



BSA's 2027 Global Cyber Agenda for an AI World

Policymakers Should Reprioritize to Meet New Challenges

The New Cyber Landscape: AI, Speed, Scale, and Sophistication

Recent breakthroughs in frontier AI cybersecurity systems, including models such as GPT-6 Astra and Mythos, are reshaping the cybersecurity landscape. These systems can independently discover vulnerabilities, combine exploits, and execute cyberattacks with unprecedented speed, scale, and sophistication. As a result, strategies, policies, and priorities must evolve rapidly.

These capabilities present both major opportunities and new risks. Frontier AI cybersecurity systems can help defenders identify vulnerabilities, strengthen threat detection, and secure complex systems more effectively. Integrated into the software development life cycle, they can help organizations identify and mitigate vulnerabilities before attackers exploit them.

At the same time, these systems reduce the expertise required to execute effective cyberattacks and compress the time between vulnerability discovery and exploitation. The result is a structural shift in cyber risk: attacks can emerge faster, scale more broadly, and create greater operational, financial, and reputational harm across sectors.

Rethinking Cyber Policy for an Autonomous AI Era

The rise of autonomous AI security systems requires a rethink of cyber policy. Organizations and policymakers must adapt to a world in which AI increasingly shapes both cyber defense and cyber risk. Policies designed for a slower and more human-driven threat environment may no longer be sufficient as attacks become faster, more scalable, and more sophisticated.

At the same time, many foundational cybersecurity approaches remain as important as ever. Strong leadership from the C-suite, public-private collaboration, risk-based security frameworks, internationally recognized standards, and cross-border cooperation continue to provide the foundation for effective cybersecurity policy. In fact, as cyber threats accelerate and become more complex, these principles become even more critical because they were built to adapt to technological change and recognize that cybersecurity is both an enterprise-wide and global challenge.

The challenge for stakeholders is to determine which policies and priorities remain effective, which must be strengthened, and where new efforts are required.

Policymakers should encourage and incentivize the deployment of AI-enabled tools, including those that enable internal runtime visibility and data-level controls, in addition to cybersecurity tools that help organizations defend against increasingly fast, scalable, and sophisticated external threats.

Cyber Policy Priorities for an AI World

Given the new cyber landscape, the Business Software Alliance (BSA) recommends government prioritize:

- **Deploying AI for Cybersecurity.** [Leading organizations are already deploying AI to strengthen cybersecurity](#) but adoption remains uneven across sectors and organizations. Policymakers should encourage and incentivize the deployment of AI-enabled tools, including those that enable internal runtime visibility and data-level controls, in addition to cybersecurity tools that help organizations defend against increasingly fast, scalable, and sophisticated external threats.
- **Giving Cybersecurity Professionals Priority Access to Frontier AI Cybersecurity Systems.** Companies developing advanced frontier AI cybersecurity systems are already taking steps to provide trusted defenders with early or priority access to these capabilities, but policymakers should work with industry and other stakeholders to support a predictable, structured, transparent, and globally aligned public-private partnership for determining which organizations can access the most capable systems and under what conditions.
- **Improving Vulnerability Management.** Given frontier AI cybersecurity systems' ability to discover vulnerabilities, and chain comparatively low-level vulnerabilities together to increase their impact, policymakers should invest in the infrastructure to collect, analyze, score, and publish information about vulnerabilities; support the development and deployment of patches, including for open-source software; and encourage organizations to leverage network or host-level protections called virtual patches or vulnerability shields.
- **Modernizing Legacy Systems.** Legacy and bespoke systems, more commonly used in government agencies, often operate beyond their supported life cycles or cannot be effectively patched or secured. In an environment in which malicious actors can use AI to discover and exploit vulnerabilities faster and at greater scale, these systems increasingly represent high-risk weak points. Policymakers should prioritize modernizing outdated systems and reforming procurement practices to encourage secure, updatable, and resilient technologies over the long term, including deploying post-quantum encryption.
- **Building Resilience Into Systems.** [Even before the rise of autonomous AI security systems, organizations needed to place greater emphasis on cyber resilience.](#) Today, however, organizations must increase investment in their ability to continue operating during cyber incidents and recover to a trusted state quickly. Policymakers should support these efforts by encouraging clear recovery objectives and promoting capabilities such as AI-enabled recovery tools, immutable storage, and regularly tested restoration processes.
- **Aligning Regulations to Strengthen Cybersecurity.** Fragmented and overlapping cybersecurity regulations continue to shift resources away from cybersecurity and to compliance checklists, particularly in the realm of cyber incident reporting. While this challenge is not new, it is more urgent in an era of AI-enabled cyber threats, where defenders must move faster and operate at greater scale. Policymakers should [align and streamline cybersecurity requirements across sectors and jurisdictions](#).
- **Upgrading to Post-Quantum Cryptography.** The timing of the arrival of cryptographically relevant quantum computers remains uncertain, but "harvest-now, decrypt-later" attacks are here today and the transition to post-quantum cryptography (PQC) will take years to complete. Organizations should leverage available AI-enabled solutions to inventory cryptographic assets and take risk-based approaches to deploying PQC today so they can upgrade without disrupting critical operations. Policymakers should accelerate this transition by supporting upgrade road maps, prioritizing high-value systems, updating procurement guidance and approach, and encouraging the adoption of PQC standardized by the National Institute of Standards and Technology (NIST) across the public and private sectors.
- **Measuring Cybersecurity Outcomes.** [Organizations should track operational metrics such as mean time to detect, mean time to respond](#), as well as vulnerability remediation timelines, to ensure investments are delivering real-world improvements. Policymakers should work with industry to develop, support, and use these metrics to ensure cybersecurity requirements drive concrete cybersecurity improvements.