 2024, https://www.crowdstrike.com/en-us/press-releases/2024-crowdstrike-global-threat-report-release/