The Next Imperative: Geopolitics and the AI Power Play

The questions boards should be asking


Fumbi Chima


Andreea Bulisache

This article is the third in a four-part series designed to reframe the AI conversation for senior executives and board directors.

Artificial Intelligence (AI) has moved beyond its origins as a research endeavor to become a central pillar of global strategic competition. Following *The Next Imperative and Capacity: From Model to Megawatt*, we now turn to the shifting geopolitical landscape, where AI is redrawing lines of influence, sovereignty, and security.

Across economies and institutions, AI is increasingly recognized as more than a technology—it is a lever of national security, economic development, and ideological governance. The race for AI leadership now encompasses not only algorithms, but also compute capacity, access to energy, talent mobility, and influence over regulatory frameworks. This convergence signals a shift that boards can no longer afford to view from the margins.

Drawing on our advisory work with organizations navigating AI strategy, policy uncertainty, and systemic transformation, we approach this topic with a dual lens: **one grounded in geopolitical analysis**, and **the other in enterprise foresight**. We write from the conviction that governance must evolve alongside innovation—and that boards must be equipped not only to adapt, but to shape the environment in which AI operates.

Boards today are called to engage with AI not only as a growth enabler but as a geopolitical force—one that affects operating models, capital flows, supply chain dependencies, and stakeholder trust. Decisions made at the highest levels of governance will shape how enterprises navigate global complexity and contribute to the long-term security and sustainability of the ecosystems in which they operate.

Organizations that embed geopolitical foresight into their AI strategies will strengthen their agility and capacity to lead in a world of accelerating realignment. Those that do not may face rising exposure—legal, operational, and reputational—in markets where AI is both a source of power and a strategic lever.

AI as a New Instrument of Sovereignty

Technological revolutions have long influenced the evolution of global power structures. AI is now extending this legacy—transforming how countries pursue strategic advantage, protect infrastructure, and influence the global digital order.

Governments around the world are integrating AI into national security doctrines, economic development plans, and digital governance models. The objective is not only to leverage AI, but to control its foundations—compute infrastructure, data flows, semiconductors, and energy.

In this context, AI systems are increasingly treated as sovereign-grade assets. Their development and deployment are shaped by export controls, investment restrictions, and national capability strategies. For globally active enterprises, this creates a new strategic landscape—one where navigating political priorities is as essential as managing platform roadmaps or customer pipelines.

AI's influence extends across domains:

Military modernization strategies

Cyber defense architectures

Next-generation industrial competitiveness

Nations that achieve leadership in AI capabilities are likely to gain disproportionate leverage across trade, finance, and digital ecosystems. (Source: Brookings Institution, 2024; WEF Global Risks Report, 2024)

Boards and CIOs should ask:

- How do emerging views of AI as a sovereign asset affect our global operating models?
- Are we adequately monitoring how national AI strategies could influence market access, partnership dynamics, or regulatory exposure?

Strategic Shifts: Fragmentation, Infrastructure, and Regulation

The early vision of a seamlessly interconnected digital economy is giving way to a more fragmented reality, accelerated by AI's strategic significance. Distinct regulatory, technological, and geopolitical blocs are emerging:

- **The U.S.- led Alliance** focuses on private-sector-driven innovation in foundational models, hyperscale infrastructure, and trusted AI systems.
- **China's Sovereign Strategy** prioritizes domestic semiconductor production, national R&D investments, and active leadership in setting global AI norms. (Source: Reuters, 2024)
- **The EU and Responsible AI Bloc** advances ethical frameworks emphasizing risk management and human rights, balancing innovation with regulatory safeguards.
- **BRICS and Emerging Powers** are forging regional collaborations aimed at reducing dependency on dominant Western and Chinese technologies. (Source: Foreign Policy, 2024)

Beneath these strategic narratives lies a critical competition over control of infrastructure:

- **Semiconductors** are now viewed as strategic commodities, with export controls reshaping global supply chains. (Source: European Commission, 2023)
- **Data sovereignty** regulations require enterprises to localize storage and processing across jurisdictions.
- **Energy availability**, particularly access to low-carbon, high-reliability power sources, is becoming a central factor in AI scalability. (Source: IEA, 2024)

Diverging regulatory environments further amplify complexity:

The **EU AI Act** introduces binding obligations for high-risk AI systems, emphasizing transparency and accountability.

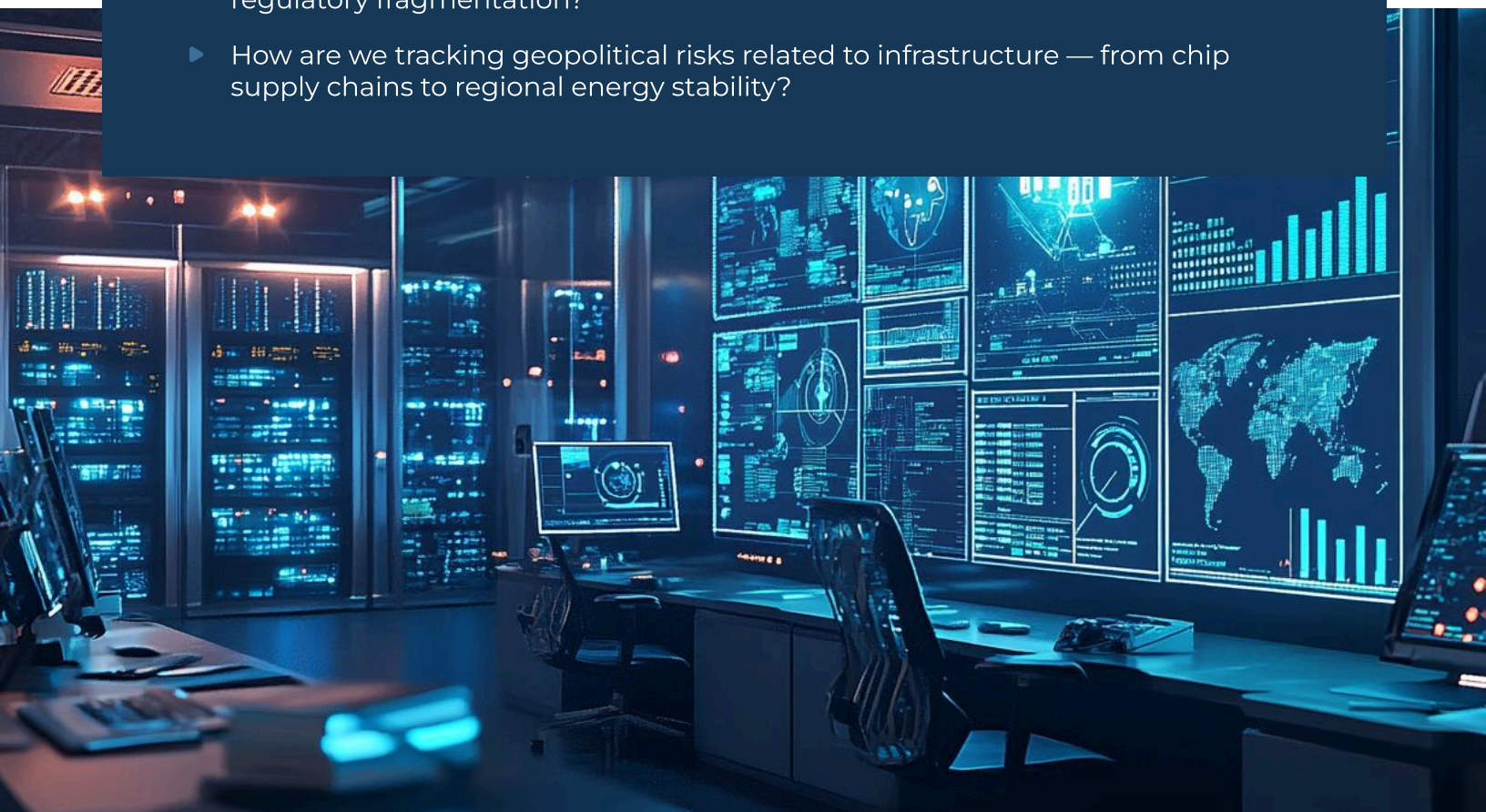
U.S. executive orders on AI governance prioritize national security and trustworthy AI principles.

China's evolving AI regulations balance acceleration with censorship and information control. (Source: OECD AI Governance Briefs, 2024)

Across these dimensions, governments are deploying sovereign AI strategies as instruments of long-term economic leadership.

Boards and CIOs should ask:

- Are our data governance, cloud, and AI model deployment strategies resilient to regulatory fragmentation?
- How are we tracking geopolitical risks related to infrastructure — from chip supply chains to regional energy stability?



Cybersecurity and Geopolitical Risk: Boardroom Imperatives

AI's integration into critical systems—from infrastructure and healthcare to finance and logistics—brings new dimensions to enterprise vulnerability. Where threat actors once targeted networks, they are now probing algorithms, training pipelines, and the datasets that underpin decision-making.

The spectrum of risk is expanding:

Model inversion attacks, **data poisoning**, and **synthetic content generation** introduce novel vulnerabilities.

Non-state actors, empowered by generative tools, are able to scale misinformation, deepen cyberattacks, and automate influence operations.

Sector-wide risk amplification emerges when AI systems coordinate across supply chains or core infrastructure. (Source: Chatham House Reports, 2024)

In this environment, cybersecurity is no longer a technical function—it is a pillar of strategic oversight. AI-specific vulnerabilities must be governed with the same discipline as financial exposure or compliance risk.

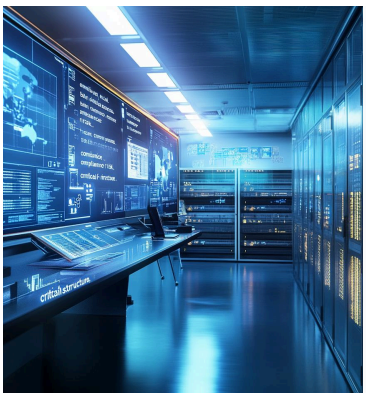
Boards and CIOs should ask:

- Have we integrated AI-specific cybersecurity risks into our enterprise-wide risk frameworks?
- Are we building internal capabilities to detect, respond to, and recover from AI-enabled threats?

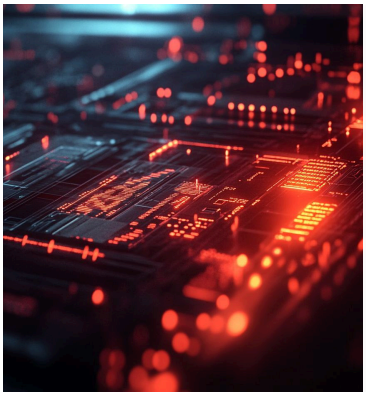
Strategic Imperatives for Boards: Navigating the New Chessboard

In a geopolitical climate shaped increasingly by AI, enterprise success will hinge not only on technological investment, but on the depth of insight guiding governance. Boards have a critical role to play in setting the tone and structure for strategic foresight, ethical adaptation, and resilient infrastructure.

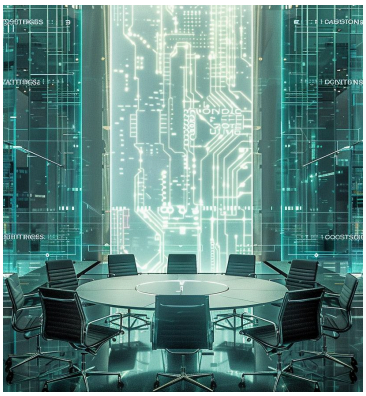
Scenario Planning and Strategic Foresight
Boards should mandate the development of AI-specific geopolitical scenarios, integrated into risk, compliance, and capital allocation frameworks. These scenarios should model disruptions such as chip embargoes, regulatory fragmentation, or regional AI bans—and provide action-oriented recommendations for adaptation.



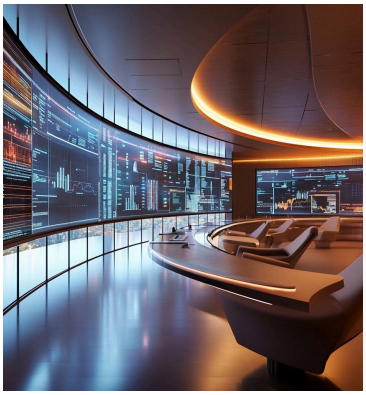
Infrastructure Diversification and Compute Agility
Diversifying access to compute—geographically and across vendors—offers both resilience and strategic leverage. Sovereign cloud partnerships, modular data center strategies, and compute resource pooling can provide insulation from shocks while supporting long-term scalability.



Cybersecurity Integration and Model Integrity
Boards should ensure that AI model governance, threat monitoring, and adversarial testing are embedded within existing cybersecurity programs. Oversight should involve collaboration across CISOs, Chief AI Officers, and legal risk teams, with attention to third-party platforms and generative content risk.



Policy Engagement and Thought Leadership
Board support for executive participation in multilateral AI coalitions, standards bodies, and ethics councils strengthens institutional influence. Active engagement with policy trends enables enterprises to anticipate shifts—and contribute to the formation of principles that shape future regulation.



Board and Executive Capability Development
Geopolitically informed AI governance demands new fluency across the board. Boards should invest in director education that spans technology, digital governance, global compliance, and security. Cross-functional literacy among board members is a marker of maturity in AI oversight.

Supply Chain Mapping and Resilience Strategy
Organizations should maintain updated, granular maps of their critical AI-related supply chains—from semiconductors to energy infrastructure—and develop options for redundancy, friendshoring, and crisis response. Transparency and agility will define enterprise preparedness in increasingly contested environments.

Boards and CIOs should ask:

- How resilient are our AI ambitions against potential geopolitical fractures?
- Are we equipping leadership with the capabilities to anticipate, navigate, and influence emerging AI governance landscapes?

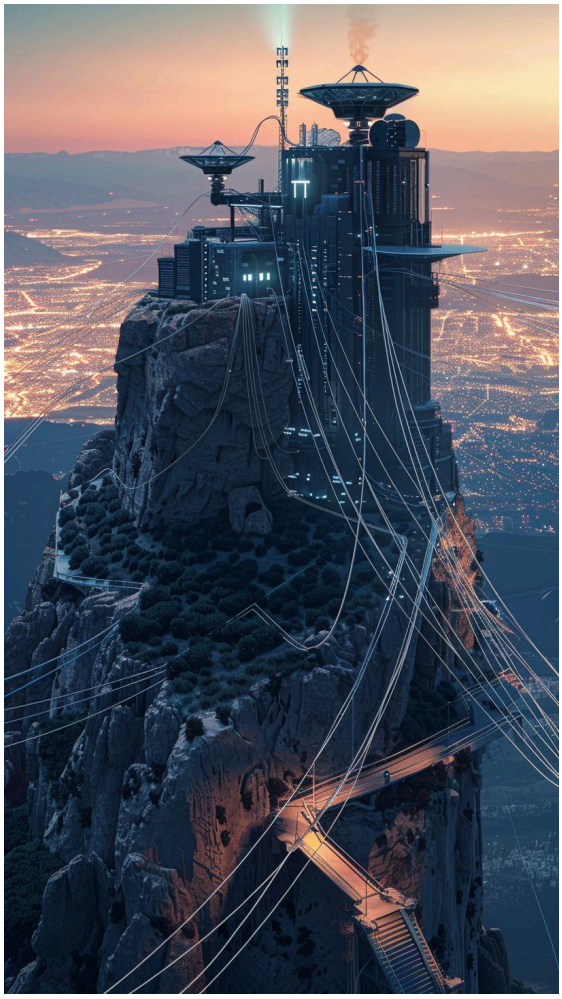
Conclusion: Geopolitics as a Central Pillar of AI Strategy

Artificial Intelligence is no longer merely a driver of digital transformation. It is a defining force in how nations assert influence, how economies compete, and how enterprises navigate opportunity and risk. Boards that frame AI through a narrow lens—focused only on ROI or product acceleration—will miss the broader implications of geopolitical entanglement. In contrast, boards that engage deeply with the evolving intersections of policy, power, and platform will position their organizations for durable leadership.

Risks of Neglecting Geopolitical Dimensions

A lack of engagement with AI's geopolitical context is not a neutral stance. It carries risk:

- **Operational Inefficiencies:** Unanticipated restrictions on data flows, compute access, or infrastructure partnerships can disrupt global operations.
- **Regulatory Penalties:** Organizations that lag in aligning with national and regional AI frameworks may face compliance violations or delayed market access.
- **Loss of Trust:** Stakeholders increasingly expect companies to demonstrate awareness of ethical and geopolitical concerns. Inattention can erode credibility with investors, regulators, and civil society.



Boards that lead with discipline and insight—shaping resilient AI strategies in light of global dynamics—will define a new standard of preparedness and principle. The coming decade will be shaped not solely by the pace of technical innovation, but by the strategic acumen with which organizations anticipate shifts, mitigate vulnerabilities, and lead responsibly.

In our next and final installment, we will explore how sustainability considerations—from energy use to environmental impact—are rapidly becoming defining factors for responsible AI leadership.

Fumbi Chima

https://www.linkedin.com/in/fumbi-chima/

Dr. Fumbi Chima is a global technology executive who has led digital and operational transformation initiatives at industry-leading brands including adidas, Burberry, Walmart, Boeing Credit Union, and Fox Networks. Her experience spans P&L ownership, M&A, operations, and enterprise technology leadership across retail, CPG, digital, and financial services. She is widely recognized as an AI thought leader with a strong reputation for aligning innovation with business goals to deliver sustainable value and competitive advantage. At adidas AG, she spearheaded large-scale infrastructure and process transformations, achieving cost savings, accelerating speed to market, and enabling cross-market scalability. Known for bridging the gap between technology and business, she fosters high-performance cultures rooted in innovation, accountability, and transparency. Her leadership has consistently increased employee engagement and organizational impact. Throughout her career, she has championed innovative solutions in data strategy, digital marketing, and cybersecurity, always with a relentless focus on driving growth and enhancing customer experience.

Andreea Bulisache

https://www.linkedin.com/in/andreeabulisache/

Andreea Bulisache is a global tech executive and strategist with deep expertise in AI, cybersecurity, and digital transformation. A former Microsoft leader, she played a key role in scaling emerging technologies and leading complex integrations such as GitHub and Databricks, translating innovation into tangible business value. As Founder of Stratified Advisory, she partners with CEOs, PE-backed companies, and boards to drive enterprise innovation and navigate digital and regulatory complexity. Known for her ability to bridge technical depth with strategic insight, Andreea has contributed to national AI and cybersecurity frameworks and frequently advises on risk, governance, and sustainable innovation. She serves as Chair of Young & Bold and sits on the International Advisory Board of Nyenrode Business University. A graduate of the Harvard Business School Women on Boards Program, she brings a forward-thinking lens to the evolving intersection of technology, geopolitics, and long-term boardroom resilience.

Links to sources referenced in this article:

Brookings Institution, "AI and National Security Briefs," 2024

World Economic Forum, "Global Risks Report," 2024

Reuters, "China AI Strategy and Global Impact," 2024

Foreign Policy, "Semiconductor Tensions and Global Supply Chain Risk," 2024

European Commission, "EU Chips Act and Green Deal Initiatives," 2023

International Energy Agency (IEA), "Data Centers and Electricity Demand," 2024

Chatham House, "AI and Cybersecurity," 2024

OECD, "AI Governance Policy Briefs," 2024

MIT Sloan Management Review, "A Playbook for Crafting AI Strategy," 2024

Stanford AI Index, "AI and Global Trends Report," 2025

RAND Corporation, "Emerging Threats to AI Supply Chains," 2024