The ESCP Geopolitics Institute Policy Papers, IP N° 2026-09

# Quasi-Sovereign Corporate Power: Governing critical firms in an era of geopolitical fragmentation

Wang, Ziqiao*
Oberhauser, Marc**

ESCP Business School

**Abstract**

In an era of geopolitical fragmentation, a small number of multinational corporations have acquired quasi-sovereign corporate power (QSCP): the capacity to shape national security outcomes through direct control over non-substitutable technologies and infrastructures. Unlike traditional corporate political influence, QSCP enables firms to arbitrate access to strategic systems, shape deterrence dynamics, and influence interstate conflict without formal political authority or democratic accountability.

This paper argues that QSCP represents a structural governance gap in the international system. Existing regulatory, legal, and security frameworks, designed for either sovereign states or conventional market actors, are ill-equipped to manage firms whose assets have become integral to warfighting, deterrence, and strategic stability. The paper outlines a five-step governance logic for national governments and international institutions to address this emerging challenge, aiming to reduce systemic risk while preserving innovation and resilience.

Keywords: Sovereignty; Power; Governance; Policy; Techno-nationalism

* Doctoral Researcher, ESCP Business School
**Professor, ESCP Business School

# Quasi-Sovereign Corporate Power: Governing Critical Firms in an Era of Geopolitical Fragmentation

In recent years, geopolitical power has increasingly diversified away from traditional state institutions and towards of a small number of multinational corporations that control critical technologies and infrastructures. Satellite communication networks, leading-edge semiconductor foundries, cloud platforms, and software ecosystems have become central to military operations, economic resilience, and national security, due to their non-substitutability (Farrell & Newman, 2019).

This development poses a fundamental challenge to existing governance frameworks. While states remain formally sovereign, their capacity to act increasingly depends on private firms whose assets are deeply embedded in strategic systems. Decisions taken by corporate executives about service provision, technological deployment, or investment location can now shape conflict dynamics, deterrence credibility, and diplomatic bargaining. These firms' strategic importance is underscored by the Global Risks Report 2026, which identifies 'geoeconomic confrontation' as a top global risk. Including the weaponization of supply chains and dependencies of pivotal corporate actors (World Economic Forum, 2026).

This ESCP policy paper introduces the concept of quasi-sovereign corporate power (QSCP) to capture this emerging reality. QSCP refers to the ability of certain firms to exercise state-like influence over geopolitical outcomes through enforceable control over non-substitutable, systemically embedded assets, without possessing formal political authority or democratic accountability (Wang & Oberhauser, 2025). The paper argues that QSCP constitutes a structural governance gap in the international system and outlines policy options for addressing it.

## Quasi-sovereign corporate power: A new governance challenge

Corporate involvement in geopolitics is not new. Historical cases, from colonial trading companies to Cold War-era multinationals, demonstrate that firms have long influenced diplomacy and state behaviour (Bucheli & DeBerge, 2024). This structural entanglement has been a global historical norm. In the United States, Gilded Age financial dynasties such as the House of Morgan functioned as quasi-sovereign anchors, famously intervening to stabilize the federal government's gold reserves during the Panic of 1895 (Chernow, 2001). In Japan, the state-directed modernization and military expansion of the Meiji era relied heavily on family-controlled zaibatsu conglomerates, notably Mitsui and Mitsubishi. Similarly, the profound symbiosis between political authority and private commerce has deep roots in China, exemplified by the Cohong merchants and the state-supervised *guandu shangban* (official supervision and merchant operation) enterprises of the late Qing dynasty (Jones, 2005). Consequently, modern firms do not operate in a purely apolitical environment and remain subject to state countervailing powers such as regulation and public procurement. Yet these earlier forms of corporate power were typically contingent and substitutable. States could nationalize assets, replace suppliers, or reassert control when political or security imperatives demanded it.

QSCP represents a qualitatively different phenomenon. It does not imply that firms completely escape the political authority of states. Rather, their contemporary power is not rooted merely in lobbying, resource extraction, or privileged political access, but in real-time

operational control over non-substitutable systems that are structurally embedded in military, economic, and informational architectures. When such systems are disrupted or withdrawn, entire operational domains can degrade rapidly, even collapse. In these contexts, firms do not merely influence political environments; they help constitute them. This shift reflects a broader reallocation of strategic authority in the international system. In critical domains such as satellite communications, advanced semiconductor manufacturing, cloud infrastructure, and other digitally mediated systems, states increasingly depend on privately owned and operated assets that cannot be readily replaced in the short- to medium-term. As a result, decisions taken by corporate actors, regarding service continuity, technological deployment, or investment location, now carry direct consequences for military effectiveness, economic resilience, and diplomatic leverage. Unlike traditional corporate political influence and corporate diplomacy (Li et al., 2022), this power is exercised not through persuasion or advocacy but through operational control over infrastructures upon which states themselves rely.

The rise of QSCP exposes a growing mismatch between where strategic power resides and how it is governed. International law remains largely state-centric, offering limited guidance on the responsibilities of private actors whose actions shape conflict dynamics or deterrence credibility. Security planning often assumes reliable access to critical systems without corresponding command authority or continuity guarantees. At the same time, democratic accountability mechanisms are strained when decisions with profound public consequences are taken by unelected corporate actors operating under commercial, and sometimes political, imperatives. This situation does not reflect a deliberate erosion of sovereignty, but rather an unintended governance gap created by the rapid concentration of strategic capabilities in private hands.

Leaving QSCP largely ungoverned introduces significant systemic risks. In crisis situations, unilateral corporate decisions, whether driven by legal uncertainty, financial pressure, or leadership discretion (such as Elon Musk's decisions regarding Starlink connectivity), can escalate conflicts, undermine alliance commitments, or weaken national resilience. Strategic dependencies may be weaponized not only by states but also indirectly through corporate chokepoints. At the same time, blunt policy responses such as nationalization or overly restrictive regulation risk fragmenting critical infrastructures and undermining innovation. The policy challenge is therefore not whether QSCP should be governed, but how it can be governed in a manner that preserves security, economic vitality, and legitimacy.

Importantly, QSCP firms are not merely sources of vulnerability. When aligned with public objectives, they can provide essential public goods, including emergency connectivity, infrastructure resilience, and rapid response capabilities in crisis settings. The task for policymakers is not to exclude such firms from geopolitical domains, but to integrate their capabilities into governance arrangements that ensure predictability, accountability, and coordination. This requires recognizing QSCP firms as neither ordinary market actors nor sovereign authorities, but as a distinct category of strategic actors whose power must be governed where it actually resides: in the infrastructures, systems, and the dependencies that underpin contemporary geopolitics.

## A policy process for governing QSCP

For policymakers, a firm can be understood as exercising QSCP when three conditions are simultaneously met: (1) its technology or infrastructure is non-substitutable within crisis time horizons; (2) it retains operational control levers (e.g., access credentials, update

pipelines, routing rules) that allow it to enable, restrict, or disable security-relevant functions; and (3) these capabilities are embedded in state crisis decision-making and cross-border dependency structures, such that corporate choices materially constrain state action in real time. The following five-step process translates this diagnostic into concrete implications for governance.

### Identify - Focus on non-substitutability, not corporate size or sector

Not all multinational corporations pose the same governance challenge. QSCP arises where firms control non-substitutable systems whose disruption would generate immediate security, economic, or military consequences. Non-substitutability in this context differs from traditional market domination or monopoly. A monopoly describes market concentration and pricing power. Non-substitutability, by contrast, describes functional indispensability under conditions of geopolitical stress. A firm may face competitors in ordinary market conditions yet remain irreplaceable in the short term when embedded within critical infrastructures, defence systems, or tightly coupled global value chains. Over longer time horizons, states may pursue diversification, reshoring, or strategic autonomy to reduce exposure. However, within the compressed timeframe of crisis decision-making, these systems often cannot be replaced rapidly enough to prevent operational disruption. Policy responses should therefore focus on functional criteria, such as technological chokepoints, single points of failure, and systemic embeddedness, rather than firm size, nationality, or market share alone.

For instance, Starlink's relevance does not stem from SpaceX's size, but from the non-substitutability of its low-latency satellite network during wartime. Similarly, TSMC's geopolitical importance derives from its unique position in advanced semiconductor manufacturing, not from being a "tech firm" per se. The same functional logic applies beyond these cases. Microsoft's provision of systemic cloud defence and cyber threat intelligence to Ukraine in the early stages of the Russian invasion illustrates how cloud infrastructures can become security-critical. In the informational domain, large digital platforms exercise structural influence over cognitive security and political discourse, while hardware chokepoints, such as South Korea's dominance in High Bandwidth Memory chips essential for advanced AI systems (Miller, 2022), demonstrate how specific components can acquire strategic indispensability. Governments should therefore identify QSCP firms through dependency and substitutability assessments (including 'time-to-replace' metrics), rather than through blanket regulation of industries.

### Anticipate - Regulate strategically, often before markets exist

QSCP highlights the limits of reactive regulation. In some strategically sensitive and security-salient domains, governance now precedes market maturity, e.g., in quantum computing in Europe (European Commission, 2025). Likewise, US imposed export controls pre-emptively restricted advanced artificial intelligence chip architectures well before widespread commercialization, and the EU's ex ante security screenings for foundational artificial intelligence models through the AI Act. Emerging technologies with anticipated security impact are increasingly regulated, restricted, or "weaponized" long before they reach commercial scale (National Intelligence Council., 2021). Our research evidence shows that export controls, investment and security screening, and strategic classification might be imposed years before market-ready products exist, based purely on expected geopolitical relevance. Policymakers should adopt such anticipatory governance approaches, regulating QSCP-relevant technologies early based on projected strategic

impact rather than current market penetration. Such early engagement helps prevent technological lock-ins, in which corporate indispensability becomes structurally entrenched before public authorities have the opportunity to shape governance conditions.

### Constrain - Nationalization is not a viable solution; continuity is

When confronted with strategic dependence on private firms, nationalization is often proposed as a remedy. In the context of QSCP, however, nationalization rarely resolves the underlying problem and may exacerbate it. Strategic infrastructures such as semiconductor fabrication ecosystems or global satellite constellations are transnational, technologically complex, and deeply embedded in global networks. Nationalizing a semiconductor foundry does not recreate the tacit knowledge, supplier networks, and global customer integration that make firms like TSMC indispensable. Rather than prioritizing ownership, policymakers should focus on governance instruments that preserve functionality. These instruments must encompass both legally binding regulations and set targeted guardrails that establish strict continuity obligations, crisis-time service guarantees, and coordinated contingency planning across jurisdictions. Containment strategies that do not address functional replacement or continuity risks may increase systemic vulnerability rather than reduce it.

### Command - Integrate QSCP firms into security governance

QSCP firms already function as de facto security actors. Treating them solely as regulated entities ignores their operational role in crisis response, deterrence, and infrastructure resilience. Effective governance, therefore, requires structured integration into security planning rather than exclusion or ad hoc engagement. Starlink's coordination with U.S. and Ukrainian authorities during the Russia–Ukraine war was largely improvised under crisis conditions. TSMC's role in Taiwan's deterrence posture, by contrast, is embedded in long-term strategic coordination with allied governments. However, leverage over QSCP firms is not evenly distributed. Home states possess structural advantages, while dependent states, particularly non-domiciled governments, face asymmetric exposure. In such contexts, countervailing leverage must be generated collectively or institutionally. This can include coordinated market access conditionality, joint procurement frameworks, interoperability requirements, regulatory harmonization, and strategic investment screening. Over time, diversification and capability development can reduce dependency; in the short term, formalized crisis protocols and continuity obligations can mitigate vulnerability. Governments should therefore establish formal public–private security interfaces for QSCP firms, including crisis protocols, continuity guarantees, information-sharing arrangements, and (where appropriate) supervised 'break-glass' procedures that clarify who can do what, and under which oversight, when systems become security-critical.

### Protect – Human security is part of governing QSCP

QSCP governance must extend beyond infrastructure and systems to include human security. Executives and critical employees, such as engineers and operators of critical infrastructures, of QSCP firms increasingly operate in environments where corporate decisions intersect directly with armed conflict and geopolitical coercion. A recently foiled Russian plot to assassinate the CEO of a major arms manufacturer supplying Ukraine illustrates that corporate leaders can become strategic targets when firms are embedded in security conflicts (Bo Lillis et al., 2024). Risk management frameworks should therefore

expand to include personnel protection, crisis communication, and coordination between corporate security and state authorities. Governing QSCP is not only about managing power but also about safeguarding those who operate strategic chokepoints. Governance frameworks must therefore expand to address the de facto security exposure of corporate personnel operating strategic infrastructures analogous to those afforded to diplomatic or other strategically protected civilian actors. Typically, the respective home governments of individuals are required to protect their citizens, but in geopolitically relevant cases, collaboration between allies or the country where critical operations reside provides this protection. In the case of the foiled plot, US intelligence services, shared their information with the Germans, whose security service were then able to protect the targeted executive. Importantly, extending state-backed security establishes a mutual security pact. This dynamic effectively grants the protecting state reciprocal leverage to demand corporate cooperation during geopolitical crises.

## Conclusion

QSCP has moved from the margins to the centre of contemporary geopolitics. As control over non-substitutable technologies and infrastructures increasingly shapes security, deterrence, and economic resilience, the boundary between state authority and market activity has become fundamentally blurred. The key challenge for policymakers is no longer whether corporations exercise geopolitical influence, but how this power can be governed in ways that uphold security, legitimacy, and democratic accountability. Considering the global footprint of these corporations, strictly national controls remain insufficient and prone to regulatory arbitrage and will therefore require robust transnational coordination and governance through transnational organizations.

This paper has argued that addressing QSCP requires a shift from reactive responses to a more structured governance logic. The suggested five-step governance process—identify, anticipate, constrain, command, protect—offers a practical approach to governing the accumulation of strategic power by private actors. Importantly, this approach does not seek to curtail corporate power, nor to reassert state authority through blunt instruments. Instead, it provides a pragmatic framework for governing power where it actually resides: in infrastructures, dependencies, and operational decision-making. As geopolitical fragmentation deepens and technological competition accelerates, the ability of governments to apply this logic consistently will shape not only the stability of critical systems but also the future balance between private power and public authority in the global order.

## References

Bo Lillis, K., Bertrand, N., & Pleitgen, F. (2024, July 11). *Rheinmetall: US and Germany foiled Russian plot to assassinate Armin Papperger CEO of arms manufacturer sending weapons to Ukraine*. CNN Politics. https://edition.cnn.com/2024/07/11/politics/us-germany-foiled-russian-assassination-plot

Bucheli, M., & DeBerge, T. (2024). Multinational enterprises' nonmarket strategies: Insights from History. *International Business Review*, *33*(2), 102198. https://doi.org/10.1016/j.ibusrev.2023.102198

Chernow, R. (2001). *The house of Morgan: An American banking dynasty and the rise of modern finance*.

European Commission. (2025, October 31). *Quantum | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/quantum

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International security. *International Security, 44*(1), 42–79. https://doi.org/10.5040/9780815750352.ch-002

Jones, G. (2005). *Multinationals and global capitalism: From the nineteenth to the twenty first century*. Oxford University Press.

Li, J., Shapiro, D., Peng, M. W., & Ufimtseva, A. (2022). Corporate Diplomacy in the Age of US-China Rivalry. *Academy of Management Perspectives*, *36*(4), 1007–1032. https://doi.org/10.5465/amp.2021.0076

Miller, C. (2022). *Chip war: The fight for the world's most critical technology*. Simon & Schuster.

National Intelligence Council. (2021). *Global Trends 2040: A More Contested World*. https://www.dni.gov/files/images/globalTrends/GT2040/GlobalTrends_2040_for_web1.pdf

Wang, Z., & Oberhauser, M. (2025). From Corporate Diplomacy to Quasi-Sovereign Corporate Power: Geopolitical Competition and the Reshaping of the Global Order. In *Impacts of Geoeconomics and Geopolitics on International Business* (pp. 1–41). https://doi.org/10.4018/979-8-3373-1265-1.ch001

World Economic Forum. (2026). *The Global Risks Report 2026* (Vol. 21).