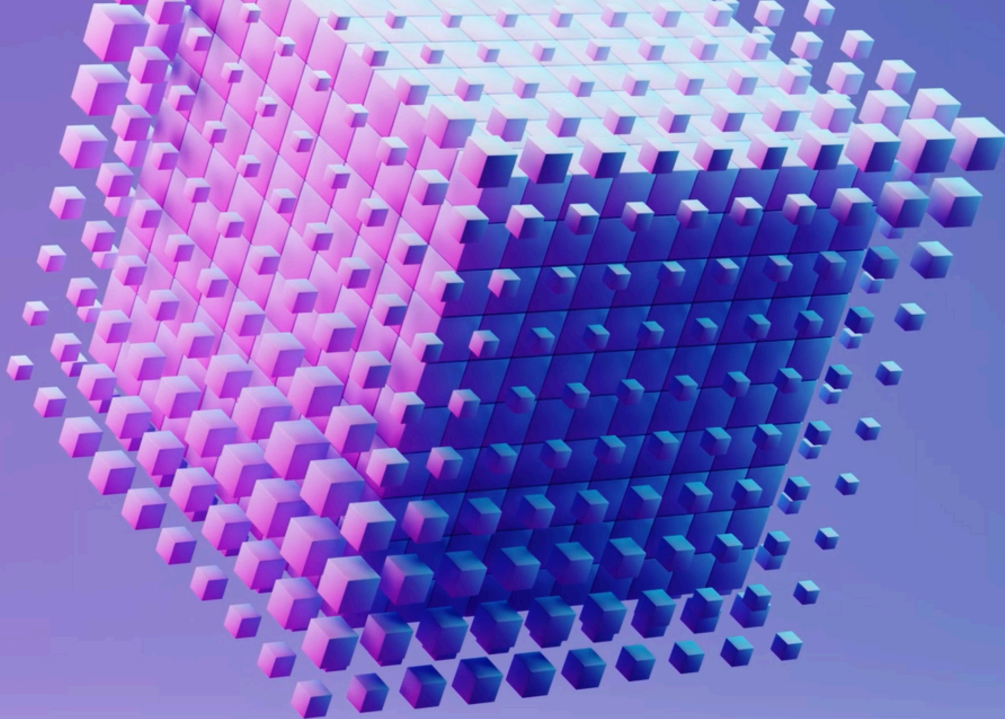


AI and National Security

Trend Topic: **Readiness**



Preparing for AI in a new security landscape

By



Klon Kitchen

Senior Fellow at
American Enterprise
Institute

Artificial intelligence (AI) is reshaping global competition, but for U.S. businesses, the challenge is no longer just about innovation—it is about survival in a geopolitical environment where national security and corporate responsibility converge.

While many executives have made progress preparing their organizations for AI's transformative potential by identifying use cases, investing in infrastructure, and tackling adoption challenges, an equally critical aspect of AI readiness demands attention: national security.

This is not only about compliance checklists and being prepared to manage a public relations crisis. It is about recognizing the broader geopolitical, economic, and security implications that AI adoption introduces and the role your organization plays in safeguarding the United States and its interests.

The Emerging National Security Imperative

AI is no longer just a tool for optimizing supply chains or streamlining customer service. It is a strategic asset—one that adversarial nations are targeting with unprecedented focus. The U.S. government sees this reality clearly. For instance, the Department of Defense views AI as a foundational technology for maintaining military superiority. Federal agencies are tightening export controls, scrutinizing data flows, and emphasizing the protection of critical infrastructure. These actions are not arbitrary; they are rational responses to real threats.

China's ambitions in AI are particularly instructive. Beijing has explicitly articulated its goal of becoming the global leader in AI by 2030. This goal is not limited to academic benchmarks or industry accolades; it is a cornerstone of a broader geopolitical strategy. China's leadership understands that AI will determine not just who innovates but who leads economically, technologically, and militarily.

This desire for dominance manifests in several ways. Chinese companies are embedding AI into surveillance systems that track millions of citizens, both domestically and abroad. Technologies like facial recognition and predictive policing are not just tools of social control but mechanisms for projecting influence globally. Additionally, China's industrial policies—such as its subsidies for AI-related technologies—give its companies an edge in global markets, creating dependencies that can be leveraged in times of geopolitical conflict.

A striking example of this is China's Belt and Road Initiative, a global infrastructure strategy that incorporates AI systems into the digital "Silk Road" to expand Beijing's political and economic influence. Many countries participating in the initiative are adopting Chinese-built AI systems for smart cities and government operations. These systems come with long-term dependencies, meaning that countries relying on them require ongoing sup-

port, updates, and integration, enabling Beijing to exert political and economic influence on a global scale.

This strategy underscores the lengths to which adversaries will go to secure strategic advantages, a trend further exemplified by recent incidents targeting U.S. AI infrastructure.

From espionage campaigns aimed at proprietary algorithms to supply chain infiltration involving hardware components, the threats are both sophisticated and pervasive. For instance, reports of Chinese-manufactured hardware components with embedded vulnerabilities have raised alarms about potential backdoors in critical systems. These risks are not theoretical; they are a daily reality in the hyperconnected global economy.

The implications extend beyond the theft of intellectual property. Consider the potential consequences of adversarial manipulation. An AI system corrupted at the training stage could subtly distort outcomes in ways that remain undetected until critical decisions—financial, operational, or even life-and-death—are impacted. This is not hypothetical; adversarial attacks on machine learning systems **are** well-documented and **are** evolving rapidly.

From espionage campaigns aimed at proprietary algorithms to supply chain infiltration involving hardware components, the threats are both sophisticated and pervasive.

Why Industry's Role is Critical

The U.S. government can only do so much. Unlike in China, where industry operates at the direction of the state, America's strength lies in its innovative private sector. This dynamic is a double-edged sword. On the one hand, it enables the kind of creativity and agility that leads to breakthroughs. On the other, it creates vulnerabilities when companies underestimate the strategic dimensions of their operations.

Failing to address national security risks is not just a vulnerability for individual organizations—it is a systemic issue. The interconnectedness of the global economy means that one compromised node can have cascading effects.

Consider the intersection of AI and supply chain security. Many organizations rely on foreign manufactured hardware—GPUs, sensors, or even basic semiconductors—that underpin their AI deployments. If these components originate from adversarial nations, they could carry backdoors or vulnerabilities that compromise not only the integrity of your systems but the broader security of critical sectors. The semiconductor shortage of recent years underscores how fragile these supply chains can be. Now, overlay that fragility with the risks of malicious interference, and the stakes become even clearer.

Washington recognizes these challenges and has begun acting accordingly. Export controls on advanced semiconductors, initiatives to reshore critical industries, and policies to strengthen public-private partnerships all point to a shared objective: safeguarding America's AI future. But these measures cannot succeed without active industry participation. The private sector is not a bystander in this fight; it is the front line.

For businesses, this is not just about avoiding sanctions or regulatory penalties. It is about competitiveness. Companies that demonstrate robust security practices and alignment with national priorities will find themselves at an advantage—whether in securing federal contracts, attracting global customers, or mitigating reputational risk in an era of heightened geopolitical scrutiny. Conversely, those that fail to adapt will face an uphill battle, as both public and private stakeholders increasingly demand accountability.

The Broader Stakes for Industry

Failing to address national security risks is not just a vulnerability for individual organizations—it is a systemic issue. The interconnectedness of the global economy means that one compromised node can have cascading effects. For example, an attack on a single AI-powered logistics platform could disrupt supply chains for entire industries, amplifying economic instability.

Additionally, as adversaries continue to innovate, the gap between offensive and defensive capabilities grows. A reactive posture will no longer suffice. Companies must adopt proactive strategies that integrate security into the DNA of their AI initiatives. This requires not only technical solutions but also cultural and organizational shifts.

Imagine the implications of an adversary subtly influencing the decisions of an AI system used to manage critical infrastructure—say, energy grids or transportation networks. The damage could cascade beyond the initial target, undermining public

trust, destabilizing economies, and even triggering broader geopolitical consequences. These risks highlight why no company, regardless of its size or industry, can afford to overlook its role in securing the broader ecosystem.


Taking Action: A Roadmap for Leaders

For CEOs and CISOs ready to take these challenges seriously, several steps can help address national security risks.

First, conduct a geopolitical risk assessment. Evaluate your AI supply chain, partnerships, and data practices through a geopolitical lens. Where are your hardware components sourced? Who are your cloud providers, and what jurisdictions govern their operations? The answers to these questions should inform a detailed risk map. Partner with firms specializing in geopolitical intelligence to understand how shifts in global politics might affect your vulnerabilities.

Second, collaborate with the U.S. government. Build formal relationships with federal agencies, such as the Department of Defense, the Department of State, and the Department of Commerce. Engage in public-private partnerships focused on AI security and participate in federal initiatives like the National Artificial Intelligence Initiative. Beyond compliance, these partnerships provide insight into emerging threats and access to tools that can enhance your organization's security posture.

Third, integrate "security by design" across the AI lifecycle. Security must be a core consideration from the outset of any AI project. This includes safeguarding training data, securing cloud storage, and testing models against adversarial attacks. Implement automated systems to monitor for unusual patterns or anomalies in AI behavior post-deployment. Consider leveraging frameworks such as the National Institute of Standards and Technology (NIST) AI Risk Management Framework to standardize your approach to identifying and mitigating risks.



Security must be a core consideration from the outset of any AI project. This includes safeguarding training data, securing cloud storage, and testing models against adversarial attacks.

Finally, build organizational resilience. National security risks are not just technical—they are operational and cultural. Create cross-functional teams that integrate security professionals, legal advisors, and technologists to ensure a holistic approach. Train your workforce to recognize and respond to emerging threats and ensure that your organization fosters a culture where security considerations are baked into innovation. Regularly simulate scenarios involving AI-related disruptions to test your readiness and identify weaknesses. Use your position as a leader to advocate for industry-wide standards and best practices in AI security. Collaborate with peers, trade organizations, and policymakers to drive initiatives that align private-sector innovation with public-sector priorities. By contributing to a secure and resilient AI ecosystem, you reinforce not only your organization's safety but also its reputation as a responsible industry leader.

Conclusion

The rise of AI represents both an extraordinary opportunity and a profound responsibility. As CEOs and CISOs, you are uniquely positioned to navigate this duality. You have already proven your ability to lead your organizations through the complexities of digital transformation. Now, the challenge is to expand that leadership to account for the broader implications of AI in an era of heightened national security risks.

Your organizations do not operate in a vacuum. They are part of a larger ecosystem that shapes and is shaped by global forces. By addressing the national security dimensions of AI readiness, you are not just future-proofing your business—you are playing a pivotal role in ensuring that the United States remains secure, competitive, and free.

The stakes are high, but so is the potential for impact. This is the moment to act decisively. As the stewards of transformative technologies, you hold the keys to both innovation and resilience. The question is not just whether you can adapt but whether you will lead.

The answer to that question will define your legacy—and the security of the systems that underpin it.

