

January 2026

Follow us on [LinkedIn](#)

## Industry Update

# Geopolitical Predictions General Counsel Need to Know for 2026

By [Ronak Desai](#), [Amir Ghavi](#), and [Marguerite Harris](#)

For general counsel (GCs), geopolitics has always represented an important consideration for managing enterprise risk. But the global volatility that characterized 2025 felt different. The past year underscored the extent to which a rapidly evolving international landscape has become a central variable in GC decision-making.

Tariff and trade tensions, ongoing armed conflict, supply chain fragility, shifting sanctions regimes, critical mineral weaponization and intensifying chip wars between the United States and China thrust geopolitics into the core of everyday legal and business judgments. The last several months underscored how these forces increasingly determine what companies can source and ship, how they price and contract, which customers and jurisdictions they can serve, and how they approach compliance, disclosures and crisis management.

Rather than being an aberration, this geopolitical turbulence is likely to have a more pronounced impact in 2026.

Here are our top nine geopolitical predictions for 2026 and what each one means for the GC agenda and board oversight.

### Tariffs and Trade

1. **Trade friction and tariffs under President Donald Trump will become more targeted and sector-specific.** The new year continues the Trump 2.0 playbook of deploying tariffs (and tariff carve-outs) to drive bargaining leverage, reshape investment flows and punish or privilege particular countries and sectors. The Trump administration's 2025 National Security Strategy (NSS) explicitly treats tariffs and related tools as core national and economic security instruments. This portends a world in which tariff actions are paired with selective relief — country-by-country, company-by-company or sector-by-sector — depending on perceived strategic alignment or investment commitments. It also suggests more frequent “midstream” shifts that are less about comprehensive trade policy and more about targeted pressure on specific supply chains, inputs and industries.

**GC Impact:** The practical consequence is a steady stream of midcycle retrading: pricing, delivery and remedies suddenly become contested when tariff assumptions move. For GCs, the risk can be mitigated through consistency by ensuring the company's positions in contracts, disputes and public-facing statements do not diverge as different business units respond to the same tariff shock in

different ways. The danger is inconsistent customer treatment, misaligned internal escalation and hard-to-defend narratives when counterparties (or investors) demand a single explanation for outcomes that were handled differently across the enterprise.

2. **The “silent tariff” will be enforcement and border friction, even when headline rates do not change.** The most consequential trade disruption for many companies in 2026 will come from the administration, not announcement, of trade barriers — specifically more scrutiny at the border, more documentation-driven interruptions, and more friction in clearance, classification, origin substantiation and valuation. As enforcement tightens, routine error rates that were previously tolerable can become operational disruptions with real financial consequences.

**GC Impact:** When enforcement becomes more stringent, trade issues migrate from the trade team to the core legal function. A held shipment becomes a performance question. A rejected shipment becomes a commercial remedies question. A recurring documentation failure becomes a counterparty management question. These are the moments when the GC is asked to quickly reconcile operational realities with contractual language and external communications. In 2026, that pattern is likely to persist even in periods when tariff rates appear stable.

3. **The Supreme Court’s decision on Trump’s IEEPA tariffs will be a 2026 inflection point for trade risk regardless of the court’s decision.** The Supreme Court is poised to decide whether President Trump had authority under the International Emergency Economic Powers Act (IEEPA) to impose sweeping “reciprocal” and related tariffs after the Court of International Trade (CIT) and the Federal Circuit ruled the tariffs exceeded that authority.

**GC Impact:** If the court upholds the Trump administration’s use of tariffs, future tariff exposure becomes harder to forecast and easier to impose quickly. If the Court narrows the president’s tariff authority as many observers expect it will, the immediate issues confronting GCs will be focused on what happens to tariffs already paid, how refunds (if any) are processed and who is procedurally positioned to benefit. The fact pattern is already emerging. Importers have filed waves of CIT cases to preserve potential refund rights, and the CIT has issued orders managing or staying refund litigation while the Supreme Court rules.

## Artificial Intelligence

4. **U.S. federal–state collision over AI hardens into an enforcement posture, not a policy debate.** This year will likely witness the federal government’s AI preemption campaign becoming increasingly aggressive, driven by President Trump’s Dec. 11, 2025, AI executive order calling for a “uniform Federal policy framework” and directing the build-out of mechanisms (including an AI litigation task force and other levers) to challenge state AI laws viewed as inconsistent with federal policy. At the same time, states will continue to legislate aggressively in targeted use cases (youth safety and “AI companion” rules are early examples), making the state pipeline of new obligations unlikely to slow simply because preemption is asserted.

**GC Impact:** GCs will have to manage sprawling legal and policy risk originating from inconsistency and collision between federal and state policies, specifically the expansion of state-by-state operational requirements while federal actors test constitutional and statutory theories to knock some of them down. For legal departments, there will be a recurring question of what the company can credibly commit to (in products, contracts and public statements) when the governing rule set may differ by state and may also be subject to federal challenge.

5. **Global AI “balkanization” accelerates as the EU regime turns operational.** The EU AI Act will move from the planning stage to possessing real operational gravity as it becomes fully applicable on Aug. 2 (with staged exceptions). Meanwhile, other jurisdictions regulate AI and data with different

priorities (sovereignty, security access, industrial policy), producing divergence rather than convergence.

**GC Impact:** For GCs, the central challenge is twofold: rules are tightening and are doing so in different directions. One jurisdiction may demand more transparency and explainability, while another treats the same disclosures as sensitive or impermissible. One regime may push data minimization and transfer restrictions, while another asserts broad state-access or localization mandates. Some frameworks emphasize risk classification and documented human oversight; others prioritize national security, content control or industrial policy in ways that change what models can do, where they can run and who can use them.

6. **The battle for AI data centers becomes a mainstream regulatory and political fight over energy, permitting, community and “who pays.”** AI-driven load growth is already pushing U.S. electricity demand toward record levels and driving controversial infrastructure responses, including the return of older “peaker” plants and new grid-rule disputes over data-center connections. Local resistance is also rising, with communities increasingly focused on land use, noise, diesel backup generation, water and transmission buildouts.

**GC Impact:** “AI risk” in this domain becomes infrastructure counsel work. Permitting friction, reliability representations, public scrutiny and regulatory conditions begin to influence what businesses can promise customers about uptime, scaling and deployment timelines, especially where power procurement and interconnection are threshold items. The proliferation of data center construction will become more politically fraught questions, competing with households and legacy industry for scarce megawatts. Utility commissions and local governments will increasingly dictate terms that ripple into commercial commitments.

## Critical Minerals

7. **Critical minerals remain a strategic chokepoint.** Critical minerals will continue to be a source of major volatility and friction between countries. China’s decision to suspend its U.S.-targeted export-approval ban for certain dual-use items through Nov. 27 is a useful illustration: restrictions can be eased tactically while the licensing architecture (and the ability to tighten it quickly) remains intact. The Trump administration’s 2025 National Security Strategy explicitly frames this as a national-security priority, warning of threats to U.S. access to “critical resources, including minerals and rare earth elements,” and emphasizing the need to expand access to “critical minerals and materials.”

**GC Impact:** For GCs, this becomes a compliance-and-contracting problem, not just a sourcing problem. When a critical input tightens, the first-order questions are rarely geopolitical, but commercial and legal: whether allocation and price-adjustment language is triggered, whether substitution is permitted without breaching specs and how customer-facing representations about availability and performance hold up when the bottleneck sits upstream. For regulated sectors and government-adjacent businesses, minerals volatility also bleeds into representations and eligibility, origin, end-use restrictions and supplier attestations that can matter as much as the physical supply itself.

## Global Immigration

8. **The “Visa War” and talent mobility mean sudden talent lockouts become a real operating risk.** Governments will increasingly use visas, vetting and entry restrictions as instruments of leverage to create the practical possibility of sudden “talent lockouts” during political freezes. In the U.S., that risk is amplified by (i) tightened entry/vetting initiatives and travel/entry restrictions, and (ii) material changes to the H-1B ecosystem, including the Department of Homeland Security’s (DHS) finalized move away from a pure lottery toward a wage-weighted selection system effective late February 2026. Beyond these formal rule changes, operational bottlenecks are already driving corporate

behavior: major tech firms have warned certain visa holders to avoid international travel because visa stamping delays could strand employees abroad for months.

**GC Impact:** A company's most valuable intellectual property often sits in the minds of a few dozen key engineers or researchers. If those individuals are suddenly rendered "undocumented" or unable to cross a border due to a political freeze, the company faces an immediate operational crisis. This will present as an enterprise-continuity issue, not an "immigration team" issue. When key personnel cannot travel (or cannot reenter), the immediate questions are commercial: project delivery, customer commitments and internal accountability for missed milestones. It also reinforces a broader structural trend: as U.S. immigration uncertainty rises, companies accelerate work placement outside the United States, including shifting more critical functions to offshore hubs (notably India). For GCs, the practical focal point is maintaining defensible, repeatable positions on how the enterprise preserves continuity across employment/assignment structures, customer-facing commitments and the representations the company makes about its ability to staff and support work across borders when mobility becomes politically contingent.

## Cyber

9. **The "Act of War" insurance gap widens with cyber attribution becoming the real coverage battleground.** As state-backed cyber operations increasingly collide with private-sector infrastructure, insurers will continue tightening "war," "hostile act" and "state-backed cyber operations" exclusions, often in ways that push disputes away from *whether an attack happened* and toward *what it is legally characterized as*. Lloyd's has already driven the market toward more explicit cyber war or cyber operations clauses and away from noncompliant wording, with implementation deadlines that effectively force clearer (and often broader) exclusion language in standalone cyber policies. The Merck/NotPetya litigation is instructive, where an appellate court held insurers failed to prove the "hostile/warlike" exclusion applied, underscoring how contested these classifications can be and why insurers are revising language to reduce ambiguity.

**GC Impact:** This turns cyber insurance from a procurement line item into a governance and narrative issue. The hard questions tend to hinge on attribution mechanics embedded in the policy: how "state-backed" is defined, what evidentiary standard applies and who gets to decide whether an incident is treated as ordinary criminal ransomware (typically intended to be covered) or a hostile or state-linked operation (often drafted to be excluded). The practical consequence is that after a major incident, coverage can turn on contested determinations made under time pressure, with material implications for loss recovery assumptions, incident-cost visibility and how the company describes the event and its financial exposure to stakeholders.



*If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:*

Amir R. Ghavi  
1-212-318-6725  
[amirghavi@paulhastings.com](mailto:amirghavi@paulhastings.com)

Ronak D. Desai  
1-202-551-1826 / 1-212-318-6601  
[ronakdesai@paulhastings.com](mailto:ronakdesai@paulhastings.com)

Marguerite Harris  
1-202-551-1771  
[margueriteharris@paulhastings.com](mailto:margueriteharris@paulhastings.com)