ARMIS FEDERAL

THE STATE OF

CYBERWARFARE

THE 2026 U.S. FEDERAL ISSUE

FEDERAL IT UNDER ATTACK: AGENCIES CONFRONT ESCALATING CYBER CONFLICT

EXECUTIVE SUMMARY

Cyberwarfare has moved from a strategic concern to an operational reality for U.S. Federal agencies. And with the rising geopolitical tension, Federal IT decision-makers are reporting an increase in cyberwarfare threats, AI-accelerated attacks, and modernization efforts slowed by escalating cyber risk.

The most striking finding is a widening preparedness gap. **While most federal leaders express confidence in their cyber readiness, a majority also report prior breaches and unresolved exposure across their environments.**

At the same time, AI-powered attacks are now viewed as the most significant cybersecurity threat facing agencies today, and emerging technologies such as quantum computing are intensifying long-term risk calculations.

The message is clear: federal cybersecurity must evolve from reactive defense to proactive, continuous exposure management across the full attack surface.

The Preparedness Gap: Confidence vs. Compromise

THE DATA

81% believe their agency is prepared to handle a cyberwarfare attack.

57% say their agency has been hacked previously and has not adequately secured its ecosystem.

60% say their organization's average ransomware payout exceeds its annual cybersecurity budget.

WHAT THIS MEANS

Federal agencies demonstrate confidence in their cyber posture. However, more than half acknowledge that their environments remain insufficiently secured. This signals a troubling gap between policy and execution.

Preparedness in federal environments is often measured in frameworks, compliance benchmarks, and strategic plans. If adversaries know your technology better than you do, even the best laid strategies fall flat. When response and recovery costs exceed annual cybersecurity investment, agencies are effectively funding consequences rather than prevention.

Global Cyberwarfare Is an Imminent Operational Threat

THE DATA

93% are concerned about cyberwarfare's impact on their agency.

57% say the threat is imminent and have reported an act of cyberwarfare.

81% believe geopolitical tensions have accelerated the expanding attack surface.

Top perceived threat actors:

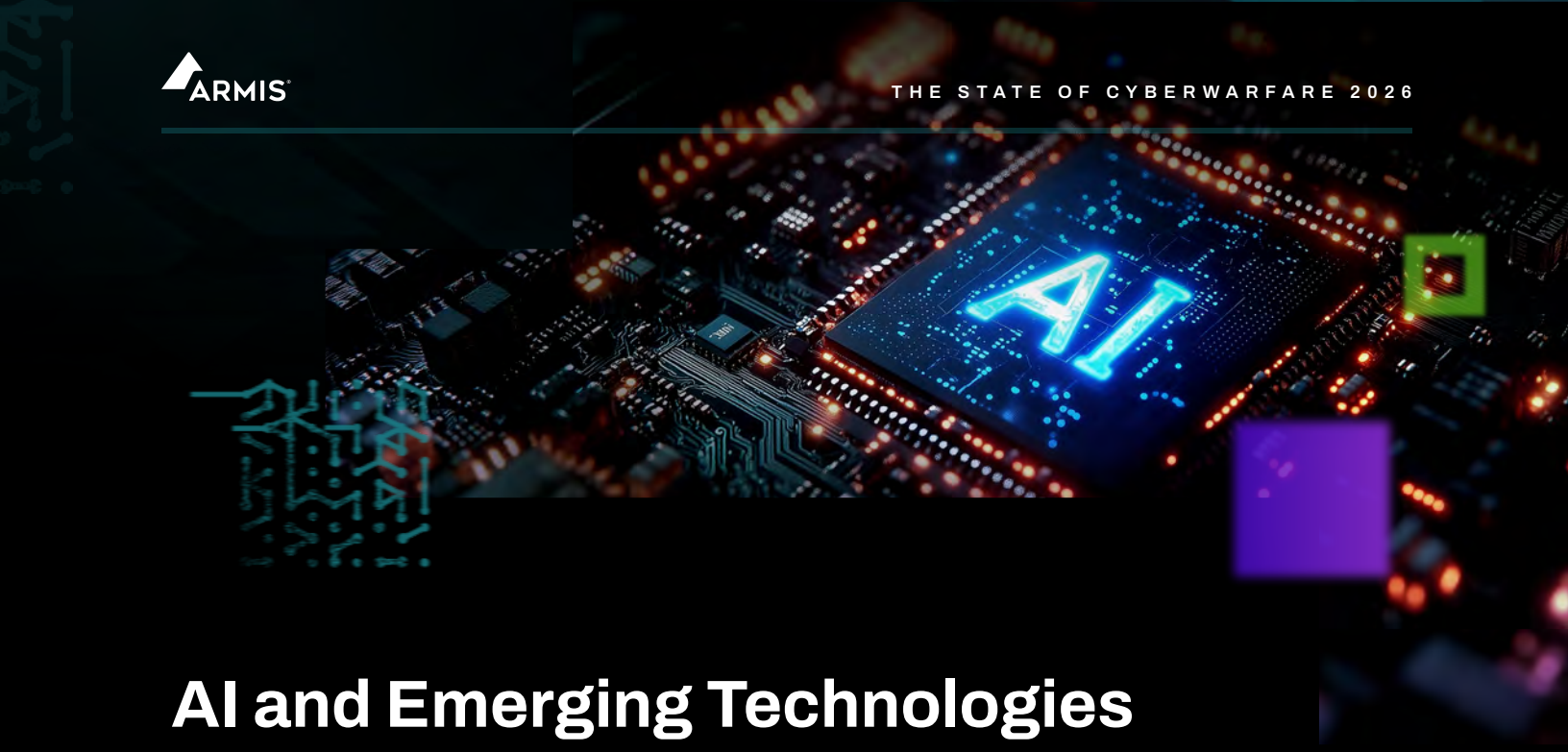
- **China 72%**
- **Russia 58%**
- **North Korea 50%**
- **Iran 23%**
- **Pakistan 11%**

WHAT THIS MEANS

Federal agencies are no longer preparing for a potential cyber conflict. They are operating within one that is ongoing and global.

Geopolitical instability is amplifying digital confrontation. As tensions rise globally, the federal networks that underpin national security, critical infrastructure, public services, and economic stability become strategic targets.

This environment requires a posture built on continuous monitoring and integrated intelligence. Agencies must assume persistent targeting and architect resilience accordingly.



AI and Emerging Technologies Are Escalating the Threat

THE DATA

58% have been impacted by an AI-generated or AI-led attack in the past 12 months.

58% identify AI-powered attacks as the biggest cybersecurity threat facing their agency.

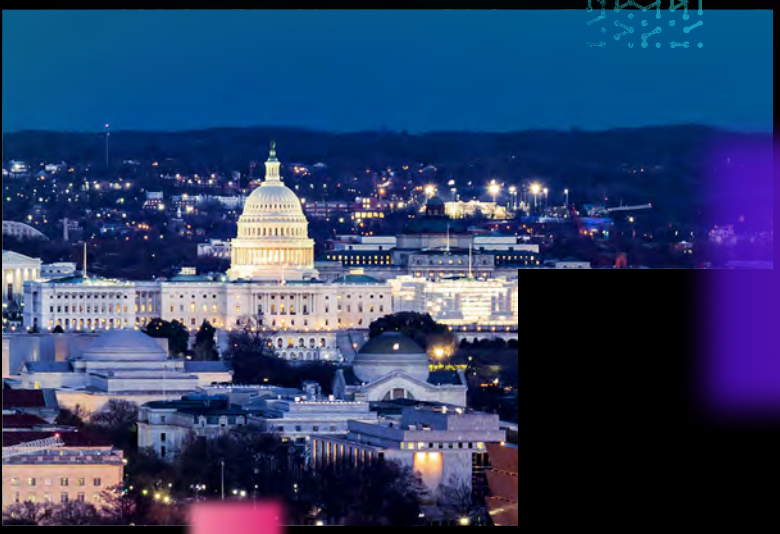
76% believe AI, quantum, and emerging technologies will create unprecedented escalation in cyber conflict capabilities.

81% agree that nation-state cyber capabilities could trigger a full-scale cyberwar that impacts critical infrastructure.

WHAT THIS MEANS

AI has fundamentally altered the tempo of cyber conflict. Automated reconnaissance, adaptive malware, and AI-assisted social engineering reduce the time between vulnerability discovery and exploitation. At the same time, the convergence of AI, quantum computing, and other emerging technologies introduces long-term systemic risk. Permanently stored sensitive data, encrypted communications, and operational systems may face future decryption or disruption scenarios.

Defense must operate at machine speed. Agencies must prepare not only for today's AI-enabled attacks but for tomorrow's escalation driven by technological convergence.



Cyber Risk Is Slowing Federal Modernization

THE DATA

60% have delayed, stalled, or stopped digital transformation projects due to cyberwarfare threats.

WHAT THIS MEANS

Cybersecurity risk is influencing strategic investment decisions across federal agencies.

When transformation initiatives are delayed due to security uncertainty, mission effectiveness and service delivery can suffer. Agencies face pressure to modernize while simultaneously defending against increasingly sophisticated adversaries.

To sustain innovation, security must function as an enabler rather than an obstacle. Reducing blind spots allows agencies to advance modernization with confidence and resilience.

Enabling a Proactive Federal Cyber Posture with Armis Federal

The findings in this report are drawn from a survey of 100 U.S. Federal IT decision-makers, conducted as part of the annual **2026 Armis Cyberwarfare Report**. This primary research underscores the realities facing federal networks: escalating cyberwarfare, AI-driven acceleration of attacks, and persistent exposure across expanding environments.

Armis Federal is committed to bringing data-driven insight to the federal cybersecurity community, helping agencies quantify risk and understand the operational implications of evolving threats.

ARMIS FEDERAL

By illuminating the total federal attack surface, Armis Federal enables agencies to:

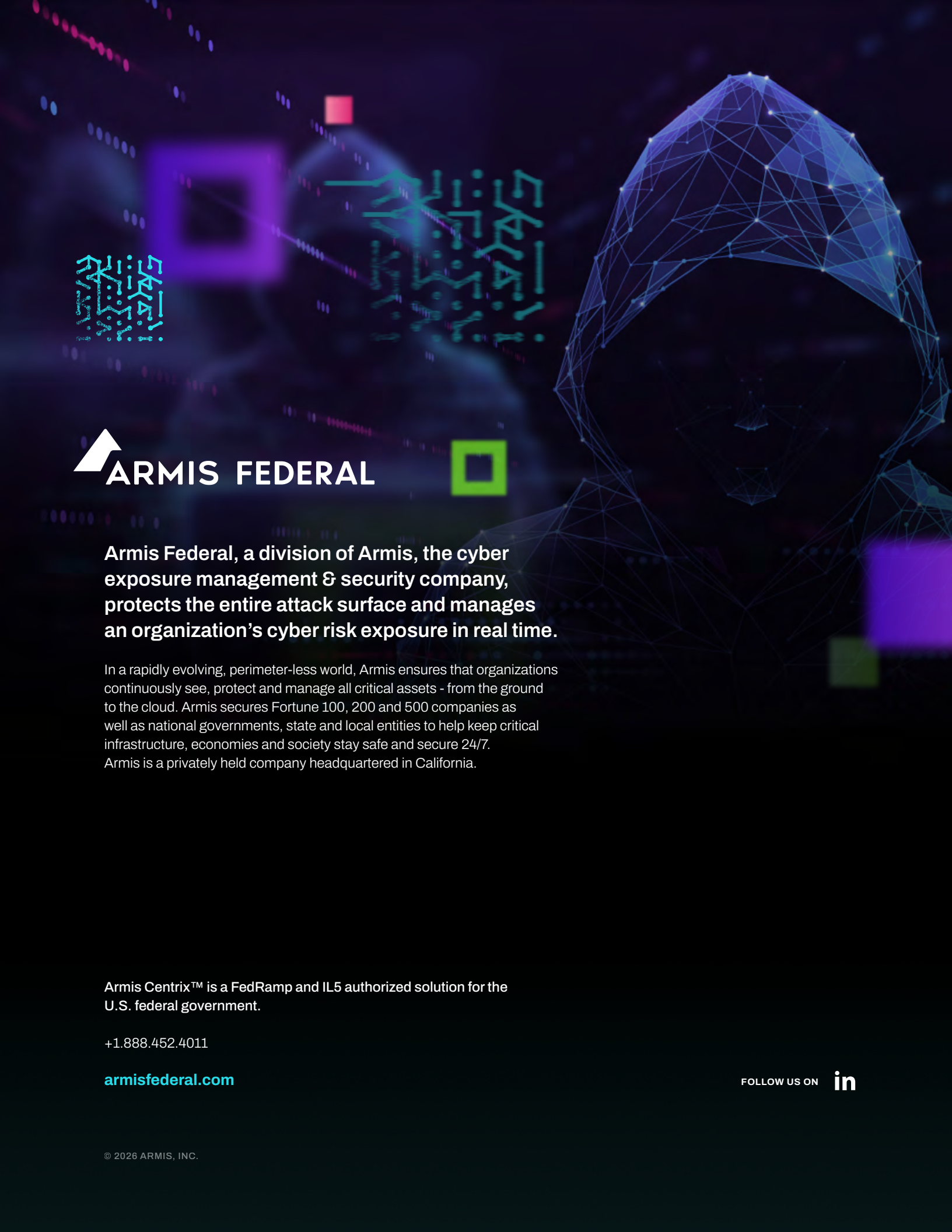
- ☑ Validate preparedness through continuous exposure insight.
- ☑ Reduce the likelihood and impact of ransomware and AI-driven attacks.
- ☑ Protect critical infrastructure and mission systems.
- ☑ Accelerate secure modernization initiatives.
- ☑ Transition from reactive incident response to proactive, intelligence-driven defense.

ARMIS CENTRIX™

Armis Centrix™, the cyber exposure management and security platform, delivers:

- ☑ Complete visibility into managed and unmanaged assets across IT, OT, IoT, medical, ICS, and cloud environments.
- ☑ Real-time asset intelligence to identify unknown, unauthorized, and misconfigured devices.
- ☑ Risk-based exposure management that prioritizes vulnerabilities based on exploitability and mission impact.
- ☑ Continuous monitoring to detect anomalous behavior and emerging threats.
- ☑ Support for Zero Trust initiatives through comprehensive asset awareness and segmentation enforcement.

As cyberwarfare intensifies and emerging technologies reshape the threat landscape, federal agencies require persistent, automated visibility across every connected asset. Armis Federal provides the foundation for resilient cybersecurity operations that align confidence with demonstrable control.



ARMIS FEDERAL

Armis Federal, a division of Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7. Armis is a privately held company headquartered in California.

Armis Centrix™ is a FedRamp and IL5 authorized solution for the U.S. federal government.

+1.888.452.4011

armisfederal.com

FOLLOW US ON in