

#48 Beyond Borders: Chinese Use of Foreign Interference Tactics in Dutch Strategic Industries

Authors: Benedetta Girardi and Hans Horan, Contributor: Alexander Krabbendam

July 2026

Key Takeaways

- Chinese foreign interference in Dutch strategic industries is systemic, long-term, and cumulative, eroding technological leadership, economic independence, and strategic autonomy rather than operating as isolated incidents.
- Beijing aims to acquire foreign technology, influence supply chains and gain strategic leverage over foreign policy.
- Interference exploits openness, digitalisation, and economic interdependence, using a coordinated toolkit of economic statecraft, cyber espionage, legal pressure, and talent-based knowledge transfer.
- In the Netherlands, the semiconductor sector faces very high risk, maritime high risk, and aerospace moderate-to-high risk of Chinese foreign interference.
- The Dutch economic model, characterized by openness, global integration, public-private cooperation and international research collaboration, is at risk from exploitation by actors willing to exploit the margins of legality and transparency.
- Governance fragmentation and insufficient oversight of knowledge flows, talent mobility, and post-investment risks limit the Netherlands' ability to detect and counter interference effectively.
- Chinese foreign interference poses long-term risks to the three pillars of Dutch national security: strategic autonomy, governance resilience, and alliance credibility.

Recommendations

1. Establish a national coordination and intelligence-sharing architecture (Foreign Interference Council + secure platform) to close gaps between public and private actors.
2. Implement mandatory, risk-based sector-wide security standards, including tiered personnel screening focused on access to “crown jewels.”
3. Create a public-private resilience fund to reduce dependencies, replace high-risk equipment with domestic options, and support domestic and EU-aligned capacity-building.
4. Promote transparency, accountability, and international alignment by coordinating at EU and NATO-levels and informing the public through published assessments.
5. Adopt a strategy of managed interdependence with China, combining selective engagement, reciprocity, and active management of critical supply-chain dependencies.

Executive Summary

Geopolitical competition in the twenty-first century is increasingly defined by control over strategic industries, technological capabilities, and critical supply chains. In this environment, the People's Republic of China employs foreign interference as part of a broader, state-driven strategy to achieve technological leadership, reduce external dependencies, and expand geopolitical influence. For the open and innovation-driven Dutch economy, this creates significant vulnerabilities.

This report examines Chinese foreign interference in three key Dutch strategic sectors, semiconductors, maritime, and aerospace. It argues that Chinese interference is not a series of isolated incidents, but a systemic and long-term threat. Individual acts of espionage or influence may appear manageable, but their cumulative effect risks undermining technological advantage, supply-chain control, and national decision-making autonomy.

Foreign interference is defined as deliberate, covert activity aimed at influencing or exploiting political, economic, or technological systems. Unlike broader hybrid threats, it focuses on penetrating internal systems while maintaining deniability. Strategic industries are especially vulnerable due to their economic importance, dual-use nature, and global integration.

China's approach is rooted in long-term industrial strategies such as Made in China 2025 and China Standards 2035, aiming to achieve leadership in advanced technologies. Foreign interference supports three primary objectives: technological acquisition, supply-chain influence, and strategic leverage. These are pursued through a diverse toolkit, including economic coercion, cyber-enabled espionage, legal pressure, and talent recruitment programs. China has uniquely integrated these tools into a coordinated state-led innovation system, enabling rapid assimilation and re-innovation of acquired knowledge.

The report's sectoral analysis finds that semiconductors present the highest strategic risk, given their centrality to modern technology and China's continued dependence on foreign capabilities. Critically positioned Dutch firms are targeted by cyber espionage and talent-based IP transfer. The maritime sector faces high risk due to its openness and global nature, with unauthorized data access and calibrated disruption affecting logistics and NATO likely. The aerospace sector faces moderate-to-high risk, with vulnerabilities in dual-use technologies and specialised knowledge.

Each sector sees three patterns: interference exploits structural openness and interdependence; tactics are coordinated and mutually reinforcing; and fragmented governance reduces effective response. These dynamics pose long-term risks to strategic autonomy, governance resilience, and alliance credibility, particularly in crisis scenarios such as escalating US–China tensions.

The report concludes that existing policy tools, such as export controls and investment screening, are necessary but insufficient. Addressing foreign interference requires a shift toward a proactive, resilience-oriented national security approach, combining cross-sector coordination, stronger public–private cooperation, and a strategic framework for managing interdependence with China.