CKN China Kennisnetwerk

Beyond Borders:

Chinese Use of Foreign Interference Tactics in Dutch Strategic Industries

Benedetta Girardi and Hans Horan
Contributor: Alexander Krabbendam
Quality assurance: Tim Sweijs

July 2026

About the authors

Benedetta Girardi is Programme Coordinator of the HCSS Europe in the Indo-Pacific programme and Strategic Analyst at HCSS. Her primary research interests regard the geopolitics and geoeconomics of the Indo-Pacific, European defence and security policy, and the interactions and ties between Europe, China, and the United States. Her research focuses on Europe's role in the Indo-Pacific, with particular attention to energy, critical raw materials, and semiconductor supply chains, as well as avenues for engagement between European and Indo-Pacific states.

Hans Horan is a Strategic Analyst at the Hague Centre for Strategic Studies (HCSS), specialising in the Indo-Pacific, cyber threat intelligence, and security and defence affairs. Prior to joining HCSS, Hans worked for over seven years in the intelligence and security industry, serving both private and public sector organisations across the globe as their Lead Cyber Intelligence and Principal Asia-Pacific Analyst.

Alexander Krabbendam is a recent Erasmus Mundus Master's graduate in European Politics, where he studied in the Czech Republic, Poland, and the Netherlands. He wrote his thesis on the role of emotions and normative inconsistency in European foreign policy. At HCSS, Alexander researched Chinese foreign interference in the Netherlands and organised the Indo-Dutch Cyber Security School (IDCSS) 2025. Alexander is also interested in expanding youth engagement, speaking at the 2025 NATO Youth Summit in Montenegro.

This report was published under the framework agreement for the China Knowledge Network (CKN) funded by the Dutch Ministry of Foreign Affairs, for knowledge exchange with all Dutch ministries regarding policy challenges and opportunities related to China. The responsibility for the content and expressed opinions lies solely with the authors. The network is managed by the Dutch ministry of Foreign Affairs, the Netherlands Institute of International Relations 'Clingendael' and the Leiden Asia Centre.

The Netherlands Institute of International Relations 'Clingendael' is a leading independent think tank and academy on international relations. The Leiden Asia Centre is an independent research centre affiliated with Leiden University. It serves as a hub for applied academic knowledge on modern Asia.

Acknowledgements

The authors would like to thank the interviewees and Tim Sweijs for their contributions to the research of this report.

Table of Contents

Executive Summary *6*

Research Purpose and Scope **6**

Foreign Interference and Strategic Industries **7**

China's Strategic Logic **8**

China's Foreign Interference Toolkit **9**

Chinese Interference in Dutch Strategic Industries **10**

Sectoral Findings 12

Semiconductors 12

Maritime Industries 14

Aerospace 15

Cross-Sectoral Patterns 17

Implications for Dutch National Security **18**

Policy Recommendations **19**

Managementsamenvatting *26*

Ongewenste Buitenlandse Inmenging en Strategische Industrieën **27**

China's Strategische Logica **28**

Het Chinese Instrumentarium voor Ongewenste Buitenlandse Inmenging **29**

Chinese Inmenging in de Strategische Industrieën van Nederland **31**

Sectorale Bevindingen 32

Halfgeleiders 32

Maritieme industrie 34

Lucht- en ruimtevaart 35

Cross-sectorale patronen 37

Implicaties voor de Nationale Veiligheid van Nederland **38**

Beleidsaanbevelingen **39**

Introduction *46*

1. Methodology *49*

1.1 Risk Likelihood & Probability Assessment Language 53

2. Strategic insights: China's approach to foreign interference in strategic industries *55*

2.1 Foreign Interference in Strategic Industries: Concept and Scope **55**

2.2 China's Strategic Logic: Why Interference Targets Industry **57**

2.3 China's Foreign Interference Toolkit: Tools and Systemic Integration 59
2.3.1 Economic Statecraft 59
2.3.2 Digital and Information Operations 61
2.3.3 Physical Interference 64
2.3.4 Legal Pressure 66
2.3.5 Talent-based technological espionage 68

2.4 From Interference to Strategic Advantage: Chinese Systemic Integration of Interference Efforts 69

3. Chinese Interference in Dutch Strategic Industries: Sectoral Manifestations of a Systemic Challenge..... 72

3.1 The Semiconductor Sector 74
3.1.1 Motivation 75
3.1.2 Entry points 77
3.1.3 Likely interference scenarios 78
3.1.4 Strategic risk..... 81
3.1.5 Gaps and policy actions 83

3.2 The Maritime Sector 86
3.2.1 Motivation 86
3.2.2 Entry points 88
3.2.3 Likely interference scenarios 90
3.2.4 Strategic risk..... 92
3.2.5 Gaps and policy actions 94

3.3 The Aerospace Sector 97
3.3.1 Motivation 97
3.3.2 Entry points 99
3.3.3 Likely interference scenarios 101
3.3.4 Strategic risk..... 102
3.3.5 Gaps and policy actions 104

3.4 Cross-Sectoral Synthesis: Patterns of Vulnerability and Governance Challenges .. 105

4.Implications for Dutch National Security and Building Resilience Against Foreign Interference 108

4.1 Strategic implications for Dutch national security 108

4.2 Policy Recommendations 109
4.2.1 Establish a national coordination and intelligence-sharing architecture for foreign interference 110
4.2.2 Implement mandatory, risk-based sector-wide security standards 110
4.2.3 Embed foreign interference risk into industrial and innovation policy via a public–private resilience fund 112
4.2.4 Promote transparency, accountability, and international alignment 113
4.2.5 Strategically manage interdependence through selective, reciprocal & leverage-based engagement..... 114

Executive Summary

Research Purpose and Scope

Geopolitical competition in the twenty-first century is increasingly shaped not only by territorial conquest but by control over strategic industries, technological capabilities, and critical supply chains. In this environment, states seek to secure long-term economic dominance, technological leadership, and national security by influencing or dominating key industrial ecosystems. For open, innovation-driven economies, such as the Netherlands, this shift has significant implications.

This report examines how the People's Republic of China (the PRC, also known as China) employs foreign interference tactics to target strategic industries in the Netherlands. It focuses on three sectors that are simultaneously pillars of Dutch economic strength and sources of strategic vulnerability: semiconductors, maritime, and aerospace. Together, these sectors underpin national prosperity, European supply chains, and transatlantic security, while also being deeply embedded in global markets and knowledge networks.

The report has three objectives. First, it conceptualises foreign interference in the context of strategic industries and analyses China's strategic logic and interference toolkit. Second, it assesses the extent of Chinese interference and associated risks across three Dutch strategic industries through sector-specific case studies. Third, it draws out the implications of these findings for Dutch national security and proposes policy measures to enhance resilience.

The central conclusion is that Chinese foreign interference in Dutch strategic industries should be understood as a systemic, long-term threat rather than a collection of isolated incidents. While individual acts of espionage, coercion, or influence may appear manageable in isolation, their aggregate effect risks eroding the Netherlands' technological edge, economic independence, and strategic autonomy. At the same time, the Netherlands faces a structural dilemma. China is a major trading partner and a rising geopolitical power that will remain a central actor in global economic and technological systems.

In tandem, the Netherlands finds itself in the middle of an increasingly tense geopolitical landscape, as tensions between two larger powers (the US and China) continue to escalate. As such, managing this relationship, while continuing to promote and protect the Netherlands' strategic sectors and engaging with actors such as China, requires balancing continued engagement and mutual interdependence with the need to identify, mitigate, and protect against vulnerabilities that can be exploited for strategic leverage.

Foreign Interference and Strategic Industries

Foreign interference refers to deliberate, covert activities by external actors to influence, manipulate, or exploit the political, economic, or technological systems of another state. While public debate has often focused on electoral meddling or disinformation, contemporary foreign interference increasingly targets economic and technological systems, including private firms, research institutions, supply chains, and industrial infrastructure.

Foreign interference overlaps with broader concepts such as hybrid threats and grey-zone activity but remains analytically distinct. Hybrid threats describe coordinated actions across multiple domains below the threshold of armed conflict, whereas foreign interference is more narrowly focused on penetrating internal systems and decision-making processes while maintaining deniability. Its defining features are intentionality, opacity, and ambiguity, which complicate detection, attribution, and response.

Strategic industries are especially attractive targets for foreign interference. These are sectors whose capabilities, outputs, or infrastructure are essential to national security, economic resilience, and long-term geopolitical competitiveness. Their strategic value stems from their role in enabling innovation, sustaining critical supply chains, and producing technologies with dual-use applications in both civilian and military domains.

For the Netherlands, strategic industries are both a source of strength and of exposure. The Dutch economic model is characterised by openness, deep integration into global markets, close public-private cooperation, and strong international research collaboration. These features drive

innovation and growth but also create entry points that can be exploited by actors willing to operate at the margins of legality or transparency.

China's Strategic Logic

Chinese foreign interference targeting Western strategic industries is not ad hoc behaviour. It is embedded in a long-term, state-driven strategy aimed at achieving technological self-sufficiency, reducing dependence on foreign suppliers, shaping global standards, and strengthening China's military-industrial base.

Since the late 1970s, China has pursued a gradual shift from labour-intensive production toward high-value, innovation-driven sectors. This trajectory has been formalised through industrial strategies such as Made in China 2025 and China Standards 2035, which aim to elevate Chinese firms to global leadership in advanced manufacturing and emerging technologies.

However, geopolitical tensions, particularly with the United States, have increasingly constrained China's access to advanced technologies, markets, and components. Export controls, investment screening, and technology restrictions have exposed structural dependencies within China's industrial system. At the same time, rapid technological change has made intellectual property (IP), proprietary knowledge, and system integration decisive sources of competitive advantage.

In this context, foreign interference serves three interlinked objectives for Beijing:

1. **Technological acquisition:** Accelerating domestic innovation by acquiring foreign intellectual property, data, and expertise.
2. **Supply-chain influence:** Reducing vulnerability to external pressure while increasing leverage over foreign dependencies.
3. **Strategic leverage:** Shaping regulatory environments, market conditions, and political debates in ways that constrain foreign policy choices.

These objectives guide China's selective and adaptive use of interference tools across different industries and countries.

China's Foreign Interference Toolkit

China[1] deploys a broad and flexible set of foreign interference instruments. These tools are rarely used in isolation; rather, they are combined and sequenced to exploit sector-specific vulnerabilities and geopolitical circumstances.

Economic statecraft plays a central role. China leverages market access, trade dependencies, investment flows, and control over critical raw materials to influence foreign firms and governments. Over time, these practices have been formalised through legal and regulatory instruments, such as export controls, sanctions regimes, and entity lists, that explicitly link economic measures to political and security objectives.

Digital and information operations complement economic leverage. Cyber espionage targeting companies, research institutions, and supply chains enables the theft of intellectual property and sensitive data. Information operations seek to shape regulatory debates, public narratives, and market perceptions in favour of Chinese industrial interests. While their effectiveness in Western contexts varies, cyber-enabled espionage remains a persistent and high-impact tool.

Physical interference, though less common in Europe, has become increasingly salient. Incidents involving undersea cables and critical infrastructure demonstrate China's willingness to operate in the grey zone, applying pressure while maintaining plausible deniability.

[1] It should be understood that foreign interference actions are undertaken by a range of China-directed actors, ranging from state-owned companies and private companies to intelligence operations conducted by Ministry of State Security (MSS) operatives. Nevertheless, given Beijing and Chinese President Xi Jinping's top-down approach to controlling its foreign interference toolkit, the distinction between actions by alleged private citizens and those of the government becomes blurry. Moreover, this distinction is made even more opaque by the fact that MSS agents will often adopt covers as private citizens to conduct their foreign interference activities. Therefore, China will be used as the operative word to describe actions that are either state-sanctioned or directed.

Legal pressure, or lawfare, involves the strategic use of legal and regulatory frameworks to constrain foreign firms. This includes joint venture requirements, licensing regimes, and enforcement actions that can be used to extract technology, influence corporate behaviour, or punish non-compliance.

Finally, **talent-based technological espionage** constitutes a diffuse but highly effective form of interference in strategic industries. State-linked talent recruitment programmes target individuals with access to advanced knowledge, encouraging the transfer, whether voluntary or coerced, of research and IP into China's innovation system.

What distinguishes Chinese interference is not only the breadth of these tools but also Beijing's ability to integrate their outputs into a coordinated state-driven innovation ecosystem linking industry, research institutions, and the military.

As a consequence, Chinese foreign interference generates strategic risk through systemic integration. Externally acquired knowledge and data are absorbed into China's innovation system through a structured process of acquisition, analysis, assimilation, and re-innovation. This allows Chinese firms, which are often state-backed, to accelerate development, reduce research costs, and undercut foreign competitors.

Over time, this dynamic reduces China's dependence on foreign technologies while increasing foreign dependence on Chinese manufacturing capacity, components, and standards. For open economies such as the Netherlands, this creates long-term vulnerabilities that are difficult to reverse once technological leadership or supply-chain control has been lost.

Chinese Interference in Dutch Strategic Industries

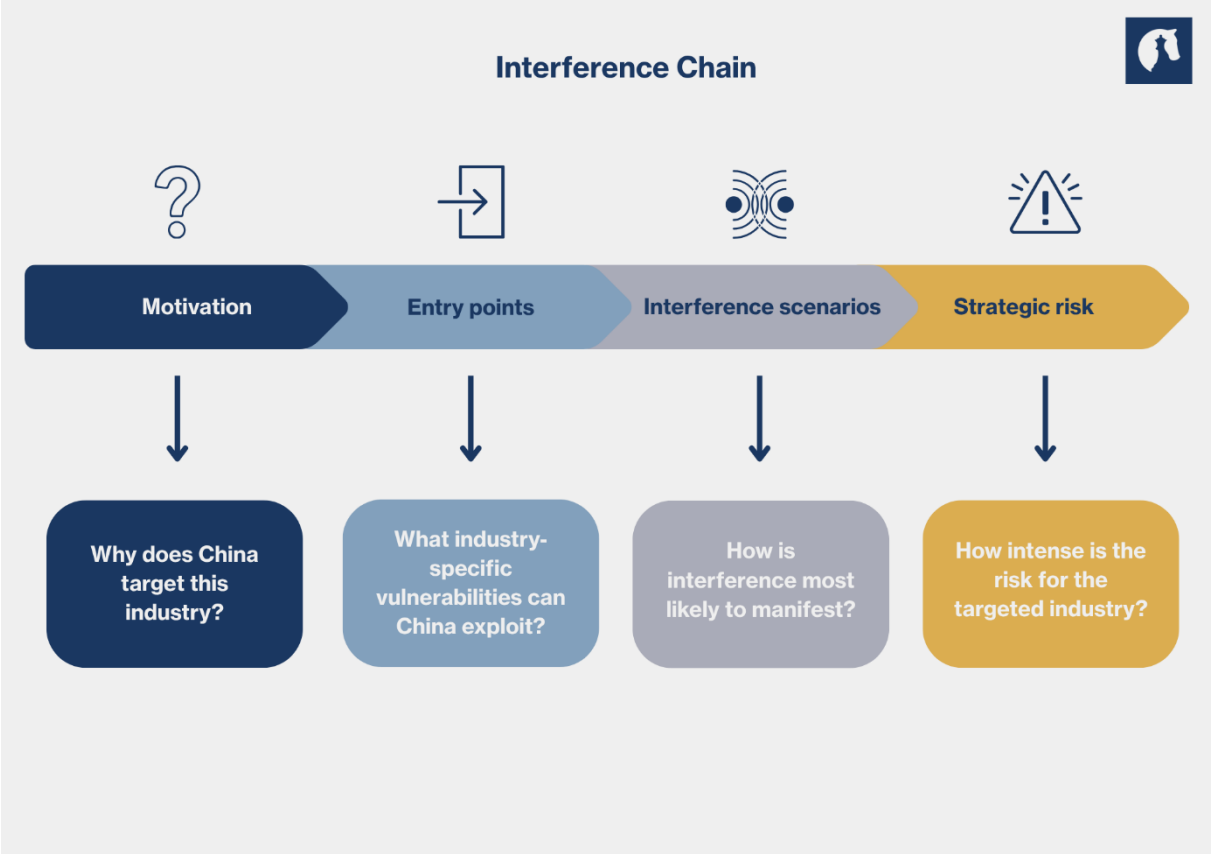
To translate these dynamics into policy-relevant insights, the report applies an Interference Chain to three case studies: the semiconductor, maritime, and aerospace sectors (see Figure 1 below).

This approach links Chinese motivations to sector-specific entry points, likely interference scenarios, and resulting strategic risks.

Risk is assessed by combining probability (composed of four indicators: strategic relevance, historical targeting, accessibility, and sector-specific vulnerabilities) and impact (operationalised through economic, technological, supply-chain, and security consequences). The report also provides an overview of current Dutch responses to foreign interference in the three strategic industries, highlights gaps, and proposes policy actions to enhance sectoral resilience.

This structured approach enables systematic comparison across sectors and highlights where intervention can most effectively disrupt interference chains. The analysis employs desk research, open-source data collection, and interviews with experts and industry professionals.

Figure 1 Interference Chain Overview



Sectoral Findings

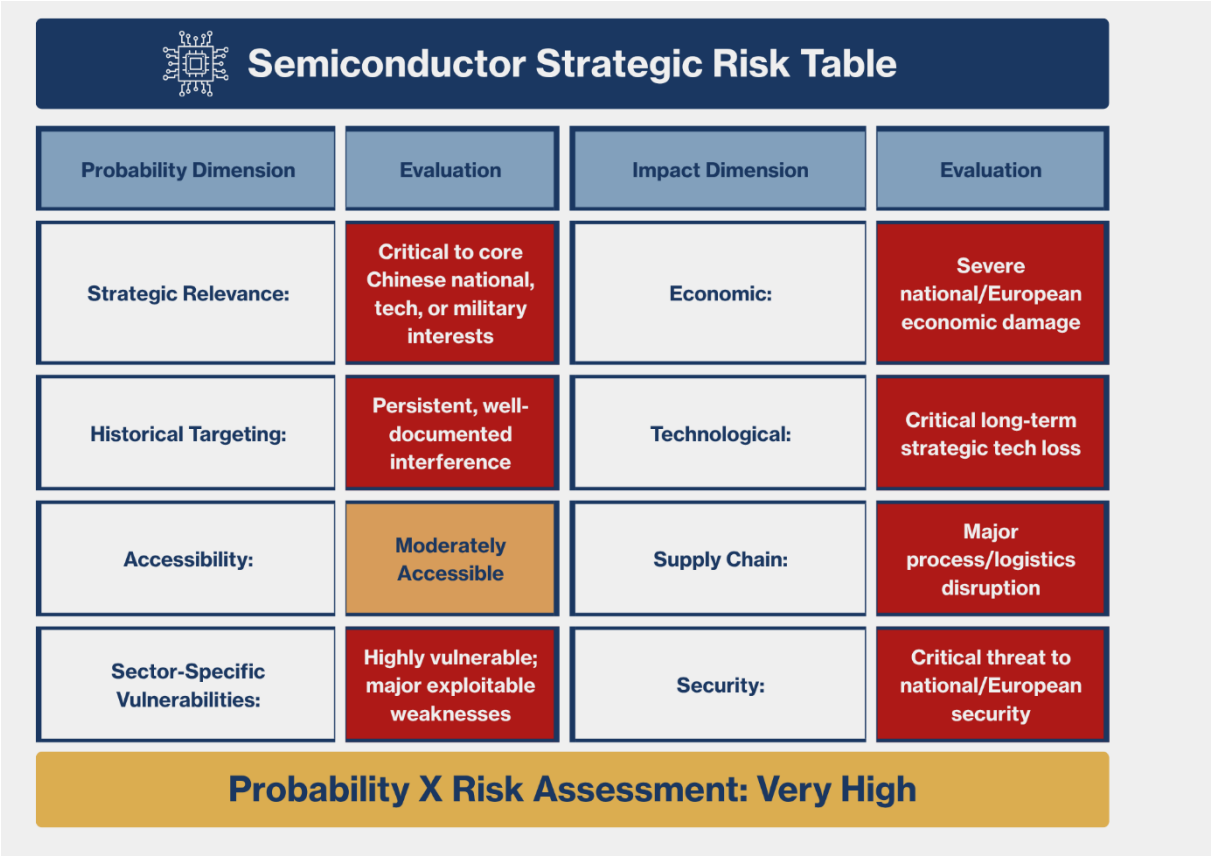
Semiconductors

The semiconductor sector represents the highest strategic risk (see Table 1 below). Semiconductors underpin virtually all modern technologies and are central to economic competitiveness and military capability. Despite massive investment, China remains dependent on foreign technology for advanced chip manufacturing. Dutch firms occupy uniquely critical positions in this ecosystem.

Strong Chinese motivation, persistent historical targeting, and high-impact consequences combine to produce a very high-risk profile. Likely forms of interference include cyber espionage, talent-based IP theft, and exploitation of dependencies on critical raw materials. While Dutch

export controls and investment screening address some risks, they remain less effective at addressing cumulative knowledge transfer and the formation of long-term dependencies.

Table 0-1 Semiconductor Strategic Risk



To enhance semiconductor sectoral resilience, the report recommends that Dutch policymakers:

1. Reinforce investment screening mechanisms
2. Develop a national semiconductor continuity strategy
3. Pursue selective industrial cooperation to shape mutual interdependence
4. Introduce high-assurance Operational Security (OpSec) certification
5. Strengthen personnel vetting for sensitive sites

Maritime Industries

The maritime sector presents a high strategic risk driven by openness, scale, and systemic importance (see Table 2). Ports, shipping, and logistics require constant interaction with foreign firms and digital systems. Chinese firms hold significant positions across global maritime value chains relevant to the Dutch maritime sector, creating opportunities for intelligence gathering and influence.

Interference is highly likely to take the form of cyber-enabled espionage, data access, and calibrated disruption rather than overt sabotage. Even limited interference will highly likely have cascading effects on energy supplies, industrial production, and NATO logistics, such as the delivery of NATO ships. Recent cybersecurity initiatives have improved resilience, but gaps remain in standardisation, intelligence sharing, and management of foreign ownership and data access.

Table 0-2 Maritime Strategic Risk

Maritime Strategic Risk Table

Probability Dimension	Situation	Impact Dimension	Situation
Strategic Relevance:	Some strategic value	Economic:	Severe national/European economic damage
Historical Targeting:	Persistent, well-documented interference	Technological:	Small setbacks
Accessibility:	Highly accessible, easy to influence	Supply Chain:	Breakdown of critical supply chains
Sector-Specific Vulnerabilities:	Significant structural weaknesses	Security:	Moderate security concerns

Probability X Risk Assessment: High with cascading effects

To enhance maritime sectoral resilience, the report recommends that Dutch policymakers:

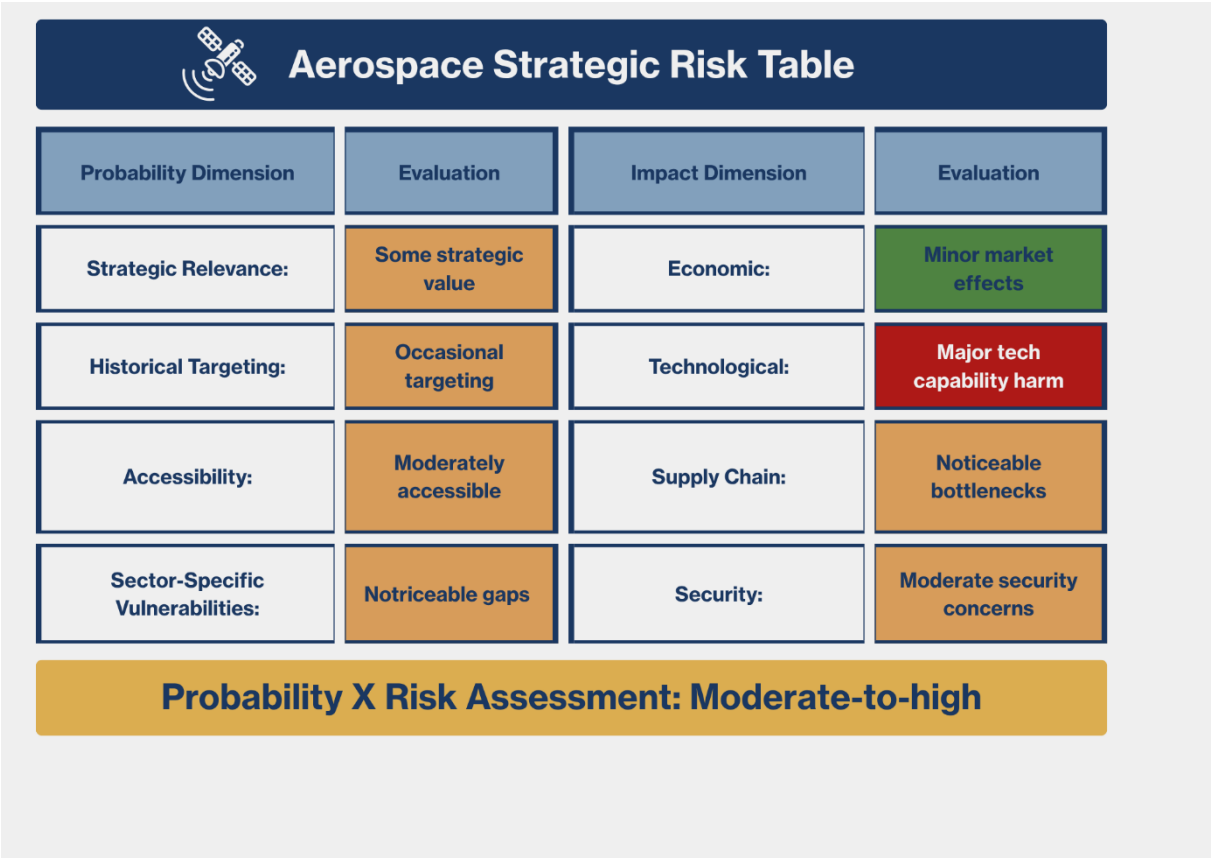
1. Mandate port cybersecurity and procurement standards
2. Launch a high-risk equipment replacement programme
3. Create a maritime intelligence sharing architecture
4. Institutionalise public–private resilience exercises
5. Reform insurance and liability frameworks

Aerospace

The aerospace sector represents a moderate-to-high risk (see Table 3). China continues to lag behind Western competitors in this sector, creating incentives to acquire foreign technology. Dutch aerospace firms and research institutions possess specialised capabilities with dual-use applications.

Likely interference focuses on talent-based espionage, cyber-enabled IP theft, and supply-chain coercion through critical raw materials. While the economic impact is less systemic than in semiconductors or maritime trade, the technological and security consequences, particularly for defence and space capabilities, are significant.

Table 0-3 Strategische Risico's voor de lucht- en ruimtevaartsector



To enhance aerospace sectoral resilience, the report recommends that Dutch policymakers to:

1. Create a national aerospace counterintelligence coordination mechanism between existing counterintelligence services and Dutch private sector leaders.
2. Set mandatory security clauses for joint ventures
3. Develop strategic material stockpiles
4. Strengthen export control enforcement and R&D safeguards
5. Centralise oversight of sensitive aerospace supply chains

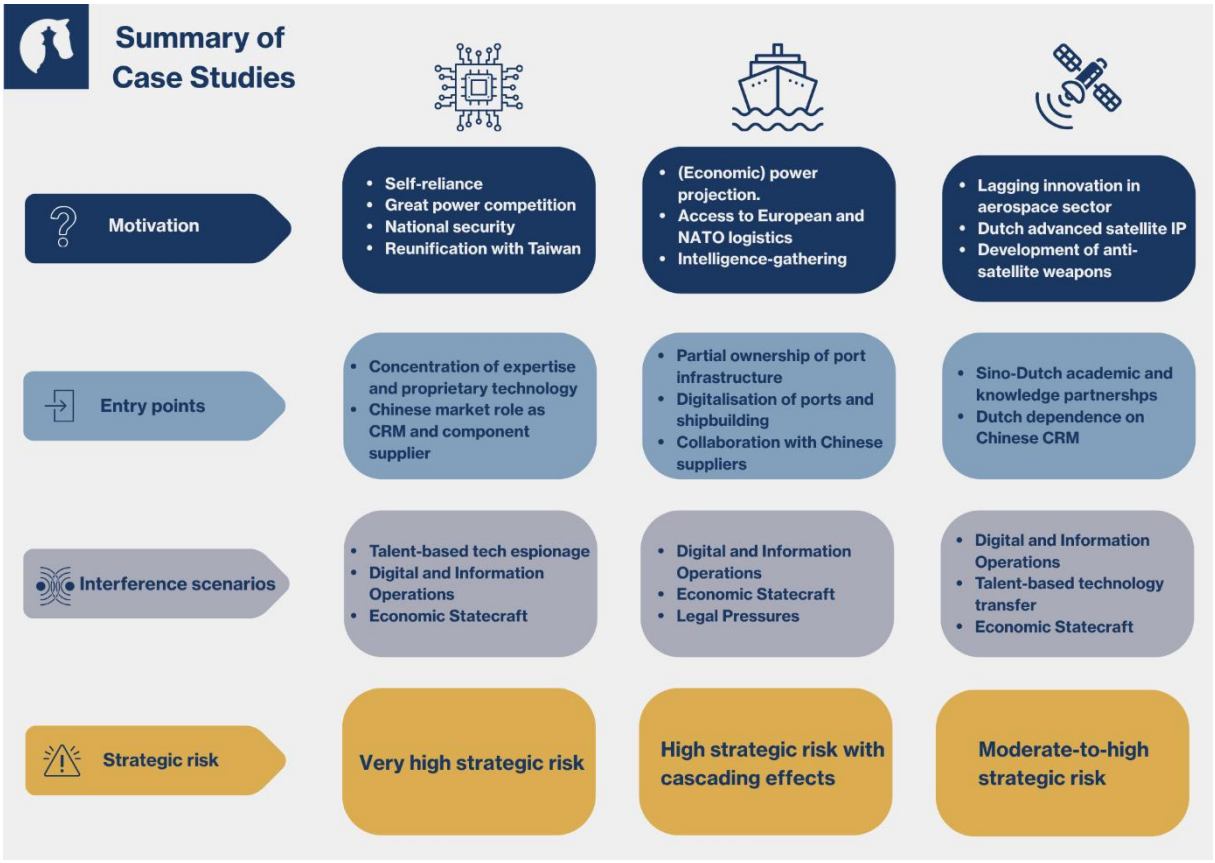
Cross-Sectoral Patterns

A comparative assessment of the three case studies reveals several recurring patterns that are central to understanding Chinese interference as a national security challenge for the Netherlands (See Figure 2 below). Across all three sectors, three common patterns emerge:

1. Chinese interference exploits openness, digitalisation, and economic interdependence.
2. Interference tactics are not operated in isolation but rather as concerted efforts pursuing an overarching objective.
3. Uncontrolled governance fragmentation limits effective detection and response.

These findings indicate that foreign interference in Dutch strategic industries constitutes a systemic challenge requiring coordinated, cross-sectoral policy responses. While sector-specific measures remain necessary, they are insufficient in themselves and should be complemented by an overarching national security approach.

Table 2 Maritime Strategic Risk



Implications for Dutch National Security

Chinese foreign interference in strategic industries poses long-term risks to the three pillars of Dutch national security: strategic autonomy, governance resilience, and alliance credibility.

Chinese interference directly undermines the Netherlands' strategic autonomy, as dependencies created through technology transfer, supply-chain exposure, or legal pressures can be leveraged in times of geopolitical tension.

In a crisis scenario, such as a heightened confrontation over Taiwan, Chinese leverage over strategic industries will likely constrain Dutch policy choices, delay military readiness, or limit participation in allied responses. The risk is not necessarily immediate disruption, but the gradual narrowing of options available to Dutch decision-makers.

Furthermore, Chinese interference exploits the defining features of the Dutch governance model: openness, decentralisation, strong public-private cooperation, and international collaboration. The exploitation of these historical strengths risks creating governance fragmentation across government, industry, and research institutions.

Lastly, Dutch strategic industries are deeply embedded in the EU and NATO systems. Interference that undermines their reliability, security, or integrity therefore has alliance-level consequences. Semiconductor tools, maritime infrastructure, and aerospace capabilities are all critical nodes in European and transatlantic security architectures.

Addressing these challenges requires a shift from reactive, transaction-based controls toward a proactive, resilience-oriented national security approach.

Policy Recommendations

Existing policy instruments such as export controls, investment screening, and cybersecurity measures are necessary but insufficient as they leave significant gaps in oversight of knowledge flows, talent mobility, informal technology transfer, post-investment and minority-stake risks, intelligence sharing between public and private actors, and cross-sectoral coordination, with the result that Dutch policy is better equipped to manage individual transactions than to counter long-term, layered Chinese interference strategies.

To enhance resilience to Chinese interference, the report concludes with 5 key policy recommendations that build on existing Dutch policy, and that should be combined with sectoral-specific interventions:

1. **Establish a national coordination and intelligence-sharing architecture for foreign interference**

The Netherlands should establish a permanent national coordination and intelligence-sharing architecture dedicated to foreign interference in strategic industries, with the purpose of closing the information gap between public and private actors and enabling timely, coordinated responses.

This architecture should combine two mutually reinforcing elements:

- A cross-sector Foreign Interference Council under the guidance of the NCTV, bringing together government, industry, academia, and civil society. The council should operate at the strategic level, with industry-specific subgroups (e.g. semiconductors, maritime, aerospace) to address sectoral risk profiles and vulnerabilities.
- A secure intelligence-sharing platform or mechanism, enabling structured, two-way information exchange between public intelligence services (AIVD/MIVD)[2], relevant ministries, and trusted private-sector actors (such as industry leaders or vetted private security and intelligence organisations).

This recommendation builds directly on the whole-of-society approach to hybrid threats articulated in the *Defensienota 2024* and aligns with the coordination role of the NCTV in a specific sub-field of foreign interference, as outlined, for instance, in the *Cybersecuritybeeld Nederland 2025*.[3] Furthermore, it addresses current capacity constraints within AIVD/MIVD by enabling companies to supplement state intelligence with vetted private intelligence capabilities, while ensuring government oversight and contextualisation.

[2] AIVD (General Intelligence and Security Service) & MIVD (Military Intelligence and Security Service)
[3] "Defensienota 2024," onderwerp, Ministerie van Defensie, Ministerie van Defensie, 2024, 130, https://www.defensie.nl/onderwerpen/defensienota; "Cybersecuritybeeld Nederland 2025," rapport, Ministerie van Justitie en Veiligheid, Ministerie van Algemene Zaken, November 26, 2025, https://www.rijksoverheid.nl/documenten/rapporten/2025/11/26/tk-bijlage-1-cybersecuritybeeld-nederland-2025

2. Implement mandatory, risk-based sector-wide security standards

Develop baseline requirements for cybersecurity, supply chain integrity, foreign investment screening, and insider threat management across all sensitive industries. Chief amongst these should be standardising a tiered employee screening process. This process will focus on ensuring that employees and researchers with affiliations with institutions known to be used by Beijing for espionage-related activities are not hired.

This tiered process should move beyond the Ministry of Justice's standard "Verklaring Omtrent Het Gedrag" (VOG or Certificate of Behaviour). This is because such VOG background checks do not account for applicants' actions, behaviours, and connections outside of the Netherlands or the European Union, which those operating at the behest of the Chinese government will have. Applicants may not be subject to a screening process solely on the basis of their ethnicity, as this would constitute discrimination under Dutch labour law. Instead, a company's tiered system should critically assess what its organisation's "crown jewels"[4] are and who has access to them.

Based on this crown jewel assessment, a tiered screening system is created, whereby those with the most direct access to these crown jewels (e.g., IT workers, C-Suite, mid-level managers, etc.) undergo a more stringent screening process based on several factors (e.g., an applicant's susceptibility to blackmail or bribery, given personal ties or financial health). In contrast, less high-profile applicants (e.g., working students or contractors) will undergo a background check that adequately reflects their seniority and level of access to the company's crown jewels.

Such policies could build on the Netherlands' *Knowledge Security Screening Bill* proposal, which is aimed primarily at academia.[5] Standards should be co-designed with the representatives from the concerned industries to balance practicality, resilience, and industry-specific needs.

[4] A company's most valuable, profitable, or strategically critical assets.
[5] "Screening for Researchers Wising to Handle Sensitive Knowledge," nieuwsbericht, Cultuur En Wetenschap Ministerie van Onderwijs, Ministerie van Algemene Zaken, April 7, 2025, https://www.government.nl/latest/news/2025/04/07/screening-for-researchers-wising-to-handle-sensitive-knowledge

3. **Embed foreign interference risk into industrial and innovation policy via a public–private resilience fund**

Create a funding mechanism in tandem with the EU and NATO to support the replacement of high-risk foreign equipment, e.g., server motherboards, Baseboard Management Controller, or large ship-to-shore (STS) cranes, with European-made equivalents, the diversification of suppliers within Europe, domestic capacity-building for critical technologies in the Netherlands, cybersecurity and infrastructure upgrades. This funding mechanism should be monitored and maintained by an independent subcommittee structure that includes representation from relevant ministries and industry stakeholders (e.g., Internal Affairs, Defence), as well as intelligence and security services.

This funding mechanism should build on the previous two recommendations by using the threat assessments to identify where structural vulnerabilities exist and where money can be most effectively invested. The funding should also, as far as possible, align with EU- and NATO-level initiatives (e.g., the EU Chips Act and CRM strategies) to ensure Europe-wide resilience and to ensure that the Netherlands maintains interoperability with its EU and NATO partners.

Given the rapidly shifting geopolitical landscape, this fund should also include a surge capacity function that activates during crises (e.g., trade sanctions, severe cyber campaigns). A predefined set of escalation triggers would unlock accelerated procedures and additional tranches of funding to help prevent significant economic damage to the Netherlands' strategic industries.

The fund's independent governing body should regularly review (e.g., every 1-2 years) strategic priorities and adjust funding priorities based on factors such as the pace of technological change, geopolitical conditions, and risk appetites.

This mechanism would complement existing initiatives such as Project Beethoven, a €2.5 billion government-supported effort to strengthen semiconductor production capacity in the Netherlands, and the Defence Industrial Strategy. A built-in surge capacity should enable

accelerated funding and procedures during crises (e.g., sanctions escalation or severe cyber campaigns).

4. Promote transparency, accountability, and international alignment

To reinforce democratic oversight and international coherence, the Netherlands should publish regular, non-classified assessments of trends in foreign interference, building on the Cybersecuritybeeld Nederland model.[6] These assessments should also build upon the EU and NATO's standards (e.g., Articles 2 and 3), programmes, and resilience efforts (e.g., the NATO Resilience Reference Curriculum or the European Preparedness Union Strategy). In particular, these reports should inform public debate without compromising sensitive sources.

At the international level, the Netherlands should actively promote coordination within the EU and NATO on investment screening, critical technology procurement, supply chain security, incident response, and sanctions alignment. This can be achieved by furthering existing cooperation between the Dutch government and industry with multilateral dedicated fora such as the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

Domestically, compliance with resilience measures should be incentivised through procurement preferences, insurance mechanisms, and recognition schemes, rather than relying solely on enforcement. These measures would complement existing initiatives and Dutch societal and military resilience policies, such as the December 2025 Letter to the House of Representatives on the Netherlands' resilience and preparedness against hybrid and military threats (e.g., de Wet weerbaarheid kritieke entiteiten or Cyberbeveiligswet).[7]

[6] NCTV, "Cybersecuritybeeld Nederland 2025," NCTV, accessed March 17, 2026, https://www.nctv.nl/onderwerpen/c/cybersecuritybeeld-nederland

[7] Ruben Brekelmans et al., "Kamerbrief Weerbaarheid En Militaire Paraatheid Tegen Hybride En Militaire Dreigingen," Rijksoverheid, December 12, 2025, https://www.rijksoverheid.nl/documenten/kamerstukken/2025/12/12/tk-kamerbrief-weerbaarheid-en-militaire-paraatheid-tegen-hybride-en-militaire-dreigingen

5. Strategically manage interdependence through selective, reciprocal and leverage-based engagement

The Netherlands should complement its defensive resilience measures with a strategy of *managed interdependence* vis-à-vis China, aimed at preserving economic benefits while reducing asymmetric dependencies and coercion risks. In addition, the Netherlands, in combination with the EU, should also look to move beyond viewing this relationship as one-sided in nature and seek to be more proactive in its approach towards China. Indeed, as highlighted in the case studies, China still maintains numerous dependencies on Dutch and EU businesses in sectors such as aerospace and semiconductors, allowing these players to act from a position of strength instead of weakness. This approach builds directly on existing Dutch policy that recognises both the necessity of engagement with China and the risks associated with unmitigated dependence.[8]

Operationally, this two-fold approach would first entail:

- Identifying and explicitly delineating "safe-to-engage" domains where cooperation with Chinese actors poses limited national security risk, such as climate mitigation technologies, basic research with low dual-use potential, public health, and international standards-setting. Providing clarity on these domains would reduce uncertainty for industry and academia and prevent over-securitisation.
- Embedding reciprocity and risk-awareness into economic and innovation policy. Engagement should be conditional on minimum standards regarding market access, IP protection, data governance, transparency of ownership, and the absence of state-directed interference.
    - Actively manage dependencies by mapping and controlling critical nodes in value chains. Dutch and European actors should retain control over key stages such as system integration, design, certification, software, and servicing, even when Chinese inputs are involved. Systematic mapping of sectoral dependencies and vulnerabilities should inform investment screening, procurement policy, export control calibration, and diplomatic

[8] *Kamerbrief Open Strategische Autonomie* (Ministerie van Buitenlandse Zaken, 2022), https://open.overheid.nl/documenten/ronl-5b134a1ba15379fdfc6ecb0b6dcc431843087193/pdf?utm.

engagement, ensuring that security and economic objectives are coherent and mutually reinforcing.

In tandem, the Netherlands and its EU partners would:

- Maintain its reverse dependencies vis-à-vis China by improving their strategic sectors, such as aerospace or semiconductors, launching programmes to support the further development of skills, such as engineering in high-technology, and the business environment required to maintain their competitive edge over Chinese businesses.
- Instituting an export measurement control for technology, components or other aspects related to these actors' critical sectors. In contrast to an export control mechanism, which would restrict trade to Chinese partners, this trade mechanism should be targeted at maintaining a strict overview of which critical technologies or components, including dual-use technology, are being sent to Chinese actors and/or their known partners. Such a mechanism would allow the Hague and Brussels to maintain an overview and track record of where Beijing's interests currently are vis-à-vis Europe's strategic innovations, how this is evolving, and act as an early warning signal if Beijing is becoming less dependent on them. For the success of this mechanism, the Hague and Brussels would need to either limit or maintain a similar overview process for key technologies that Beijing acquires through other trade mechanisms, such as "Greenfield Investments".[9]

By embedding engagement with China within a structured framework of reciprocity, transparency, and dependency management, the Netherlands can move from a reactive posture to a more confident, strategic, and proactive approach. This approach reinforces national resilience not only by reducing exposure to interference, but also by preserving room for manoeuvre and leveraging the Netherlands' economic strengths in an increasingly competitive geo-economic environment.

[9] Erik Canton and Irune Solera, *Greenfield Foreign Direct Investment and Structural Reforms in Europe: What Factors Determine Investments?*(European Commission, 2016), https://economy-finance.ec.europa.eu/document/download/74b8b7d0-c56c-4306-825c-c55d5b0d68b3_en?filename=dp033_en.pdf&prefLang=pl

Managementsamenvatting

Geopolitieke concurrentie in de eenentwintigste eeuw wordt niet alleen meer bepaald door territoriale expansie maar steeds meer door controle over strategische industrieën, technologische capaciteiten, en kritieke toeleveringsketens. In deze context streven staten ernaar om hun langdurige economische dominantie, technologische voorsprong en nationale veiligheid veilig te stellen door invloed uit te oefenen op, of controle te verkrijgen over, essentiële industriële ecosystemen. Voor open, op innovatie gerichte economieën zoals Nederland, heeft deze verschuiving grote gevolgen.

Dit rapport onderzoekt hoe de Volksrepubliek China (de PRC, hierna China) strategieën van ongewenste buitenlandse inmenging (OBI) inzet om strategische industrieën in Nederland te beïnvloeden. De focus ligt op drie sectoren die tegelijkertijd zowel de pijlers zijn van de Nederlandse economie als de bron van strategische kwetsbaarheid: de halfgeleiders-, maritieme en lucht- en ruimtevaartindustrie. Deze sectoren dragen bij aan de nationale welvaart, vormen de ruggengraat van Europese toeleveringsketens en trans-Atlantische veiligheid, en zijn bovendien diep verweven met internationale markten en kennisnetwerken.

Het rapport kent drie doelstellingen. Ten eerste schetst het een begrippenkader rond buitenlandse inmenging in strategische sectoren en analyseert het de strategische drijfveren en het instrumentarium van China in deze context. Ten tweede brengt het aan de hand van drie sectorspecifieke casussen de aard en omvang van Chinese inmenging en de daaraan verbonden risico's in drie Nederlandse strategische sectoren in kaart. Ten derde worden de implicaties van deze bevindingen voor de Nederlandse nationale veiligheid besproken en worden beleidsmaatregelen voorgesteld om de weerbaarheid te kunnen vergroten.

De centrale conclusie luidt dat Chinese OBI in strategische sectoren beschouwd moet worden als een systemische, langdurige dreiging, en niet als een reeks op zichzelf staande incidenten. Hoewel individuele gevallen van spionage, dwang of beïnvloeding op zichzelf beheersbaar lijken, kan de opstapeling ervan de technologische kansen, economische zelfstandigheid en strategische autonomie van Nederland ondermijnen. Tegelijkertijd bevindt Nederland zich in een structureel dilemma: China is enerzijds een belangrijke handelspartner en anderzijds een

geopolitieke grootmacht die blijvend centraal zal staan in wereldwijde economische en technologische systemen.

Bovendien opereert Nederland in een steeds gespannener geopolitiek speelveld, nu de spanning tussen twee grootmachten (de VS en China) verder oploopt. Het onderhouden van deze relatie, waarbij Nederland zijn strategische sectoren doorgaans blijft beschermen en tegelijkertijd de samenwerking met onder andere China moet voortzetten, vraagt om het vinden van een balans tussen blijvende economische en technologische samenwerking enerzijds en het herkennen, beperken en afdekken van kwetsbaarheden anderzijds.

Ongewenste Buitenlandse Inmenging en Strategische Industrieën

Ongewenste buitenlandse inmenging (OBI) betreft doelbewuste, heimelijke activiteiten van externe actoren gericht op het beïnvloeden, manipuleren of uitbuiten van het politieke, economische of technologische systeem van een ander land. Waar het publieke debat vaak gericht is op verkiezingsbeïnvloeding of desinformatie, richt hedendaagse OBI zich in toenemende mate op economische en technologische systemen, waaronder private ondernemingen, kennisinstellingen, toeleveringsketens en de industriële infrastructuur.

OBI overlapt met bredere begrippen als hybride dreigingen en *grey zone*-activiteiten, maar kent een analytisch onderscheid. Hybride dreigingen verwijzen naar gecoördineerde acties over meerdere domeinen uitgevoerd onder de drempel van gewapend conflict, terwijl OBI zich specifieker richt op het binnendringen van interne systemen en besluitvormingsprocessen, met behoud van ontkenbaarheid. Kenmerkend voor OBI zijn intentioneel handelen, ondoorschijnenheid en ambiguïteit, wat detectie, toerekening en reactie bemoeilijkt.

Strategische sectoren zijn bij uitstek aantrekkelijk voor OBI. Dit zijn sectoren waarvan de capaciteiten, producten of infrastructuur van cruciaal belang zijn voor nationale veiligheid, economische weerbaarheid en blijvende geopolitieke concurrentiekracht. Hun strategische betekenis ligt in het stimuleren van innovatie, het borgen van vitale toeleveringsketens en het ontwikkelen van technologieën met zowel civiele als militaire toepassingen.

Voor Nederland vormen strategische sectoren zowel een bron van kracht als van kwetsbaarheid. Het Nederlandse economische model wordt gekenmerkt door openheid, diepe integratie in wereldmarkten, nauwe publiek-private samenwerking en sterke internationale onderzoek relaties. Deze kenmerken stimuleren innovatie en groei, maar creëren ook toegangspunten die benut kunnen worden door actoren die opereren aan de randen van wettelijkheid en transparantie.

China's Strategische Logica

Chinese buitenlandse inmenging die zich richt op westerse strategische sectoren is geen ad hoc gedrag, maar maakt deel uit van een langetermijnstrategie die door de staat wordt aangestuurd. Het doel hiervan is technologische zelfredzaamheid, het verkleinen van de afhankelijkheid van buitenlandse leveranciers, het beïnvloeden van mondiale standaarden en het versterken van China's militair-industriële basis.

Sinds het einde van de jaren zeventig streeft China naar een geleidelijke verschuiving van arbeidsintensieve productie naar hoogwaardige, innovatieve sectoren. Deze koers is institutioneel geformaliseerd via industriële strategieën als Made in China 2025 en China Standards 2035, die ernaar streven Chinese bedrijven tot mondiale koplopers te maken op het gebied van geavanceerde productie en opkomende technologieën.

Verhoogde geopolitieke spanningen, met name met de Verenigde Staten, beperken echter in toenemende mate China's toegang tot geavanceerde technologieën, markten en componenten. Exportbeperkingen, investeringsscreening en technologische restricties leggen zo structurele afhankelijkheden binnen het Chinese industriële systeem bloot. Tegelijkertijd zorgt snelle technologische ontwikkeling ervoor dat intellectueel eigendom (IP), vertrouwelijke kennis en systeemintegratie doorslaggevende concurrentievoordelen zijn geworden.

Binnen deze context biedt OBI drie onderling verbonden doelen voor Peking:

1. **Technologische acquisitie:** Het versnellen van binnenlandse innovatie door het verkrijgen van buitenlands intellectueel eigendom, data en expertise.
2. **Invloed op toeleveringsketens:** Het verminderen van de kwetsbaarheid voor externe druk terwijl tegelijkertijd de eigen onderhandelingspositie, door afhankelijkheden van buitenlandse partijen, wordt vergroot.
3. **Strategische invloed:** Het beïnvloeden van reguleringskaders, marktomstandigheden en politieke discussies op een wijze die buitenlandse beleidsopties beperkt.

Samen sturen deze doelstellingen China's selectieve en flexibele inzet van beïnvloedingsmiddelen in verschillende sectoren en landen.

Het Chinese Instrumentarium voor Ongewenste Buitenlandse Inmenging

China beschikt over een breed en flexibel arsenaal aan middelen om OBI uit te oefenen. Deze instrumenten worden zelden afzonderlijk ingezet, maar juist gecombineerd en gestructureerd toegepast om in te spelen op sectorspecifieke kwetsbaarheden en geopolitieke omstandigheden.

Economisch machtsmiddelgebruik (*economic statecraft*) staat hierin centraal. China benut markttoegang, handelsafhankelijkheden, investeringsstromen en controle over kritieke grondstoffen om invloed uit te oefenen op buitenlandse bedrijven en overheden. In de loop der tijd zijn deze praktijken geformaliseerd via juridische en regulatoire instrumenten, zoals exportrestricties, vergunningseisen en entiteitenlijsten, waarbij economische maatregelen expliciet worden gekoppeld aan politieke en veiligheidsdoelen.

Digitale en informatie-operaties vormen een aanvulling op deze economische invloed. Cyberspionage die zich richt op bedrijven, kennisinstellingen en toeleveringsketens maakt diefstal van IP en gevoelige data mogelijk. Informatie-operaties proberen regulatoire discussies, publieke opinievorming en marktpercepties te sturen ten gunste van Chinese industriële

belangen. Hoewel de effectiviteit daarvan in westerse contexten uiteenloopt, blijft cyber-gebaseerde spionage een aanhoudend en impactvol instrument.

Fysieke inmenging, hoewel minder gebruikelijk in Europa, begint aan belang te winnen. Incidenten rond onderzeese kabels en kritieke infrastructuur illustreren China's bereidheid om in de *grey* zone te opereren, waar ze druk uitoefenen en plausibele ontkenning behouden.

Juridische druk, ook wel *lawfare*, betrekt zich tot het strategisch inzetten van juridische en regulatoire kaders om buitenlandse bedrijven te beperken. Dit omvat onder meer verplichte joint ventures, vergunningseisen en handhavingsacties, waarmee technologie kan worden afgedwongen, gedrag van bedrijven kan worden gestuurd, of gebrek aan naleving kan worden bestraft.

Ten slotte vormt **talentgedreven technologische spionage** een diffuse, maar uiterst effectieve vorm van OBI in strategische sectoren. Door staatsgestuurde talentenwervingsprogramma's worden personen met toegang tot geavanceerde kennis gericht benaderd, met als doel het overbrengen—vrijwillig of onder dwang—van onderzoek en IP naar het Chinese innovatiesysteem.

Wat Chinese inmenging onderscheidt, is niet enkel de breedte van het instrumentarium, maar vooral het vermogen van Peking om de opbrengsten daarvan te integreren binnen een gecoördineerd, door de staat aangestuurd innovatie-ecosysteem waarin industrie, kennisinstellingen en het leger nauw samenwerken.

Hierdoor creëert Chinese OBI strategisch risico door systemische integratie: kennis en data die extern zijn verkregen, worden via een gestructureerd proces van acquisitie, analyse, assimilatie en (her)innovatie opgenomen in China's innovatieketen. Dit stelt veelal staatsgesteunde Chinese bedrijven in staat om ontwikkeling te versnellen, onderzoeksuitgaven te beperken en buitenlandse concurrenten buiten spel te zetten.

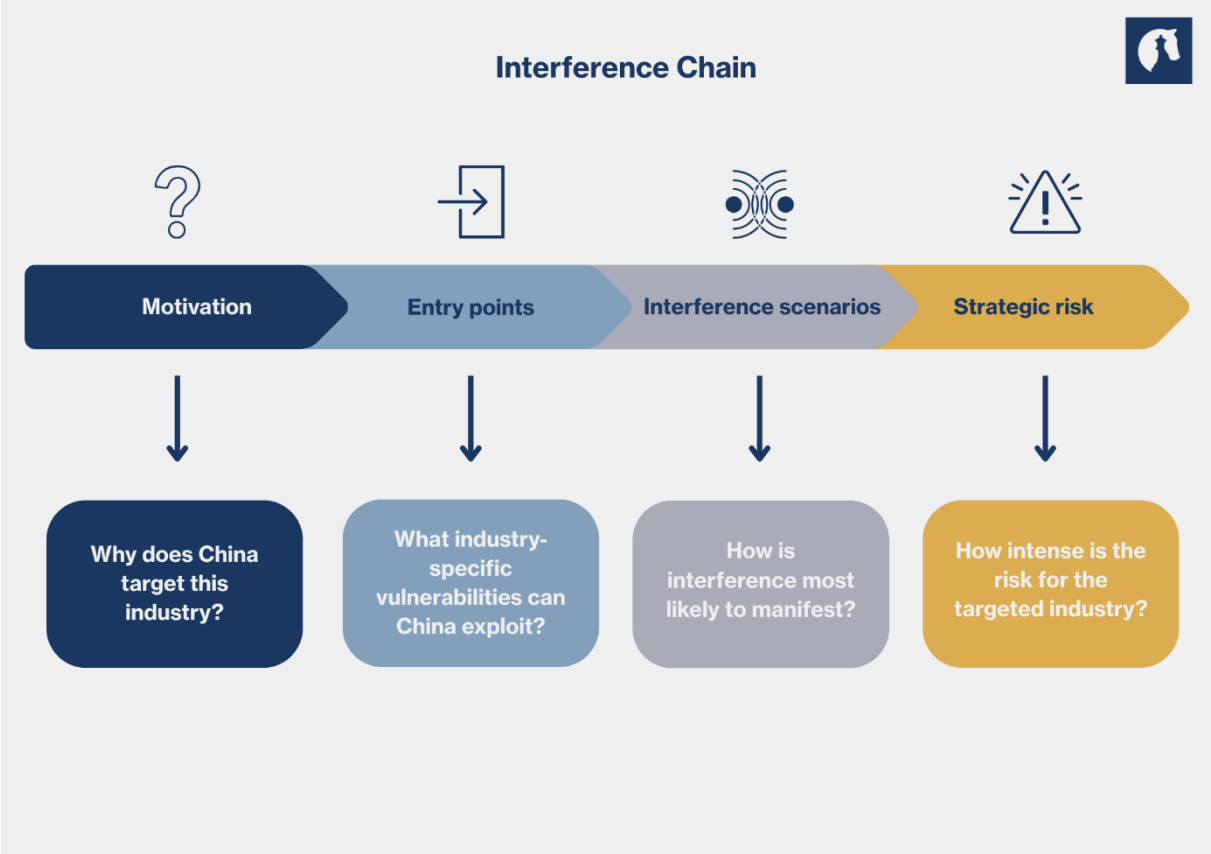
Op lange termijn vermindert deze dynamiek de afhankelijkheid van China van buitenlandse technologieën, terwijl de afhankelijkheid van andere landen van Chinese productiecapaciteit, -componenten en -standaarden juist toeneemt. Voor open economieën als die van Nederland leidt dit tot langdurige kwetsbaarheden die moeilijk terug te draaien zijn zodra technologische voorsprong of controle over toeleveringsketens eenmaal is verloren.

Chinese Inmenging in de Strategische Industrieën van Nederland

Om deze dynamieken te vertalen naar beleidsrelevante inzichten, past het rapport een zogenaamde *Interference Chain*toe op drie casussen: de halfgeleiders-, maritieme sector en lucht- en ruimtevaartsector (zie Figuur 1 hieronder). Deze benadering verbindt de Chinese motieven aan sectorspecifieke toegangspunten, waarschijnlijke inmengingsscenario's en de daaruit voortkomende strategische risico's.

De risico's worden beoordeeld door de waarschijnlijkheid (samengesteld uit vier indicatoren: strategisch belang, historische doelwitkeuze, toegankelijkheid en sectoreigen kwetsbaarheden) te combineren met de impact (geoperationaliseerd aan de hand van economische, technologische, toeleveringsketen- en veiligheidsconsequenties). Het rapport biedt daarnaast een overzicht van het huidige Nederlandse beleid ten aanzien van buitenlandse inmenging in de drie strategische sectoren, benoemt de bestaande lacunes en doet aanbevelingen voor beleidsmaatregelen om de veerkracht van de betreffende sectoren te vergroten.

Figuur 1 Overzicht Interference Chain



Sectorale Bevindingen

Halfgeleiders

De halfgeleidersector vertegenwoordigt het hoogste strategische risico (zie Tabel 1 hieronder). Halfgeleiders vormen de basis van vrijwel alle moderne technologieën en zijn essentieel voor zowel economische concurrentiekracht als militaire capaciteiten. Ondanks enorme investeringen blijft China voor geavanceerde chipproductie afhankelijk van buitenlandse technologie. Nederlandse bedrijven nemen een unieke en cruciale positie in binnen dit ecosysteem.

Hoge Chinese motivatie, aanhoudende gerichte activiteiten in het verleden en de grote impact bij succesvolle OBI zorgen samen voor een zeer hoog risicoprofiel. Waarschijnlijke vormen van OBI zijn onder meer cyberspionage, op talent gerichte diefstal van IP voornamelijk gericht op

sectorale talenten en het uitbuiten van Nederlandse afhankelijkheden van kritieke grondstoffen. Hoewel Nederlandse exportbeperkingen en investeringsscreening bepaalde risico's deels ondervangen, blijven zij toch minder effectief in het voorkomen van structurele kennisoverdracht en het ontstaan van langdurige afhankelijkheidsrelaties.

Tabel 1 Het strategische risico van halfgeleiders

Semiconductor Strategic Risk Table

Probability Dimension	Evaluation	Impact Dimension	Evaluation
Strategic Relevance:	Critical to core Chinese national, tech, or military interests	Economic:	Severe national/European economic damage
Historical Targeting:	Persistent, well-documented interference	Technological:	Critical long-term strategic tech loss
Accessibility:	Moderately Accessible	Supply Chain:	Major process/logistics disruption
Sector-Specific Vulnerabilities:	Highly vulnerable; major exploitable weaknesses	Security:	Critical threat to national/European security

Probability X Risk Assessment: Very High

Om de weerbaarheid van de halfgeleidersector te versterken, adviseert het rapport Nederlandse beleidsmakers om:

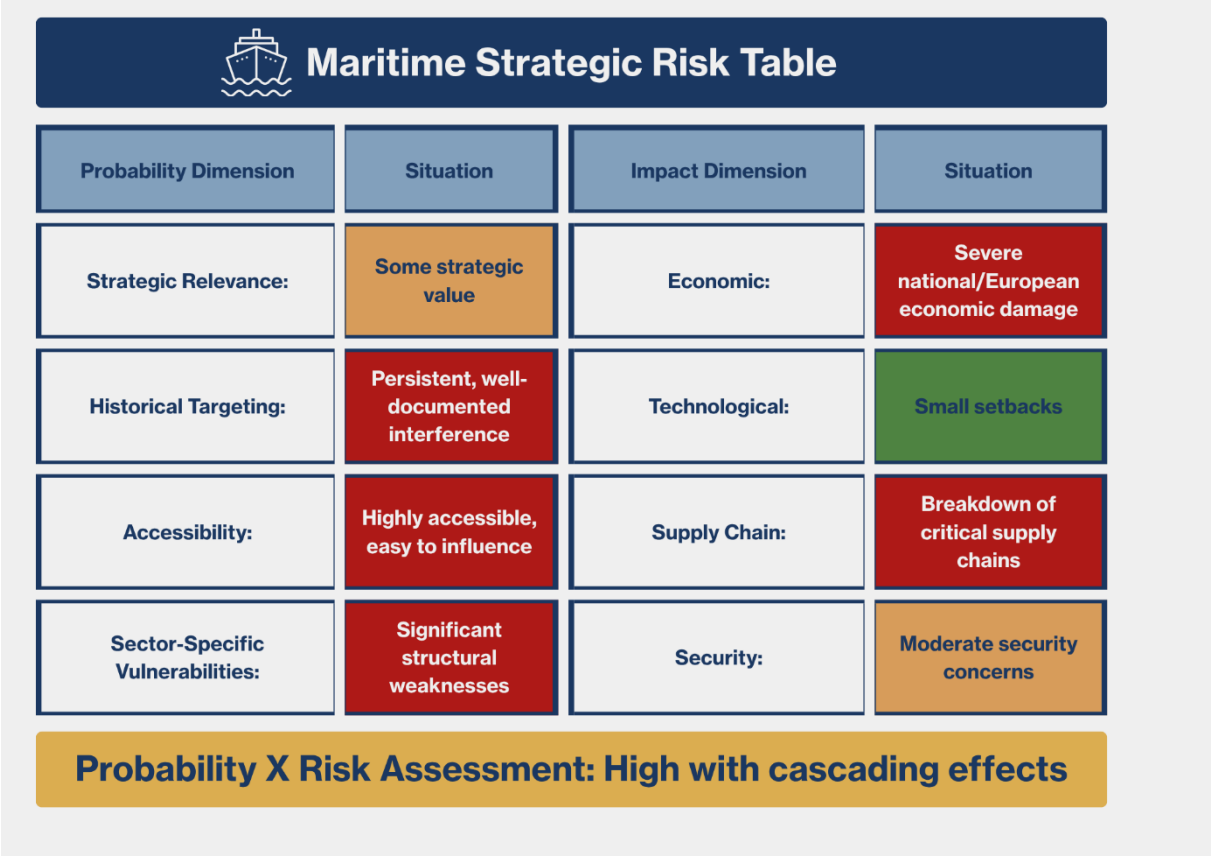
1. De mechanismen voor investeringsscreening verder te versterken
2. Een nationale continuïteitsstrategie voor de halfgeleidersector te ontwikkelen
3. Selectieve industriële samenwerking aan te gaan om wederzijdse afhankelijkheid actief te sturen
4. Certificering voor operationele veiligheid (OpSec) met hoge zekerheid in te voeren
5. De screening van personeel op gevoelige locaties te intensiveren

Maritieme industrie

De maritieme sector vormt een hoog strategisch risico door haar open karakter, schaalgrootte en systeemkritische rol (zie Tabel 2). Havens, scheepvaart en logistiek vereisen voortdurende interactie met buitenlandse bedrijven en digitale systemen. Doordat Chinese ondernemingen belangrijke posities bekleden in wereldwijde maritieme waardeketens die van belang zijn voor de Nederlandse sector, schept dit mogelijkheden voor inlichtingenvergaring en beïnvloeding.

OBI zal naar verwachting vooral plaatsvinden via cyberspionage, toegang tot data en gerichte ontregeling, eerder dan via openlijke sabotage. Zelfs beperkte OBI zal waarschijnlijk al verstrekkende gevolgen hebben voor energievoorziening, industriële productie en NAVO-logistiek, zoals de levering van NAVO-schepen. Recente initiatieven op het gebied van cyberweerbaarheid hebben de veerkracht versterkt, maar er blijven lacunes bestaan op het vlak van standaardisatie, informatie-uitwisseling, het beheer van buitenlands eigendom en data-toegang.

Tabel 2 Strategisch Risico van de Maritieme Sector



Om de weerbaarheid van de maritieme sector te vergroten, adviseert her rapport Nederlandse beleidsmakers om:

1. Verplichte normen voor cyberveiligheid en inkoop in te voeren in havens
2. Een vervangingsprogramma voor risicovolle apparatuur te starten
3. Een maritieme architectuur voor informatie-uitwisseling op te zetten
4. Publiek-private weerbaarheidsoefeningen te institutionaliseren
5. Verzekerings- en aansprakelijkheidskaders te hervormen

Lucht- en ruimtevaart

De lucht- en ruimtevaartsector kent een matig tot hoog strategisch risico (zie Tabel 3). China blijft op dit terrein achter bij westerse concurrenten, wat hen sterk aanspoort om buitenlandse

technologie te verwerven. Nederlandse lucht- en ruimtevaartbedrijven en onderzoeksinstellingen beschikken over specialistische kennis met toepassingen voor tweeërlei gebruik.

Waarschijnlijke vormen van OBI zijn onder meer op spionage gericht op talent, diefstal van IP gestuurd door cyber en druk op toeleveringsketens via kritieke grondstoffen. Hoewel de economische impact minder systeemkritisch is dan in de halfgeleider- of maritieme sector, zijn de technologische en veiligheidsconsequenties aanzienlijk, met name voor defensie en ruimtevaartscapaciteiten

Tabel 3 Strategische Risico's voor de lucht- en ruimtevaartsector

Aerospace Strategic Risk Table

Probability Dimension	Evaluation	Impact Dimension	Evaluation
Strategic Relevance:	Some strategic value	Economic:	Minor market effects
Historical Targeting:	Occasional targeting	Technological:	Major tech capability harm
Accessibility:	Moderately accessible	Supply Chain:	Noticeable bottlenecks
Sector-Specific Vulnerabilities:	Notriceable gaps	Security:	Moderate security concerns

Probability X Risk Assessment: Moderate-to-high

Om de weerbaarheid van de lucht- en ruimtevaartsector te vergroten, adviseert het rapport Nederlandse beleidsmakers om:

1. Een nationaal coördinatiemechanisme op te zetten tussen bestaande contraspionagediensten en Nederlandse marktleiders in de private sector
2. Verplichte veiligheidsclausules in joint ventures te stellen
3. Strategische voorraden van essentiële materialen aan te leggen
4. De handhaving van exportcontrole en de borging van R&D-veiligheid te versterken
5. Het toezicht op gevoelige lucht- en ruimtevaart toeleveringsketens te centraliseren

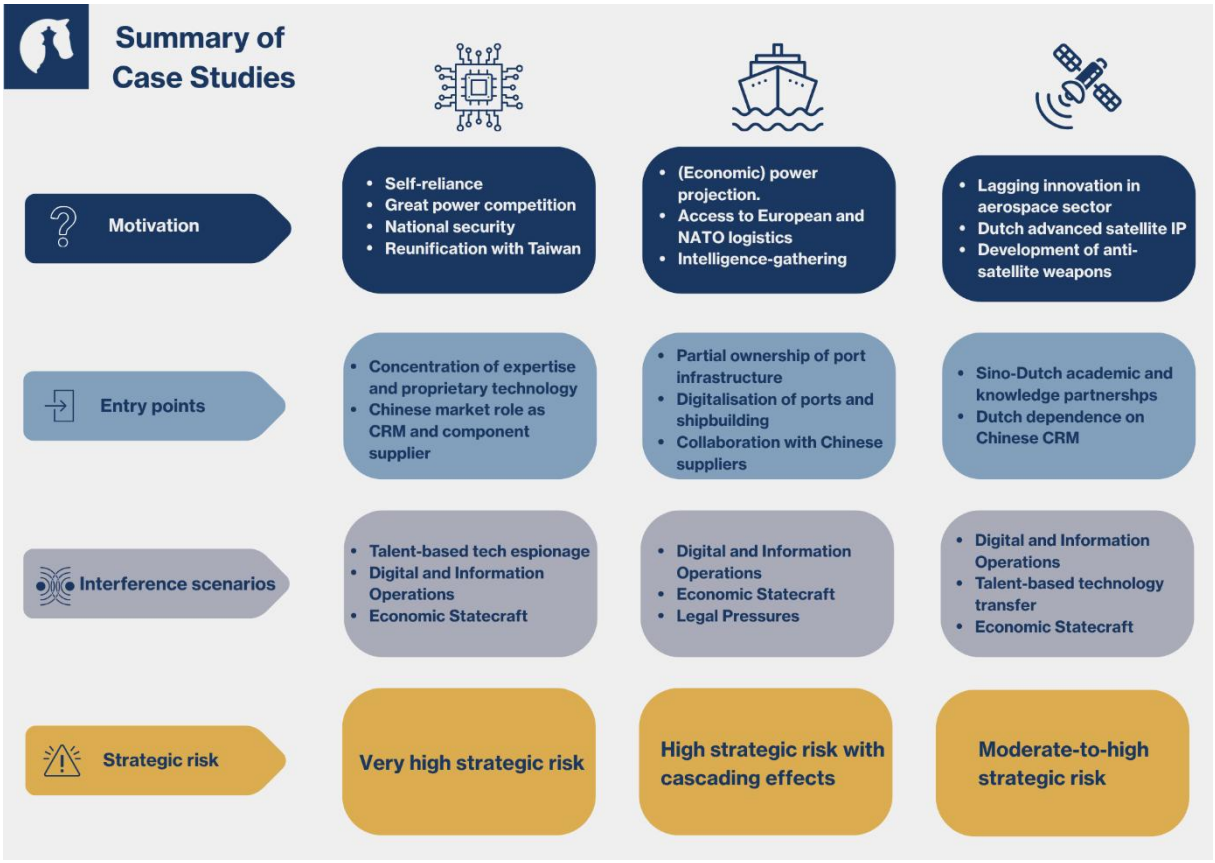
Cross-sectorale patronen

Een vergelijkende analyse van de drie casussen laat verschillende terugkerende patronen zien die essentieel zijn voor het begrijpen van Chinese OBI als een veiligheidsvraagstuk op nationaal niveau voor Nederland (zie Figuur 2 hieronder). Bij alle drie de sectoren heen komen drie gemeenschappelijke patronen naar voren:

1. Chinese OBI maakt gebruik van openheid, digitalisering en economische verwevenheid.
2. OBI-tactieken worden niet afzonderlijk ingezet, maar als gecoördineerde inspanningen met een overkoepelend doel.
3. Ongecontroleerde fragmentatie binnen de overheid belemmert effectieve detectie en respons.

Deze bevindingen geven aan dat OBI in Nederlandse strategische sectoren een systemische uitdaging vormt, die om gecoördineerde, sectoroverstijgende beleidsmaatregelen vraagt. Sectorspecifieke maatregelen blijven noodzakelijk, maar zijn op zichzelf onvoldoende en dienen te worden aangevuld met een bredere nationale veiligheidsbenadering.

Figuur 2 Samenvatting van casussen



Implicaties voor de Nationale Veiligheid van Nederland

Chinese OBI in strategische sectoren brengt op de lange termijn risico's met zich mee voor de drie pijlers van de Nederlandse nationale veiligheid: strategische autonomie, bestuurlijke weerbaarheid en geloofwaardigheid van de alliantie.

Chinese OBI ondermijnt direct de strategische autonomie van Nederland, doordat afhankelijkheden, die ontstaan via technologische overdracht, blootstelling in toeleveringsketens of juridische druk, kunnen worden uitgebuit in tijden van geopolitieke spanning.

In een crisissituatie, zoals een escalatie rondom Taiwan, zal Chinese invloed op strategische sectoren waarschijnlijk de beleidsruimte van Nederland beperken, de militaire paraatheid vertragen of de deelname aan bondgenootschappelijke reacties inperken. Het grootste risico

schuilt niet per se in acute ontwrichting, maar in het geleidelijk verminderen van de handelingsopties voor Nederlandse besluitvormers.

Bovendien maakt Chinese OBI gebruik van de kenmerken die het Nederlandse bestuursmodel juist zo typeren: openheid, decentralisatie, sterke publiek-private samenwerking en internationale samenwerking. Het uitbuiten van deze krachten riskeert de fragmentatie van toezicht en autoriteit binnen overheid, bedrijfsleven en kennisinstellingen.

Ten slotte zijn Nederlandse strategische sectoren diep verankerd in het EU- en NAVO-systeem. OBI die hun betrouwbaarheid, veiligheid of integriteit ondermijnt, heeft daarom gevolgen op het niveau van de alliantie. Halfgeleidertechnologie, maritieme infrastructuur en lucht- en ruimtevaartcapaciteiten zijn allemaal cruciale schakels in de Europese en trans-Atlantische veiligheidsarchitectuur.

Om deze uitdagingen het hoofd te bieden, is een verschuiving nodig van reactieve, op transacties gebaseerde controlemaatregelen naar een proactieve, nationale veiligheidsstrategie gericht op weerbaarheid.

Beleidsaanbevelingen

Bestaande beleidsinstrumenten zoals exportcontroles, investeringsscreenings en cybersecuritymaatregelen zijn noodzakelijk, maar ontoereikend. Ze laten aanzienlijke lacunes achter in het toezicht op kennisstromen, talentmobiliteit, informele technologische overdracht, risico's na investeringen en bij minderheidsbelangen, informatie-uitwisseling tussen publieke en private partijen en sectoroverstijgende coördinatie. Het Nederlandse beleid is hierdoor beter uitgerust om individuele transacties te beheersen dan om langdurige, gelaagde Chinese OBI-strategieën tegen te gaan.

Om de weerbaarheid tegen Chinese inmenging te vergroten, sluit het rapport af met vijf kernaanbevelingen die voortbouwen op het bestaande Nederlandse beleid en die gecombineerd dienen te worden met sectorspecifieke interventies:

1. Richt een nationale coördinatie- en intelligentiedelingsstructuur op voor OBI

Nederland zou een permanente nationale coördinatie- en intelligentiedelingsstructuur moeten oprichten, specifiek gericht op OBI in strategische sectoren. Het doel is het dichten van de informatiekloof tussen publieke en private actoren en het mogelijk maken van tijdige, gecoördineerde reacties.

Deze structuur zou uit twee onderdelen moeten bestaan die elkaar onderling versterken:

- Een sectoroverstijgende Raad voor Buitenlandse Inmenging onder regie van de NCTV, waarin overheid, bedrijfsleven, wetenschap en maatschappij samenkomen. De raad moet opereren op strategisch niveau, met sectorspecifieke subgroepen (zoals halfgeleiders, maritiem, lucht- en ruimtevaart) om sectorspecifieke risico's en kwetsbaarheden te adresseren.
- Een veilig platform of mechanisme voor intelligentiedeling, waarmee gestructureerde tweezijdige informatie-uitwisseling mogelijk wordt tussen publieke inlichtingendiensten (AIVD/MIVD), relevante ministeries en betrouwbare private actoren (zoals marktleiders of gescreende private beveiligings- en inlichtingenorganisaties).

Deze aanbeveling bouwt direct voort op de brede benadering van hybride dreigingen zoals verwoord in de *Defensienota 2024*, en sluit aan bij de coördinerende rol van de NCTV in een specifiek beleidsveld van buitenlandse inmenging, zoals uiteengezet in onder andere het *Cybersecuritybeeld Nederland 2025*. Verder biedt het een antwoord op de huidige capaciteitsgrenzen van AIVD/MIVD. Door bedrijven in staat te stellen om, onder toezicht en duiding van de overheid, private inlichtingenmogelijkheden verantwoord aan te wenden ter aanvulling van de staatsinlichtingen.

2. Voer verplichte, risico gebaseerde, sectorbrede veiligheidsstandaarden in

Stel basisvereisten op voor cybersecurity, integriteit van toeleveringsketens, screening van buitenlandse investeringen en het beheer van interne dreigingen in alle gevoelige sectoren. Centraal hierin moet zijn het standaardiseren van een gelaagd screeningsproces voor personeel. De aandacht ligt hierbij met name op het waarborgen dat medewerkers en onderzoekers met banden met instellingen waarvan bekend is dat zij door Peking worden ingezet voor spionageactiviteiten, niet worden aangenomen.

Dit gelaagde proces dient verder te gaan dan de standaard “Verklaring Omtrent Het Gedrag” (VOG) van het Ministerie van Justitie. Reden is dat VOG-controles geen rekening houden met handelingen, gedragingen of connecties buiten Nederland of de Europese Unie – juist relevante factoren bij personen die mogelijk in opdracht van de Chinese overheid opereren. Sollicitanten mogen niet uitsluitend op basis van hun etniciteit aan een screening worden onderworpen, aangezien dit als discriminatie geldt volgens de Nederlandse arbeidswetgeving. Het is daarom belangrijk dat bedrijven kritisch bepalen wat binnen hun organisatie de zogeheten “kroonjuwelen” zijn en wie daar toegang toe heeft.

Op basis van deze kroonjuwelenevaluatie wordt een screeningssysteem op verschillende niveaus ingericht. Degenen met meest directe toegang tot deze kroonjuwelen (zoals IT-medewerkers, directieleden, of middenmanagers) ondergaan een strenger screeningsproces op basis van verschillende factoren (bijvoorbeeld gevoeligheid voor chantage of omkoping, persoonlijke relaties of financiële situatie). Minder risicovolle sollicitanten (zoals werkstudenten of externe opdrachtnemers) ondergaan een achtergrondcontrole die past bij hun senioriteit en mate van toegang tot de kroonjuwelen van het bedrijf.

Dergelijk beleid kan voortbouwen op de Nederlandse voorstel *screening kennisveiligheid*, die zich primair op de academische sector richt. Standaarden dienen samen met vertegenwoordigers uit de betreffende sectoren te worden ontwikkeld om een evenwicht te vinden tussen uitvoerbaarheid, weerbaarheid en sectorspecifieke behoeften.

3. Veranker het risico van OBI in industrie- en innovatiebeleid via een publiek-privaat weerbaarheidsfonds

Stel een financieringsmechanisme in, samen met de EU en NAVO, om onder meer de vervanging van risicovolle buitenlandse apparatuur mogelijk te maken (bijvoorbeeld servermoederborden, Baseboard Management Controllers of grote ship-to-shore (STS) kranen) door Europees geproduceerde alternatieven, de diversificatie van leveranciers binnen Europa, de opbouw van binnenlandse capaciteit voor kritieke technologieën in Nederland, en investeringen in cybersecurity- en infrastructuurversterking. Dit fonds dient te worden beheerd door een onafhankelijke subcommissie waarin vertegenwoordigers van relevante ministeries en industriële belanghebbenden (bijvoorbeeld Binnenlandse Zaken, Defensie) zitting hebben, evenals de inlichtingen- en veiligheidsdiensten.

Het financieringsmechanisme moet voortbouwen op de eerdere twee aanbevelingen door dreigingsanalyses te gebruiken om structurele kwetsbaarheden te identificeren en te bepalen waar investeringen het meeste effect zullen hebben. Daarbij moet het fonds zoveel mogelijk aansluiten bij initiatieven van de EU en NAVO (zoals de EU Chips Act en strategieën omtrent kritieke grondstoffen) om Europese weerbaarheid te waarborgen en interoperabiliteit van Nederland met EU- en NAVO-partners te behouden.

Gezien het snel veranderende geopolitieke landschap dient het fonds ook te beschikken over een ‘surge capacity’-functie, die kan worden geactiveerd in crisissituaties (zoals bij handelssancties of grootschalige cyberaanvallen). Via vooraf bepaalde escalatietriggers kunnen versnelde procedures en aanvullende financieringsrondes worden ontgrendeld, om zo te voorkomen dat strategische sectoren van de Nederlandse economie ernstig geschaad worden.

Het onafhankelijke bestuur van het fonds dient strategische prioriteiten regelmatig te herzien (bijvoorbeeld elke 1 à 2 jaar) en het investeringsbeleid aan te passen op basis van factoren als het tempo van technologische ontwikkeling, geopolitieke omstandigheden en risicobereidheid.

Dit mechanisme sluit aan bij bestaande initiatieven zoals de Defensie Industrie Strategie en Project Beethoven, een door de overheid gesteund programma van €2,5 miljard om de Nederlandse productiecapaciteit voor halfgeleiders te versterken. Een ingebouwde surge-capaciteit zou het fonds in staat stellen om tijdens crises versnelde financiering en procedures mogelijk te maken (bijvoorbeeld bij een escalatie van sancties of ernstige cybercampagnes).

4. Bevorder transparantie, verantwoording en internationale afstemming

Om het democratisch toezicht en de internationale samenhang te versterken, zou Nederland op regelmatige basis openbare, niet-geclassificeerde analyses van trends in OBI moeten publiceren naar het voorbeeld van het *Cybersecuritybeeld Nederland*. Deze rapportages dienen daarnaast aan te sluiten bij de EU's en NAVO's standaarden zoals artikelen 2 en 3), programma's en weerbaarheidsinitiatieven (zoals *het NATO Resilience Reference Curriculum* of de *European Preparedness Union Strategy*). Het is daarbij van belang dat deze rapporten het publieke debat voeden, zonder gevoelige bronnen of methoden te compromitteren.

Op internationaal niveau dient Nederland actief samenwerking binnen de EU en NAVO te bevorderen op het gebied van investeringsscreening, inkoop van kritieke technologie, beveiliging van toeleveringsketens, incident response en sanctiecoördinatie. Dit kan onder meer door het versterken van bestaande samenwerking tussen de Nederlandse overheid en het bedrijfsleven via multilaterale, gespecialiseerde fora zoals het European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

Nationaal zou de naleving van weerbaarheidsmaatregelen gestimuleerd moeten worden via inkoopvoorkeuren, verzekeringsmechanismen en erkenningssystemen, in plaats van uitsluitend via handhaving. Deze maatregelen vullen bestaande initiatieven en het Nederlandse beleid voor maatschappelijke en militaire weerbaarheid aan, zoals onder andere beschreven in de Kamerbrief van december 2025 over de Nederlandse paraatheid en weerbaarheid tegen hybride en militaire dreigingen (zoals de Wet weerbaarheid kritieke entiteiten of de Cyberbeveiligswet).

5. Beheer strategisch de onderlinge afhankelijkheid via selectieve, wederkerige en op onderhandelingspositie gebaseerde samenwerking

Nederland zou zijn defensieve weerbaarheidsmaatregelen moeten aanvullen met een strategie van *gemanagede interdependentie* ten opzichte van China, gericht op het behouden van economische voordelen en het verminderen van asymmetrische afhankelijkheden en risico's op dwang. Daarnaast moeten Nederland en de EU verder gaan dan het beschouwen van deze relatie als eenzijdig en juist proactiever optreden richting China. Zoals uit de casestudies al blijkt, heeft China nog altijd aanzienlijke afhankelijkheden van Nederlandse en Europese bedrijven, bijvoorbeeld in sectoren als lucht- en ruimtevaart en halfgeleiders. Dit stelt Europese spelers in staat vanuit kracht in plaats van zwakte te opereren. Deze benadering sluit aan bij het bestaande Nederlandse beleid dat zowel het belang van samenwerking met China als de risico's van onbeheersbare afhankelijkheid erkent.

Operationeel bestaat deze tweesporenaanpak uit:

- Het identificeren en expliciet afbakenen van "veilige" samenwerkingsdomeinen waarin samenwerking met Chinese partijen slechts beperkte nationale veiligheidsrisico's met zich meebrengt – zoals klimaatmitigatietechnologieën, fundamenteel onderzoek met weinig "dual-use" potentieel, publieke gezondheidszorg en het opstellen van internationale standaarden. Duidelijkheid over deze domeinen vermindert onzekerheid voor industrie en kennisinstellingen en voorkomt overmatige securitisering.
- Wederkerigheid en risicobewustzijn centraal stellen in het economische en innovatiebeleid. Samenwerking dient afhankelijk te zijn van minimale eisen ten aanzien van markttoegang, bescherming van intellectuele eigendom, databeheer, eigendomsstructuren en het ontbreken van staatsgeleide inmenging.
- Actief sturing geven aan afhankelijkheden door kritieke knooppunten in waardeketens in kaart te brengen en te controleren. Nederlandse en Europese partijen moeten de regie houden over essentiële onderdelen zoals systeemintegratie, ontwerp, certificering, software en onderhoud, ook wanneer Chinese toeleveringen worden gebruikt. Systematische analyse van sectorafhankelijke kwetsbaarheden moet richting geven aan investeringsscreening, inkooopbeleid, exportcontrole en diplomatieke acties, zodat veiligheids- en economische doelen op elkaar zijn afgestemd en elkaar versterken.

Tegelijkertijd zouden Nederland en zijn EU-partners:

- De wederzijdse afhankelijkheid ten opzichte van China behouden door de eigen strategische sectoren, zoals lucht- en ruimtevaart of halfgeleiders, verder te versterken en programma's te starten voor ontwikkeling van relevante technische vaardigheden en van een aantrekkelijk ondernemersklimaat, om zo het concurrentievoordeel ten opzichte van Chinese bedrijven te behouden.
- Een exportmeetmechanisme instellen voor technologieën, componenten of andere aspecten van deze strategische sectoren. Anders dan bij gewone exportcontroles, die gericht zijn op restrictie van handel met Chinese partijen, is een dergelijk mechanisme bedoeld om scherp zicht te houden op welke kritieke technologieën of componenten (inclusief dual-use technologie) worden geleverd aan Chinese actoren en/of hun bekende partners. Daarmee kunnen Den Haag en Brussel inzicht en overzicht behouden over waar de Chinese belangen liggen ten opzichte van Europese strategische innovaties, hoe dit zich ontwikkelt, en vroegtijdig signaleren als China minder afhankelijk wordt van deze technologieën. Om dit effectief te laten functioneren, dienen Den Haag en Brussel ook voor belangrijke technologieën die China via andere handelsmechanismen (zoals 'Greenfield Investments') acquireert een soortgelijk toezichtproces te hanteren.

Door samenwerking met China in te bedden in een gestructureerd kader van wederkerigheid, transparantie en afhankelijkheidsmanagement, kan Nederland de stap zetten van reactief naar een zelfverzekerd, strategisch en proactief beleid. Deze aanpak vergroot de nationale weerbaarheid niet alleen door de blootstelling aan inmenging te beperken, maar ook door het eigen handelingsvermogen te behouden en het economische krachtpotentieel van Nederland te benutten in een steeds competitievere geo-economische omgeving.

Introduction

Ever-growing and shifting geopolitical competition is reshaping the global economy, with economic powers such as China and the US vying to protect their political and economic interests. Chief among these is the tit-for-tat effort to control global supply chains and to lead strategic industries, such as AI, with Beijing taking a leading role. However, the growing tension between these two powers has led them to enact tit-for-tat trade measures to hinder each other's economic growth. Indeed, Washington and its allies, including The Hague, have increasingly placed trade restrictions on China. These actions are aimed not only at slowing its access to advanced components and equipment, but also at hindering the development of technologies such as AI and semiconductors, and at increasing costs and limiting access to key markets and components, including next-generation semiconductors produced in Taiwan.

As such, these restrictions have stifled Beijing's efforts to diversify and develop its economic portfolio via legitimate channels and presented an obstacle to its geopolitical goal of achieving economic hegemony on the international stage. In order to overcome these barriers, Beijing has increasingly employed licit alongside illicit tactics, such as foreign interference, for a range of purposes, including monitoring Western companies in strategic industries, such as maritime, semiconductor, or aerospace, to determine whether they pose a threat to Chinese business interests or have developed any technology that could benefit China's economic development.

For the Netherlands, these interference operations pose a particularly salient challenge, given the country's advanced semiconductor capabilities, world-leading maritime expertise, and a high-value aerospace industry. These strengths have not only made the Netherlands an attractive location for investment but also attracted foreign interference from actors such as China, which seeks to become a world leader in these sectors. Despite warnings from Dutch government officials, including former Defence Minister Ruben Brekelmans, and intelligence services about the growing threat of Chinese foreign interference against Dutch businesses and the aforementioned sectors, there is little clarity about the exact ramifications and pervasiveness in

the Netherlands across the country's strategic sectors, such as maritime, semiconductor, and aerospace.[10]

However, the Netherlands faces a structural dilemma. China is a major trading partner and an important geopolitical power, but one that is at odds with other key allies, such as the US. Nevertheless, Beijing is and will remain a central actor in global economic and technological systems. As such, managing this relationship, while continuing to promote and protect the Netherlands' strategic sectors and engaging with actors such as China, requires balancing continued engagement and mutual interdependence with the need to identify, mitigate, and protect against vulnerabilities that can be exploited for strategic leverage.

Building on these developments and the urgent need for greater conceptual clarity, this report will disentangle the nature, scope, and strategic purpose of Chinese foreign interference in the Netherlands. More specifically, the report will research the extent to which Chinese actors, including the government, military, and industry, employ foreign interference measures, such as disinformation, cyber espionage, and sabotage, to interfere in Dutch strategic industries.

This research will be framed around the three guiding questions: What does the concept of foreign interference encompass and what are the specific characteristics of Chinese foreign interference; How are the semiconductors, aerospace, and maritime industries affected by Chinese interference tactics; And how can the Netherlands protect its strategic industries against foreign interference strategies?

To address these questions, the report will employ a mixed-methods approach combining comparative analysis, open-source intelligence (OSINT), interviews, and sector-specific case studies. Chapter 1 will further outline the methodological approach, namely how publicly available information and expert and industry insights are used to map China's interference ecosystem and its deployment in the Netherlands.

[10] Rory O'Neill, "Dutch Defense Minister Warns of Chinese Spying Threat," POLITICO, May 31, 2025, https://www.politico.eu/article/ruben-brekelmans-netherlands-china-spying-intelligence/

Section 2 will expand on the methodology by examining China's overarching approach to foreign interference in industries it deems strategically important. This chapter clarifies the strategic logic underpinning Beijing's targeting of foreign firms, particularly those in the maritime, aerospace, and semiconductor industries, and maps the tools and practices the PRC employs across economic statecraft, digital and information operations, physical interference, and legal and political domains.

Section 3 then turns to the Dutch context, investigating how this systematic challenge materialises across three of the Netherlands' most strategically important industries: semiconductors, maritime, and aerospace. Drawing on sector-specific case studies, this chapter identifies how Chinese actors deploy distinct interference tactics within each industry and the vulnerabilities and governance challenges created by this activity.

Finally, section 4 assesses the implications for Dutch national security, examining the strategic consequences of sustained foreign interference for the Netherlands' economic resilience, technology sovereignty, and long-term national security. To address the identified vulnerabilities, HCSS proposes a set of policy recommendations to help the Hauge mitigate these risks. Taken together, this report provides Dutch policymakers, industry stakeholders and security professionals with a cross-sectoral assessment of the nature and magnitude of Chinese foreign interference in the Netherlands. By sharpening the national understanding of the China-related threat landscape and China's systemic approach to the Dutch maritime, aerospace, and semiconductor industries, the Netherlands' key stakeholders will be able to develop effective defensive measures to safeguard the Netherlands' economic prosperity in the years to come.

1. Methodology

The report has three principal goals, namely (1) to shed light on Chinese foreign interference practices in strategic industries; (2) to assess the risk of Chinese interference in three Dutch strategic industries; and (3) to spell out the implications of Chinese interference in strategic industries for Dutch national security and provide policy recommendations to enhance resilience to such interference.

To do so, the report implements a three-step methodology based on open source information and expert interviews. First, it provides the conceptual grounding by defining foreign interference and analysing the Chinese foreign interference toolkit through a literature review and desktop research. This first step, carried out in section 2, clarifies both what is meant by foreign interference and the specific use of Chinese foreign interference in strategic industries. While existing research addresses Chinese leverage over governmental bodies, elections, and trade processes, this research focuses in depth on industry.[11] This adds to the existing public knowledge of Chinese hybrid interference tools. Section 2 also offers a taxonomy of foreign interference tactics that China employs to target strategic industries abroad, presenting a comprehensive toolkit that extends beyond well-known export controls and trade restrictions.

Section 3 takes a further step by analysing three case studies of Dutch strategic industries vulnerable to China's interference, namely the semiconductor, maritime, and aerospace sectors. The case studies have been selected because of the strategic and economic importance of these industries to the Netherlands and their vulnerability to foreign interference. The semiconductor, aerospace, and maritime sectors form pillars of the Dutch economy, contributing substantially to national innovation, industrial growth, and international trade. The Netherlands is home to globally recognised firms that not only drive technological advancement but also underpin Dutch and European economic resilience. The strategic significance of these industries makes it imperative to develop a nuanced understanding of the risks posed by foreign interference.

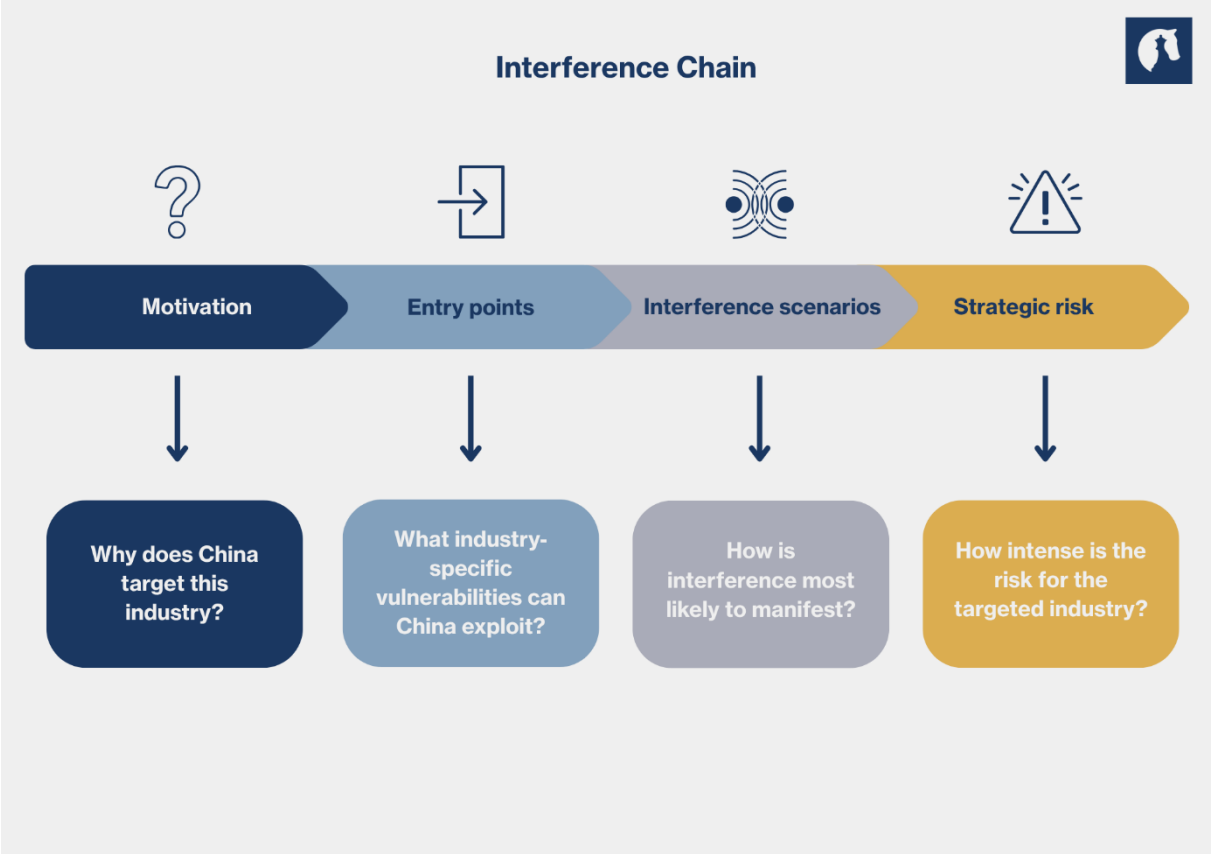
[11] For examples of existing work focusing on China's interference in other fields, see: Ardi Bouwers and Susanne Kamerling, *Chinese Influence and Interference in the Dutch Media Landscape* (China Knowledge Network, 2024), https://www.chinakennisnetwerk.nl/publications/chinese-influence-and-interference-dutch-media-landscape; *Handbook on Countering Russian and Chinese Interference in Europe* (n.d.), accessed May 27, 2025, https://www.europeanvalues.cz/wp-content/uploads/2020/10/Handbook-on-Countering-Russian-and-Chinese-Interference-in-Europe.pdf; Sean Quirk, "Lawfare in the Disinformation Age: Chinese Interference in Taiwan's 2020 Elections," *Harvard International Law Journal* 62, no. 2 (2021): 525–68.

Equally important is the inherent vulnerability of these sectors to foreign interference. Each relies on complex, globally integrated supply chains, proprietary technologies, and sensitive intellectual property, rendering them susceptible to cyber espionage, intellectual property theft, and strategic acquisitions by foreign entities. With China demonstrating a growing interest in acquiring technological capabilities and exerting influence in key global industries, these sectors face heightened exposure. A detailed understanding of these vulnerabilities is crucial for developing robust defence mechanisms to protect critical industries and mitigate potential risks posed by Chinese interference.

In its 2024 annual report, the Dutch Military Intelligence and Security Service (MIVD) already highlighted that these three sectors were targeted by Chinese espionage efforts.[12] The research deepens the public understanding of these efforts by proposing a structured analysis of the three industries across all types of interference identified in the taxonomy. To do this, the report applies a structured analytical lens that links *methods* to *effects* through an Interference Chain (see Figure 3 below). Rather than examining interference tools in isolation, it traces how specific instruments are operationalised through concrete entry points, exploit sectoral vulnerabilities, and ultimately generate strategic risks. This approach allows for systematic comparison across industries and clarifies where policy intervention can most effectively disrupt the interference chain. This sequential framework analyses Chinese interference processes and their effects on Dutch national security through a four-step chain, as seen in Figure 3.

[12] "MIVD Openbaar jaarverslag 2024," Ministerie van Defensie, 2024, https://www.rijksoverheid.nl/documenten/jaarverslagen/2025/04/22/mivd-openbaar-jaarverslag-2024; "Chinese Spies Target Dutch Industries to Strengthen Military, Intelligence Agency Says," China, *Reuters*, April 18, 2024, https://www.reuters.com/world/china/chinese-spies-target-dutch-industries-strengthen-military-intelligence-agency-2024-04-18/

Figure 3 Interference Chain



The first step is establishing the motivation behind the Chinese targeting of a certain industry. Acknowledging this is fundamental to recognising the potential magnitude of Chinese interference. Then, looking at sector-specific vulnerabilities that provide Beijing with entry points allows for identifying weaknesses and hotspots for Dutch policymakers to keep in mind. The third step draws from the previous two and section 2 to highlight which tools China is more likely to use in a series of likely interference scenarios[13]. Lastly, the fourth step highlights the risks associated with the targeted Dutch strategic industry through an Impact X Probability framework.

The probability dimension considers four sub-factors: strategic relevance, historical targeting, accessibility, and sector-specific vulnerabilities. The impact dimension similarly comprises four sub-factors: economic, technological, supply chain, and security.

[13] The report adopts the UK Ministry of Defence's Probability Yardstick as the benchmark to define the language used in the report when it comes to definitions of likelihood. See section 1.1 for a specific breakdown.

The probability and impact indicators are then scored on a 1-5 scale based on a database[14] (see footnote for link to the dashboard created from the database) compiled through open-source research and interviews, according to the criteria in Table 4. The combined score yields the final risk score, providing a nuanced, structured view of the risks each sector faces.

Table 4 Probability and Impact Indicators

Probability	Indicator	Definition	Low	Low-to-moderate	Moderate	Moderate-to-high	High
	Strategic Relevance	Importance of the sector to Chinese economic, technological, or military goals	Minimal relevance to Chinese goals	Limited relevance	Some strategic value	High importance to economic/ tech goals	Critical to core Chinese national, tech, or military interests
	Historical Targeting	Evidence of past interference	No known past interference	Rare/isolated cases	Occasional targeting	Frequent targeting	Persistent, well-documented interference
	Accessibility	Ease with which interference can occur	Very difficult to access or influence	Consistent legal, infrastructural, and security barriers	Moderately accessible	Few barriers	Highly accessible, easy to influence
	Vulnerability	Internal weaknesses that make the sector attractive	Strong governance; few weaknesses	Minor weaknesses	Noticeable gaps	Significant structural weaknesses	Highly vulnerable; major exploitable weaknesses
Impact							
	Economic	Financial or market consequences	Negligible financial impact	Minor market effects	Moderate economic disruption	Large financial/ market consequences	Severe national/European economic damage
	Technological	Effect on innovation and strategic capabilities	No effect on innovation	Small setbacks	Meaningful delays or risks	Major tech capability harm	Critical long-term strategic tech loss
	Supply Chain	Disruption to critical processes or logistics	Minimal disruption	Localised delays	Noticeable bottlenecks	Major process/logistics disruption	Breakdown of critical supply chains
	Security	Consequences for national or European security	No security implications	Limited risks	Moderate security concerns	Serious national/ European risks	Critical threat to national/European security

[14] This database was used, amongst other things, to inform the CLARIS dashboard, which provides further details on foreign interference cases in the Netherlands and beyond.

The case study analysis concludes by examining measures undertaken to date to protect Dutch strategic industries, as well as existing gaps and policy actions to address sector-specific vulnerability to Chinese interference.

Lastly, section 4 connects the sectoral analysis with broader implications for Dutch national security and offers overarching policy recommendations to protect Dutch critical sectors from foreign interference. In particular, it examines measures that bring together the private and public sectors to promote a whole-of-society approach to challenges posed by foreign interference.

The analyses and findings in sections 2, 3, and 4 have been corroborated by interviews with industry representatives and experts from the knowledge community. These interviews served to integrate and inform the team's data collection, expert judgment, and recommendations. The interview outcomes are used throughout the report. However, for privacy reasons, most interviewees have been anonymised throughout the text, as they were given the option to remain anonymous.

1.1 Risk Likelihood & Probability Assessment Language

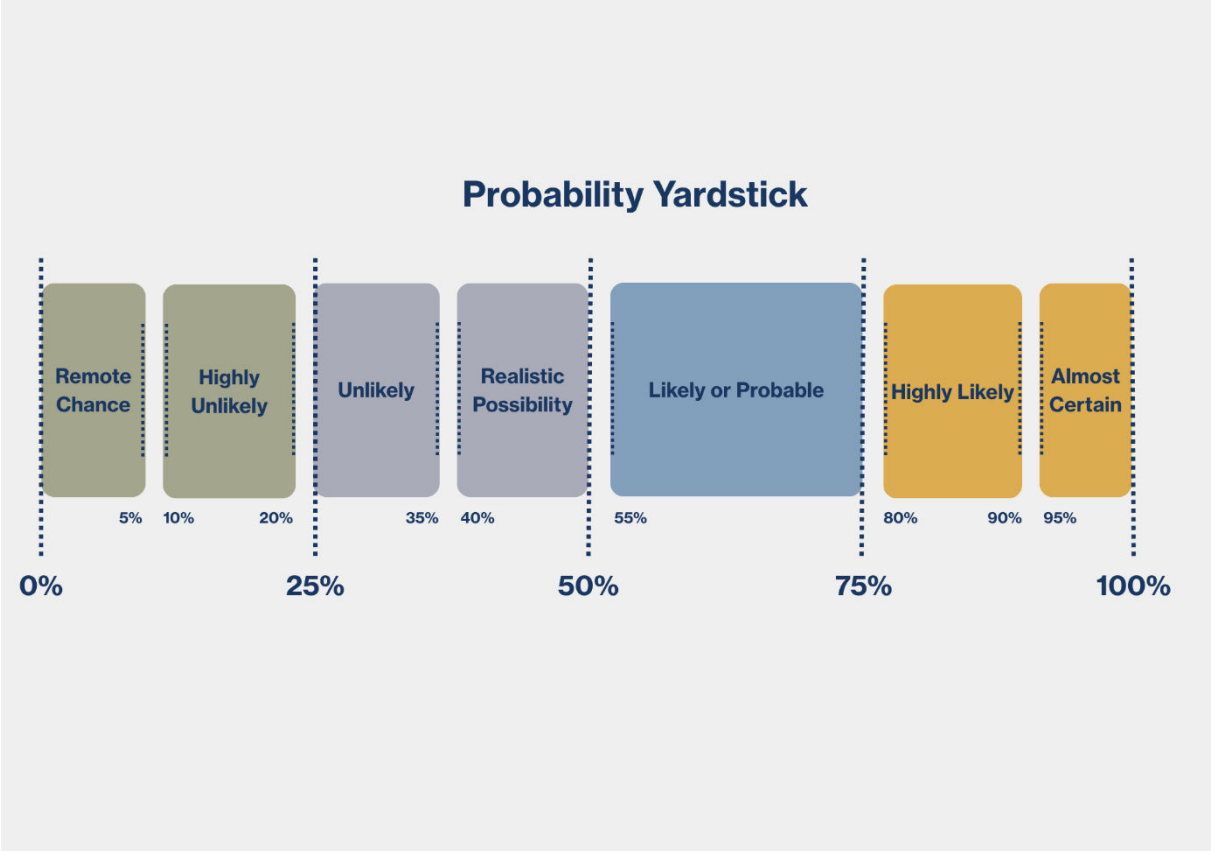
Given the highly uncertain and subjective nature of scenario-based analysis, HCSS has adopted the United Kingdom (UK) Ministry of Defence's probability yardstick metric. This open-source yardstick will help readers understand both why certain probability-related language is used and what it means. The UK Ministry of Defence (MoD) notes that "Intelligence assessments aim to explain something that has happened (insight), or to predict what might happen next (foresight). Intelligence analysts piece together assessments from an incomplete number of jigsaw pieces. Analysts therefore use a shared vocabulary of likelihood that aids clarity for both analysts and their readers, whilst communicating the probability that explanation or prediction is correct".

The UK MoD went on to state that "the yardstick splits the probability scale into seven distinct numerical ranges. Terms are assigned to each probability range. The yardstick was informed by

academic research and corresponds to the average reader's understanding of each term. The scale is not continuous to avoid a false impression of accuracy".[15]

The UK's metric is adopted instead of the Dutch intelligence services' metrics because it is publicly accessible, whereas the latter are not readily available through open-source research, upon which the report is based. Although this yardstick and definition were created by the UK government, they are widely used within the global intelligence and academic communities. This ensures its applicability even within the Dutch context.

Figure 9 UK Ministry of Defence's Probability Yardstick



[15] UK Ministry of Defence, "Defence Intelligence – Communicating Probability," Gov.Uk, February 17, 2023, https://www.gov.uk/government/news/defence-intelligence-communicating-probability

2. Strategic insights: China's approach to foreign interference in strategic industries

Geopolitical competition is increasingly structured around control over strategic industries rather than territory alone. As advanced economies seek to secure technological leadership, protect supply chains, and preserve national security, industrial capabilities with dual-use potential have become central arenas of rivalry.[16] During an interview, Dutch Sinologist Ardi Bouwers agreed with this notion that China has emerged as a particularly active actor, pursuing a long-term strategy to reduce external dependencies, acquire critical technologies, and shape global value chains in its favour.

Foreign interference constitutes a core instrument within this strategy. Rather than relying exclusively on overt economic measures or military coercion, Beijing increasingly employs covert, coercive, and legally ambiguous practices to influence or exploit foreign industrial ecosystems. These activities are especially effective in open economies, where market access, academic collaboration, and investment flows create structural exposure points.[17]

This section establishes the analytical foundation for assessing Chinese interference in Dutch strategic industries. It first clarifies the meaning of foreign interference in an industrial context. It then outlines China's interference toolkit, focusing on how these instruments are applied to strategic industries. Finally, it explains how externally acquired knowledge and leverage are systematically integrated into China's state-driven innovation system, generating long-term strategic risks.

2.1 Foreign Interference in Strategic Industries: Concept and Scope

Foreign interference is increasingly understood as a broad set of deliberate, covert, coercive, and opaque activities undertaken by external actors to influence or exploit a state's political,

[16] Kevin Honglin Zhang, "Geoeconomics of US-China Tech Rivalry and Industrial Policy," *Asia and the Global Economy* 4, no. 2 (2024): 2, https://doi.org/10.1016/j.aglobe.2024.100098; Allison Nathan et al., *The US-China Tech Race* (Goldman Sachs, 2025), https://www.goldmansachs.com/insights/top-of-mind/the-us-china-tech-race

[17] Ofer Fridman, "Defining Foreign Influence and Interference," *INSS Special Publication*, January 4, 2024, 1–12.

economic, or technological systems.[18] Early conceptualisations focused primarily on political meddling or information-based interference. However, more recent analyses have expanded the scope to include economic leverage, cyber operations, technology acquisition, and supply-chain manipulation.[19]

Foreign interference overlaps with, but is distinct from, broader concepts such as hybrid threats and grey-zone activity. *Hybrid threats*[20] broadly describe the deliberate and coordinated combination of overt and covert tools below the threshold of armed conflict, blending political, economic, informational, and technological measures to erode a target's sovereignty, decision-making, or societal cohesion.[21] They differ from *asymmetric warfare*, which centres on violent confrontation between militarily unequal actors,[22] and from *hybrid warfare*, which confines hybrid tools to the legally defined context of armed conflict.[23] The notion of the *grey zone* adds further complexity, capturing the ambiguous space between peace and war in which many hybrid activities unfold.[24]

Foreign interference constitutes a more targeted and purpose-specific subset of the abovementioned hybrid activities.[25] It is oriented towards penetrating and influencing the internal decision-making and critical sectors of a target state rather than pursuing the broader, multidomain destabilisation typically associated with the hybrid threat spectrum.[26] Its defining

[18] Fridman, "Defining Foreign Influence and Interference"; Mikael Wigell, "Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy," *International Affairs* 95 (February 2019), https://doi.org/10.1093/ia/iiz018; Julie Celine Bergaust and Stig Rune Sellevåg, "Improved Conceptualising of Hybrid Interference below the Threshold of Armed Conflict," *European Security* 33, no. 2 (2024): 169–95, https://doi.org/10.1080/09662839.2023.2267478
[19] Fridman, "Defining Foreign Influence and Interference," 5–6.
[20] For an in-depth analysis of Chinese hybrid threats, see: Benedetta Girardi et al., *Responding to China's Hybrid Threats: Strategic Postures for Small and Middle Powers* (The Hague Centre for Strategic Studies, 2026), https://hcss.nl/report/responding-to-chinas-hybrid-threats-strategic-postures-for-small-and-middle-powers/
[21] National Coordinator for Security and Counterterrorism, *Chimaera: An Analysis of the "hybrid Threat" Phenomenon* (Ministry of Justice and Security, 2019), 9, https://english.nctv.nl/documents/publications/2019/09/05/analysis-of-the-%E2%80%98hybrid-threat%E2%80%99-phenomenon; Sofia Romansky et al., *New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape* (The Hague Centre for Strategic Studies, 2024), 4, https://hcss.nl/wp-content/uploads/2024/05/New-Technologies-Changing-Strategies-Hybrid-Threats-HCSS-TNO-2024.pdf; Georgios Giannopoulos et al., *The Landscape of Hybrid Threats: A Conceptual Model (Public Version)* (Publications Office of the European Union, 2021), 6, https://doi.org/10.2760/44985
[22] Patrick A. Mello, "Asymmetric Warfare," in *The Wiley-Blackwell Encyclopedia of Sociology*, 2nd ed. (Wiley-Blackwell, 2015), 1, https://patrickmello.com/wp-content/uploads/2021/04/Mello-2016-EOS.pdf
[23] Sean Monaghan, "Countering Hybrid Warfare: So What for the Future Joint Force?," *Prism* 8, no. 2 (2019): 83, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf; Frank Hoffman, "'Hybrid Threats': Neither Omnipotent Nor Unbeatable," *Orbis* 54, no. 3 (2010): 443, https://doi.org/10.1016/j.orbis.2010.04.009.
[24] Donald Stoker and Craig Whiteside, "Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking," *Naval War College Review* 73, no. 1 (2020): 16, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8092&context=nwc-review
[25] Nicu Popescu, *Hybrid Tactics: Neither New Nor Only Russian*, Issue Alert (European Union Institute for Security Studies, 2015), 1, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_4_hybrid_warfare.pdf
[26] Wigell, "Hybrid Interference as a Wedge Strategy," 261–62.

features are thus intentionality, opacity, and deniability, which complicate attribution and delay response.[27]

Strategic industries are particularly attractive targets because their outputs underpin national security, economic resilience, and geopolitical influence. Their strategic value stems not only from their economic importance, but also from the dual-use potential of many of their outputs, i.e. applications in both civilian and military contexts.[28] They can thus be defined as sectors whose capabilities, outputs, or infrastructure are essential to a state's national security, technological leadership, economic sovereignty, and long-term geopolitical competitiveness, often due to their dual-use potential, centrality to critical supply chains, or role in setting global standards.[29]

As a result, interference in these industries produces effects that extend well beyond individual firms and the private sector, affecting national stability and resilience.

2.2 China's Strategic Logic: Why Interference Targets Industry

Chinese foreign interference targeting Western firms must be understood not as ad hoc behaviour, but as a systemic effort to advance Beijing's enduring objectives: securing technological self-sufficiency, shaping international standards, and ensuring the global competitiveness of Chinese firms in strategically vital industries.

Since the market reforms initiated under Deng Xiaoping in the 1970s, the Chinese Communist Party (CCP) has steadily reoriented the economy away from low-cost, labour-intensive production toward high-value, innovation-driven sectors.[30] This trajectory has been formalised

[27] Wigell, "Hybrid Interference as a Wedge Strategy," 261–62.
[28] Vinod K. Aggarwal and Andrew W. Reddie, "New Economic Statecraft and Global Technology Conflicts: The Dilemma for Middle Powers," *Business and Politics* 27, no. 4 (2025): 467–68, https://doi.org/10.1017/bap.2025.10011; Vinod K. Aggarwal and Andrew W. Reddie, "New Economic Statecraft: Industrial Policy in an Era of Strategic Competition," *World Scientific Connect*, Issues & Studies, vol. 56, no. 2 (2020), https://www.worldscientific.com/doi/10.1142/S1013251120400068.
[29] Olga Petricevic and David J. Teece, "The Structural Reshaping of Globalization: Implications for Strategic Sectors, Profiting from Innovation, and the Multinational Enterprise," *Journal of International Business Studies* 50, no. 9 (2019): 1491–93, https://doi.org/10.1057/s41267-019-00269-x; Ricardo Ernst Haar Jerry, "Supply Chains—It's All National Security Now," *The National Interest*, n.d., accessed December 15, 2025, https://nationalinterest.org/feature/supply-chains-its-all-national-security-now-213250.
[30] Petricevic and Teece, "The Structural Reshaping of Globalization," 1491.

through successive industrial strategies, most notably the Made in China 2025 (MiC25) initiative.[31] MiC25 was started in 2015 as a national industrial policy aimed at helping China and its national champions[32] "significantly reduce their reliance on foreign-produced technology and develop 70% of the components for these projects in China" across 10 industries.[33] In 2018, Beijing advanced MiC25 by launching China Standard 2035 (CS35), aiming to secure global leadership in emerging technologies through standard-setting.[34] These initiatives aim to reduce dependence on foreign technology, cultivate national champions, and position Chinese firms to set global standards in emerging sectors, as corroborated by experts such as Dutch Sinologist Ardi Bouwers.

However, the growing geopolitical tensions between Beijing and the West –particularly the US-China tensions– and subsequent trade restrictions have partially limited Beijing's access to key markets and components. Additionally, market competitiveness and the increasingly fast pace of innovation have made Intellectual Property (IP) in critical sectors highly sensitive.[35] Expanding upon this, Dutch Sinologist Ardi Bouwers and a London-based Sinologist who wished to remain anonymous stated that Beijing has been compelled to seek alternative, covert means to support its technological, military, and economic advance. This concept was further advanced by the World Economic Forum (WEF), where they stated that from Beijing's perspective, interference in foreign strategic industries thus serves three interlinked objectives, namely (1) technological acquisition to accelerate domestic innovation; (2) supply-chain influence to reduce exposure to external pressure; (3) strategic leverage to shape foreign policy behaviour.[36]

These objectives guide the selective and adaptive use of interference tools across different strategic industries.

---

[31] Jost Wubbeke et al., *Made in China 2025* (Mercator Institute for China Studies, 2016), 6–8, https://merics.org/en/report/made-china-2025

[32] A select group of large, often state-owned, enterprises (SOEs) that Beijing strategically supports to dominate key industries.

[33] Federal Bureau of Investigation, "CHINA: THE RISK TO CORPORATE AMERICA," Federal Bureau of Investigation, 2019, https://www.fbi.gov/file-repository/counterintelligence/china-risk-to-corporate-america-2019.pdf/view.
marine engineering and high-tech ships, advanced rail transportation, Electronic Vehicles (EVs), electric power equipment, agriculture, new materials, and biomedicine.

[34] Alexander Chipman Koty, "What Is the China Standards 2035 Plan and How Will It Impact Emerging Industries?," The China Brief, July 2, 2020, https://www.china-briefing.com/news/what-is-china-standards-20355

[35] Scott Kennedy, *The Power of Innovation: The Strategic Value of China's High-Tech Drive* (CSIS, 2026), 16–19, https://www.csis.org/analysis/power-innovation-strategic-value-chinas-high-tech-drive; Kevin Honglin Zhang, "Geoeconomics of US-China Tech Rivalry and Industrial Policy," 3–4.

[36] "Made in China 2025 Set the Tempo of China's Industrial Ambitions," *World Economic Forum*, June 26, 2025, https://www.weforum.org/stories/2025/06/how-china-is-reinventing-the-future-of-global-manufacturing/. -plan-how-will-it-impact-emerging-technologies-what-is-link-made-in-china-2025-goals/#:~:text=China%20is%20set%20to%20release,operate%20within%20the%20tech%20industry.

2.3 China's Foreign Interference Toolkit: Tools and Systemic Integration

To achieve the three objectives stated above, China has developed a diverse toolkit for foreign interference that it employs worldwide. These tools are rarely used in isolation; they are instead combined and sequenced based on the vulnerability of the targeted sector and the geopolitical context. For analytical clarity, they can be grouped into five categories: economic statecraft, digital and information operations, physical interference, legal pressure, and talent-based technological espionage.

Additionally, in this section, we will refer to actions undertaken by "China". However, it should be understood that these actions are undertaken by a range of China-directed actors, ranging from state-owned companies and private companies to intelligence operations conducted by Ministry of State Security (MSS) operatives. Nevertheless, given Beijing and Chinese President Xi Jinping's top-down approach to controlling its foreign interference toolkit, there is little meaningful distinction between actions by alleged private citizens and those of the government. Moreover, this distinction is made even more opaque by the fact that MSS agents will often adopt private-citizen covers to conduct their foreign interference activities. Therefore, China will be used as the operative word to describe actions that are either state-sanctioned or directed.

2.3.1 Economic Statecraft

China increasingly employs economic relations as tools of strategic influence. This approach, often termed economic statecraft, encompasses a range of practices including selective market access, investment in critical infrastructure, development financing through the Belt and Road Initiative (BRI), and targeted trade restrictions, all designed to create dependency or extract political concessions.[37] Rather than relying solely on informal pressure, China has also developed a set of new policy instruments, including export controls under its Export Control Law, formal sanctions mechanisms such as the Anti-Foreign Sanctions Law and the Unreliable Entity List, and other regulatory measures that explicitly tie economic restrictions to political or

[37] Interview with Sam Olsen, a China analyst at British Intelligence firm Sibylline and former intelligence analyst for the British Army; Vida Macikenaite, "China's Economic Statecraft: The Use of Economic Power in an Interdependent World," *JOURNAL OF CONTEMPORARY EAST ASIA STUDIES*9, no. 2 (2020): 108–26.

security goals. These tools have been deployed reactively and defensively against foreign sanctions and trade actions, as well as, at times, proactively to influence other states and their private sector.[38]

While many of these instruments are embedded within global economic governance frameworks, they are frequently deployed coercively or conditionally to blur the line between legitimate economic policy and foreign interference.[39] By leveraging its position as a dominant trading partner, investor, or supplier, Beijing can reward political compliance, punish unfavourable policy decisions, or induce self-censorship among governments and firms seeking continued access to the Chinese market. This trend was corroborated by an anonymous Dutch China expert in an interview. This form of influence is particularly effective in open economies, where commercial actors operate with significant autonomy and economic considerations often shape political decision-making.[40] An overview of China's economic coercion toolkit is offered in the table below.[41]

[38] Evan S. Medeiros and Andrew Polk, "China's New Economic Weapons," *The Washington Quarterly* 48, no. 1 (2025): 104–15, https://doi.org/10.1080/0163660X.2025.2480513.

[39] [1] Tinatin Khidasheli, *Hybrid Threats and Resilience: Safeguading Democratic Values in a Connected World* (Friedrich-Naumann-Foundation for Freedom South Caucasus, 2024), 10; Marcin Szczepański, *China's Economic Coercion: Evolution, Characteristics and Countermeasures*(European Parliamentary Research Service, 2022), 4, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738219/EPRS_BRI(2022)738219_EN.pdf.

[40] Vida Macikenaite, "China's Economic Statecraft: The Use of Economic Power in an Interdependent World," *Journal of Contemporary East Asia Studies* 9, no. 2 (2020): 110–12, https://doi.org/10.1080/24761028.2020.1848381.

[41] As the scope of this paper limits the depth of the discussion on Chinese economic statecraft, see for a more in-depth breakdown: Benedetta Girardi et al., *Responding to China's Hybrid Threats*; Szczepański, *China's Economic Coercion: Evolution, Characteristics and Countermeasures*; Medeiros and Polk, "China's New Economic Weapons"; Macikenaite, "China's Economic Statecraft"; Vinod K. Aggarwal and Andrew W. Reddie, "New Economic Statecraft: Industrial Policy in an Era of Strategic Competition."

Table 5 Summary of China's Economic statecraft tools

Tool	Mechanism	Target in Strategic Industries	Intended Effect
Selective market access	Granting or restricting entry to Chinese market	Foreign firms reliant on China	Induce political compliance; self-censorship
Trade restrictions	Tariffs, import bans, customs delays	Export-dependent sectors	Punish unfavourable policies
Investment in critical infrastructure	Equity stakes, acquisitions, port/logistics investments	Energy, transport, digital infrastructure	Create long-term dependency and leverage
Belt and Road Initiative (BRI) financing	Loans, infrastructure funding	Partner countries' industrial ecosystems	Debt dependency; political alignment
Unreliable Entity List	Blacklisting firms	Foreign companies in strategic sectors	Coerce behaviour change
Regulatory pressure	Licensing, inspections, compliance barriers	Firms operating in China	Create uncertainty; extract concessions
Supply chain dominance	Control over key inputs/materials	Manufacturing, energy, tech sectors	Structural dependency

2.3.2 Digital and Information Operations

In combination with economic statecraft, Beijing also widely employs digital and information operations to engage in foreign interference. Cyberattacks, foreign information manipulation and interference (FIMI), and cyber espionage are all aimed at projecting influence and gathering protected information in foreign jurisdictions through the digital domain.

China's use of disinformation in strategic industries is increasingly aimed at shaping regulatory debates, market perceptions, and political decision-making in ways that favour Chinese technological and industrial interests.[42] Rather than focusing solely on broad geopolitical narratives, Beijing-linked actors deploy targeted information operations to influence discussions around specific strategic sectors. A prominent example is China's sustained information

[42] Jesse S. Curtis, "Springing the 'Tacitus Trap': Countering Chinese State-Sponsored Disinformation," *Small Wars & Insurgencies* 32, no. 2 (2021): 229–65, https://doi.org/10.1080/09592318.2021.1870429.

campaign surrounding 5G infrastructure. Chinese state media, diplomatic channels, and covert online networks sought to downplay security risks associated with Chinese vendors such as Huawei, while portraying Western restrictions as protectionist, politically motivated, or technologically irrational.[43]

Similar narrative strategies have been observed in debates over semiconductor export controls, where Chinese messaging frames Western rhetoric as destabilising global supply chains and harming innovation. In tandem, China also obscured concerns over military end use and intellectual-property security.[44] These campaigns often rely on a mix of overt state media content, coordinated inauthentic behaviour on social media, and the amplification of sympathetic voices within business, academic, and policy communities abroad.[45] During an interview, a London-based China expert mentioned that China is increasingly using Western social media platforms, including videos by Western influencers invited to China, to sway opinion. Information campaigns aimed at strategic industries are hence mostly used by Beijing to strengthen its economic statecraft and shape regulatory and market debates.

However, despite this aim, China's ability to successfully shape Western narratives has been mixed.[46] For example, the multi-year disinformation campaign named Spamouflage is not achieving its intended goals because "it has lacked nuance and audience-specific content that successful nation-state disinformation campaigns from countries like Russia, Iran, and Turkey have included".[47] In line with this, French military and intelligence officials disclosed in July 2025 that Beijing utilised its embassies to conduct a disinformation campaign, with mixed results, regarding the effectiveness of French-made fighter jets used in the India-Pakistan clashes in May 2025, in an attempt to promote Chinese-made military hardware.[48]

[43] Laurens Cerulus, "Fake Websites Found Peddling Pro-Huawei Content," *POLITICO*, February 24, 2021,
[44] Olivia Tam, "China Says US Chip Controls Are Undermining Trade Consensus," *Bloomberg*, May 19, 2025, https://www.bloomberg.com/news/articles/2025-05-19/china-says-us-chip-controls-are-undermining-trade-consensus; Neal E. Robbins, "China-Origin Disinformation Campaign Stoke Taiwan Fears over Microchips," *SOAS China Institute*, August 2, 2023, https://blogs.soas.ac.uk/china-institute/2023/08/02/china-origin-disinformation-campaign-stoke-taiwan-fears-over-microchips/.
[45] Elise Thomas, "Pro-CCP 'Spamouflage' Network Pivoting to Focus on US Presidential Election," Institute for Strategic Dialogue, February 15, 2024, https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-net-work-focuses-on-us-election/.
[46] Thomas, "Pro-CCP 'Spamouflage' Network Pivoting to Focus on US Presidential Election."
[47] David Gilbert, "Why China Is So Bad at Disinformation," News, WIRED, April 29, 2024, https://www.wired.com/story/china-bad-at-disinformation/.
[48] France 24, "Beijing Disinformation Targeted French Rafale Jets to Boost Sales of China-Made Planes, Intel Says," France 24, July 6, 2025, https://www.france24.com/en/france/20250706-china-used-embassies-to-undermine-rafale-sales-after-india-pakistan-clash-french-intel-says.

Meanwhile, China employs cyber operations as a central mechanism of foreign interference in strategic industries, particularly through cyber-economic espionage. State-linked actors conduct sophisticated intrusions into corporate networks, research institutions, and critical infrastructure to exfiltrate intellectual property, proprietary technology, and trade secrets, accelerating domestic innovation and supporting initiatives such as MiC25 and CS35.[49] The sectors targeted include cloud computing, artificial intelligence, internet-connected devices, biotechnology, energy, robotics, transportation, agricultural machinery and other agricultural technology, and high-end medical devices.[50] While the focus of China's cyber espionage activity was initially squarely on countries such as the US or Taiwan, China has turned its sights on EU infrastructure and businesses in recent years as well.[51]

Other instruments of cyber interference available to Beijing are of a more disruptive nature, such as cyber sabotage or wiper malware attacks. While China has not historically engaged in destructive digital operations, Western intelligence agencies, such as the US Cybersecurity and Infrastructure Security Agency (CISA), claim to have intelligence indicating that Beijing is "preparing to launch" such attacks during a geopolitical conflict.[52] Table 6 presents a summary of the main tools discussed above.[53]

[49] "Cyber Arms Watch Monitor," *HCSS*, n.d., accessed January 8, 2026, https://hcss.nl/cyber-arms-watch-monitor/.
[50] Peter Harrell, *China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses* (CNAS, 2018), https://www.cnas.org/publications/congressional-testimony/chinas-non-traditional-espionage-against-the-united-states-the-threat-and-potential-policy-responses.
[51] David Kertai, *From Trade Deals to Trojan Horses: China's Expanding Digital Aggression on Europe* (2025), https://itif.org/publications/2025/08/01/from-trade-deals-to-trojan-horses-chinas-expanding-digital-aggression-on-europe/.
[52] "People's Republic of China Threat Overview and Advisories," Government, Cybersecurity and Infrastructure Security Agency, accessed August 20, 2025, https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china.
[53] Much has been written on Chinese cyber and information operations that goes beyond the scope of the current research; for a deeper dive into the topic, see: Cybersecurity Infrastruct. Secur. Agency, "People's Republic of China Threat Overview and Advisories"; Dave Aitel et al., *China's Cyber Operations: The Rising Threat to American Security* (Margin Research, 2022), https://margin.re/chinas-cyber-operations-the-rising-threat-to-american-security/; Cristina Vanderghen, "The Digital Battlefield: EU-China Cybersecurity Diplomacy in the 21st Century – Part I," Friends of Europe, 2025, https://www.friendsofeurope.org/insights/critical-thinking-the-digital-battlefield-eu-china-cybersecurity-diplomacy-in-the-21st-century-part-i/; Valentin Weber, "Taiwan's Offensive Cyber Capabilities and Ramifications for a Taiwan-China Conflict," Council on Foreign Relations, December 7, 2022, https://www.cfr.org/blog/taiwans-offensive-cyber-capabilities-and-ramifications-taiwan-china-conflict; Kertai, *From Trade Deals to Trojan Horses*; International Republican Institute, *Countering China's Information Manipulation: A Toolkit for Understanding and Action*(International Republican Institute, 2023), https://www.iri.org/wp-content/uploads/2023/09/Web_IRI-Toolkit-Building-Resilience-to-PRC-Information-Manipulation.pdf; European Union External Actions Services, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations* (European Union External Actions Services, 2025); Gilbert, "Why China Is So Bad at Disinformation."

Table 6 Summary of China's digital and information operations tools

Tool	Mechanism	Target in Strategic Industries	Intended Effect
Disinformation campaigns	State media, covert networks, narratives	Policy debates	Shape regulation and public opinion
Foreign Information Manipulation & Interference (FIMI)	Coordinated inauthentic behaviour, amplification	Political and regulatory communities	Influence decision-making
Social media influence	Influencers, targeted content	Public and business audiences	Normalize pro-China narratives
Narrative framing	Messaging on supply chains, innovation	Policymakers and industry leaders	Reframe Western policies as harmful
Cyber espionage	Network intrusions, data exfiltration	Corporations, R&D institutions	Acquire IP and trade secrets
Cyber sabotage	Wiper malware, infrastructure disruption	Critical infrastructure	Disruption during crises

2.3.3 Physical Interference

Physical interference constitutes the most kinetic component of China's foreign interference mechanisms and encompasses tactics such as infrastructure sabotage, paramilitary operations, arson, and assassination. While not the most common interference tools (Table 7) in strategic industries, China has increasingly demonstrated a willingness to employ this type of tactic against strategic infrastructure and industries instead of using them exclusively for political signalling, as done in the past.[54]

China's military exercises serve as a form of physical interference by shaping perceptions of risk around strategically important regions and assets. The PLA's Joint Sword-2024B exercises around Taiwan in October 2024 illustrated Beijing's willingness to use kinetic pressure in areas critical to global semiconductor manufacturing and high-technology supply chains.[55] These exercises followed political statements by Taiwan's leadership that challenged Beijing's sovereignty

[54] David Shambaugh, *China Goes Global: The Partial Power* (Oxford University Press, 2013).
[55] Meia Nouwens and Erik Green, "China's Joint-Sword B Exercise: A Calculated Follow-On," IISS, October 23, 2024, https://www.iiss.org/online-analysis/online-analysis/2024/10/chinas-joint-sword-b-exercise-a-calculated-follow-on/.

claims, reinforcing the linkage between physical interference and the protection of strategic industrial interests.[56]

While geographic distance shields European states from this kind of activity, China has been more directly linked to incidents involving physical interference with critical infrastructure in Europe and, particularly, undersea communications cables that support global finance, data flows, and industrial coordination.[57]

In November 2024, two major submarine cables in the Baltic Sea – connecting Lithuania to Sweden and Finland to Germany – were severed under circumstances that prompted sabotage investigations. A Chinese-flagged commercial vessel, *Yi Peng 3*, was reported to have traversed the cable routes with movements consistent with anchor dragging, raising suspicions of deliberate interference.[58]

Similar tactics have been observed in the Indo-Pacific. In early 2025, a Chinese-linked vessel was implicated in the cutting of an undersea fibre-optic cable near Taiwan's Keelung Harbour, disrupting communications and reinforcing concerns over grey-zone pressure on infrastructure critical to Taiwan's economy and technological sector.[59]

Undersea cables carry over 99% of global internet and data traffic, making them essential to strategic industries such as semiconductors, cloud computing, logistics, and financial services. Interference with these systems enables Beijing to exert leverage while maintaining plausible deniability and remaining below the threshold of open conflict.[60]

---

[56] "Full Text of President Lai Ching-Te's National Day Address," Focus Taiwan, October 10, 2024, https://focustaiwan.tw/politics/202410100004.
[57] Benedetta Girardi and Sean Tan, *Response and Resilience: Government Strategies for Securing Subsea Infrastructure in Europe and Asia* (The Hague Centre For Strategic Studies, 2025), 3–5, https://hcss.nl/report/response-and-resilience-government-strategies-for-securing-subsea-infrastructure-in-europe-and-asia/.
[58] Sebastian Seibt, "Hybrid Warfare? China Sabotaging Baltic Sea Cables Would Be 'Super Surprising', Experts Say," France 24, November 21, 2024, 24, https://www.france24.com/en/europe/20241121-hybrid-warfare-china-sabotaging-baltic-sea-cables-would-be-super-surprising-experts-say.
[59] Hans Horan, "Beijing's Targeting of Taiwan's Undersea Cables Previews Cross-Strait Tensions Under a Trump Presidency," The Diplomat, January 17, 2025, https://thediplomat.com/2025/01/%e2%80%8b%e2%80%8bbeijings-targeting-of-taiwans-undersea-cables-previews-cross-strait-tensions-under-a-trump-presidency/.
[60] Seibt, "Hybrid Warfare? China Sabotaging Baltic Sea Cables Would Be 'Super Surprising', Experts Say," 24.

Critical infrastructure sabotage, such as the Baltic Sea incident, constitutes the highest physically related foreign interference mechanism China currently employs against European strategic industries.

Table 7 Summary of China's physical interference tools

Tool	Mechanism	Target in Strategic Industries	Intended Effect
Military exercises	Demonstrations of force near key regions	Production hubs	Signal risk; deter political moves
Infrastructure sabotage	Physical damage to assets	Undersea cables, energy systems	Disruption; coercive signalling
Maritime grey-zone tactics	Civilian vessels used for interference	Subsea infrastructure	Plausible deniability
Communications disruption	Cutting fibre-optic cables	Data-dependent industries	Interrupt economic activity
Strategic intimidation	Presence-based coercion	Trade routes, industrial zones	Raise cost of resistance

2.3.4 Legal Pressure

Beijing employs several legal mechanisms to interfere in strategic industries. The potentially most well-known of these tools is China's utilisation of lawfare. Lawfare[61] can be defined as the "legal action undertaken to exert power or control, especially as part of a hostile campaign against a particular country or group".[62] When it comes to strategic industries, Beijing especially employs lawfare against European companies to create barriers and exert influence over their operations in and with China. Beijing utilises the variety of legal tools at its disposal to create an "unfair business environment" for Dutch businesses, often in response to EU actions perceived as unfair or discriminatory towards Chinese firms in Europe. Dutch Sinologist Frans-Paul van der Putten mentioned during an interview: “[Legal pressure] has been part of the Chinese approach for many decades”.

[61] For an in-depth breakdown on the nature, scope, and impact of Chinese lawfare see: Benedetta Girardi, Anna Hoefnagels, and Berend Kwak “Reshaping the international legal order: China's strategic use of lawfare and lessons learned for Europe”, The Hague Centre for Strategic Studies, April 2026.
[62] “Lawfare,” *Oxford English Dictionary*, March 2025 (Oxford University Press (OED)), accessed August 21, 2025, https://www.oed.com/dictionary/lawfare_n?tl=true.

Although not mandatory in all sectors, joint ventures (JVs) are required in some restricted strategic industries, and a Leiden Asia Centre survey of Dutch firms found "joint ventures in China often involve technology transfer".[63] As Dutch Sinologist Frans-Paul van der Putten described: “[Dutch Businesses] have to give something back [to China] if you are a business who has relevant technology or experience”. The US FBI similarly claimed that "joint ventures, including long-term visits, might provide an opportunity for a competing company to obtain restricted information and gain access to a vulnerable collaborative environment".[64]

Some Western companies have reported being unable to leave China during instances of geopolitical tensions between the West and China. According to an excerpt from an interview conducted with an undisclosed Dutch firm by the Leiden Asia Centre, "if anything goes wrong, if there is an accident, for example, then the company is liable. If you don't cooperate with their way of fixing the problem, they can withdraw your licenses. Or they say, 'We will have a couple of people from your company, including you, arrested'. It's pure blackmail".[65] Table 8 summarises the principal tools of legal pressure available to Beijing.[66]

Table 8 Summary of China's legal pressure tools

Tool	Mechanism	Target in Strategic Industries	Intended Effect
Lawfare	Use of legal system for strategic coercion	Foreign firms in China	Control operations; retaliate politically
Joint venture requirements	Mandatory local partnerships	Cutting-edge and restricted sectors	Enable technology transfer
Licensing pressure	Threat of revoking business licenses	Foreign companies	Force compliance
Regulatory enforcement	Selective application of laws	Multinationals	Create uncertainty and leverage
Exit barriers	Restrictions on leaving country	Foreign executives, firms	Coercion, leverage over personnel
Legal intimidation	Threats of arrest or liability	Corporate leadership	Force cooperation

[63] Ardi Bouwers and Alex Krijger, “The China Challenge Impact of the Politicised Business Environment on Dutch Companies in China,” Leiden Asia Centre, July 2020, 36, https://leidenasiacentre.nl/the-china-challenge/.
[64] Federal Bureau of Investigation, “CHINA: THE RISK TO CORPORATE AMERICA,” 4.
[65] Ardi Bouwers and Alex Krijger, “The China Challenge Impact of the Politicised Business Environment on Dutch Companies in China,” 36.
[66] For a more in-depth breakdown of Chinese lawfare, see also: Benedetta Girardi, Anna Hoefnagels, and Berend Kwak, *Reshaping the international legal order China’s strategic use of lawfare and lessons learned for Europe* (The Hague Centre for Strategic Studies, 2026); Alexandre Ferreira Gomes et al., *Standardisation with Chinese Characteristics?* (Clingendael CKN, 2025), https://www.chinakennisnetwerk.nl/publications/39-standardisation-chinese-characteristics; Mathieu Duchâtel and Georgina Wright, *China’s Extraterritoriality: A New Stage of Lawfare*, Explainer (Institut Montaigne, 2024), 72, https://www.institutmontaigne.org/en/publications/chinas-extraterritoriality-new-stage-lawfare; L.N. Nguyen and A.G. Oude Elferink, *The International Law of the Sea and the South China Sea Disputes* (Clingendael CKN, 2025), https://www.chinakennisnetwerk.nl/publications/38-international-law-sea-and-south-china-sea-disputes.

2.3.5 Talent-based technological espionage

Lastly, a particularly diffused interference tactic is the systematic state-sponsored talent recruitment aimed at acquiring advanced foreign technology, which main tools are summarised in Table 9 below.[67]

China's Thousand Talent Programme (TTP) is the most prominent of this, because it provides Beijing with the necessary talent and "know-how" to achieve its aforementioned geopolitical goals. Linked to the CCP's National Talent Development plan, it aims to recruit experts (primarily from the Chinese diaspora, though not exclusively) in science and technology sectors where China is less developed than the West. The "participants" China seeks to add to the TTP consist primarily of employees with expertise in and/or access to cutting-edge technology China has not yet developed or cannot access through the international market, due to, e.g., trade sanctions.[68]

To attract potential participants to the programme, Beijing offers benefits such as higher salaries, prestigious research positions, and honorary titles. In exchange, Beijing expects participants to bring or steal research and IP (original or otherwise) for their new Chinese employer. In a notable example, Dutch semiconductor firm ASML disclosed that a Chinese national who worked for ASML took chipmaking tool information to the Chinese telecommunications firm Huawei after leaving ASML.[69]

[67] Julie Zhu et al., *Insight: China Quietly Recruits Overseas Chip Talent as US Tightens Curbs*, August 24, 2023, https://www.reuters.com/technology/china-quietly-recruits-overseas-chip-talent-us-tightens-curbs-2023-08-24/.
[68] Julie Zhu et al., "Insight: China Quietly Recruits Overseas Chip Talent as US Tightens Curbs," Reuters, August 24, 2023,
[69] Tobias Mann, "Ex-ASML Worker Accused of Stealing Chipmaking Secrets for China Is Huawei to a New Job," The Register, October 24, 2023, https://www.theregister.com/2023/10/24/asml_ip_huawei/.

Table 9 Summary of China's talent-based technological espionage tools

Tool	Mechanism	Target in Strategic Industries	Intended Effect
State-backed talent recruitment	Incentives (salary, prestige, funding)	Scientists, engineers, executives	Attract critical expertise
Knowledge transfer requirements	Informal/explicit expectations	Research institutions, firms	Transfer innovation to China
IP exfiltration via employees	Insider access to proprietary data	High-tech firms	Accelerate domestic capabilities
Academic collaboration channels	Research partnerships	Universities, labs	Access early-stage innovation
Long-term placements	Exchanges, visiting roles	Corporate and research environments	Build access networks

2.4 From Interference to Strategic Advantage: Chinese Systemic Integration of Interference Efforts

Where Chinese foreign interference differs from that of other states is the efficacy in not only acquiring significant information and data from its activities, but also integrating it into its state-driven industrial innovation. Externally sourced knowledge, data, and expertise are absorbed into a coordinated state-driven innovation system that links civilian industry, research institutions, and the military. China integrates the fruits of its interference directly into its knowledge network and distributes it amongst its state champions and highly productive organisations to achieve the geopolitical goals stated in its economic policies.[70]

[70] Federal Bureau of Investigation, "CHINA: THE RISK TO CORPORATE AMERICA."

This integration is conducted in a four-step process (as shown in Table 10), which consists of the following:

Table 10 China's Four-Step Development Process

China's Four-Step Development Process for Gaining a Technological Edge Over the West – What happens to data after it is exfiltrated?[71]	
Introduction	Beijing utilises a variety of methods – e.g., (cyber) espionage – to introduce foreign technology and knowledge to Chinese state champions.
Understand	Beijing employs its civilian and military institutional resources to analyse and interpret the information it has acquired.
Assimilate	These resources then assimilate foreign knowledge (e.g., through reverse engineering) into China's knowledge environment and businesses.
Re-Innovate	This knowledge is then reinvented to develop China-made state-of-the-art technology that gives Chinese companies a competitive edge in the international market by making their products more cutting-edge than competitors' and cheaper, due to, e.g., time and cost savings in research and development (R&D).

Beijing's expanding toolkit for foreign interference thus generates strategic risks by enabling the rapid conversion of externally acquired knowledge into system-wide technological and economic advantages. By systematically exfiltrating sensitive data, research, and IP through various interference tactics, Beijing feeds a state-directed innovation system that seeks to understand and assimilate foreign technology at scale. This allows Chinese firms (often state-backed) to undercut Western competitors and accelerate China's move into critical supply chains. Over time, these dynamics reduce China's dependence on foreign inputs while increasing foreign dependence on Chinese technologies, manufacturing capacity, and standards.

For an open economy such as the Netherlands, these dynamics heighten exposure to strategic vulnerabilities that directly affect national security, economic competitiveness, and the integrity of its innovation ecosystem, while constraining its policy autonomy. The variety of China's foreign interference toolkit, combined with the systemic integration of information collected through interference activities, makes its use of foreign interference in strategic industries a systemic, multi-domain challenge that affects both the public and private sectors.

[71] Federal Bureau of Investigation, "CHINA: THE RISK TO CORPORATE AMERICA," 3.

Taking this into account, three policy-relevant considerations can be made:

First, Chinese foreign interference is a systemic challenge, not a series of isolated incidents. Addressing it requires moving beyond case-by-case responses toward structural resilience.

Second, traditional policy tools are insufficient. Export controls, investment screening, and cybersecurity measures address only parts of the interference chain, leaving gaps related to talent mobility, supply-chain coercion, and economic espionage.

Third, private-sector detection precedes state awareness. Companies, as the direct targets, are typically the first to detect suspicious activity, meaning effective countermeasures depend on timely information sharing between the private sector and government.

As highlighted in this chapter, Beijing's foreign interference toolkit is not purely aimed at only *gaining* a technological advantage over Western competitors; given that Chinese firms already possess such an advantage in sectors, such as green energy. In addition, this toolkit is also aimed at *maintaining* this advantage by monitoring Beijing's competitors' developments and ensuring they stay one step ahead of them. For the Netherlands, the upcoming chapter will examine where the Netherlands' maritime, aerospace, and semiconductor sectors are relative to China and assess a series of likely scenarios for how they are vulnerable to Chinese foreign interference, and whether they are being targeted because they are outpacing their Chinese counterparts or for maintenance purposes.

3. Chinese Interference in Dutch Strategic Industries: Sectoral Manifestations of a Systemic Challenge

The semiconductor, aerospace, and maritime industries are pillars of the Dutch economy, playing a vital role in national and European technological development. These sectors contribute significantly to innovation, industrial growth, and international trade. The Netherlands hosts some of the world's leading firms in these industries, and Dutch companies provide essential components and expertise that are integral to global supply chains. This includes value chains connected to Chinese firms seeking cutting-edge technology and industrial know-how.

This strategic position makes the Netherlands a target for Chinese foreign interference. For Beijing, these three industries lie at the intersection of its economic competitiveness, technological leadership, and national security. Semiconductors underpin virtually all modern electronics and advanced technologies, making control over chip design and production a critical determinant of industrial and military capability. The maritime sector is central for both Chinese trade and strategic influence, as secure shipping routes and port infrastructure enable the movement of goods, energy resources, and military assets. Aerospace represents a high-value, dual-use domain in which technological superiority translates directly into economic advantage and strategic power projection. Collectively, these sectors serve as leverage points for China to shape global supply chains, advance domestic technological self-sufficiency, and reinforce broader geopolitical objectives.[72]

While Beijing has made significant strides in acquiring the necessary knowledge, component personnel, and technology to level the economic playing field with its Western counterparts, it has not yet fully achieved this objective. Indeed, Zongyuan Zoe Liu, a Maurice R. Greenberg Fellow for China Studies at the Council on Foreign Relations, noted that when discussing China's economic innovation vis-à-vis the West, China has not achieved "self-sufficiency" in this regard. For example, Liu notes that "President Xi Jinping or the government seems to be warning Chinese tech companies not to be overly reliant on American Chips or American technology [...] [such messaging] is a signal, a realisation, that China has not yet reached technological self-sufficiency

[72] Joris Teer et al., *Competitie Tussen Grootmachten En Maatschappelijke Stabiliteit in Nederland: De Risico's van Russisch Gas, Chinese Grondstoffen En Taiwanese Chips Voor Vitale Sectoren* (The Hague Centre For Strategic Studies, 2023), https://hcss.nl/report/competitie-grootmachten-en-maatschappelijke-stabiliteit-nederland/.

yet". Liu went on to state that by "intentionally reducing their [China's] dependency on American or foreign tech, you force domestic investment and innovation [...] eventually you hope you can create your own alternative".[73]

Within this context, the Netherlands' position in the global value chains of these industries increases its strategic importance and continued appeal as a target for Chinese foreign interference. While the organisation of production, ownership structures, and regulatory environments differ across the three sectors, they are all characterised by high levels of internationalisation, reliance on complex supplier networks, and close interaction between industry, research institutions, and government. These characteristics create opportunities for foreign interference that are often incremental, legally ambiguous, and difficult to assess when viewed in isolation.

Therefore, while the following case studies examine distinct industries, they should not be read in isolation. Together, semiconductors, maritime logistics, and aerospace illustrate how Chinese foreign interference adapts to different industrial structures while pursuing consistent strategic objectives: access to critical knowledge and technology, leverage over key nodes, and long-term dependency formation. Viewed through this lens, Chinese interference in strategic industries should be understood as a cumulative process rather than a series of separated incidents. Individual acts of espionage, coercion, or influence may appear manageable in isolation, but their aggregate impact can have long-lasting disruptive effects for a state's national security, industrial and knowledge base, and societal and governance resilience.

This logic is particularly relevant for the Netherlands, whose open economic model, globally integrated supply chains, and concentration of high-value technological capabilities constitute both a key strength and a structural exposure to interference. Recognising this duality is essential to developing effective, proportionate policy responses.

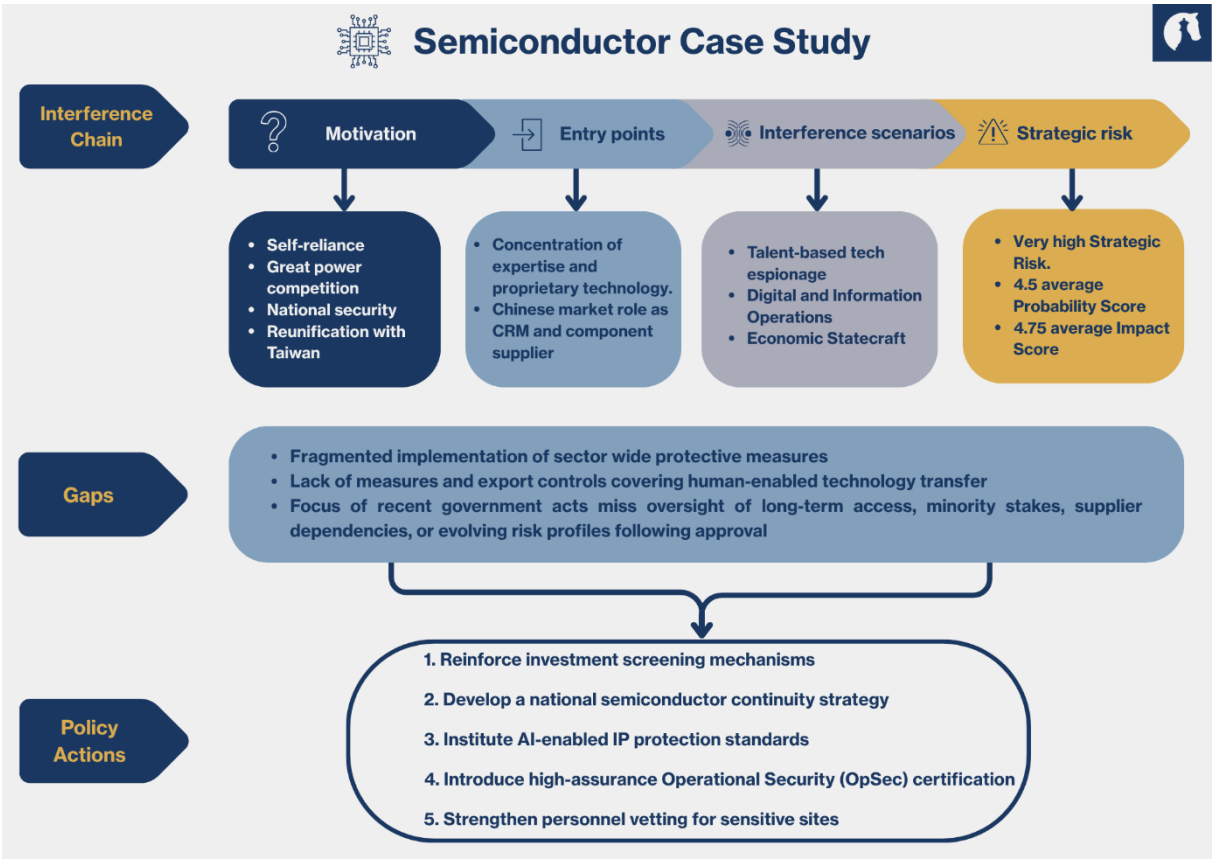
[73] Center for Strategic and International Studies (CSIS), *Understanding Chinese Power*, Pekingology, March 5, 2026, 50:36, https://www.csis.org/podcasts/pekingology/understanding-chinese-power

To translate China's interference toolkit into policy-relevant risk assessments, this report applies a structured analytical lens that links *methods* to *effects* through a four-step Interference-to-Effect chain. Rather than examining interference tools in isolation, it traces how specific instruments are operationalised through concrete entry points, exploit sectoral vulnerabilities, and ultimately generate strategic risks.

Finally, to inform such responses, each case study concludes with an assessment of existing Dutch protective initiatives, identifies where gaps remain, and analyses how these gaps could be addressed. These sectoral findings provide the empirical foundation for the cross-sectoral synthesis and policy recommendations developed in section 4.

3.1 The Semiconductor Sector

Figure 4 Overview of Semiconductor Case Study



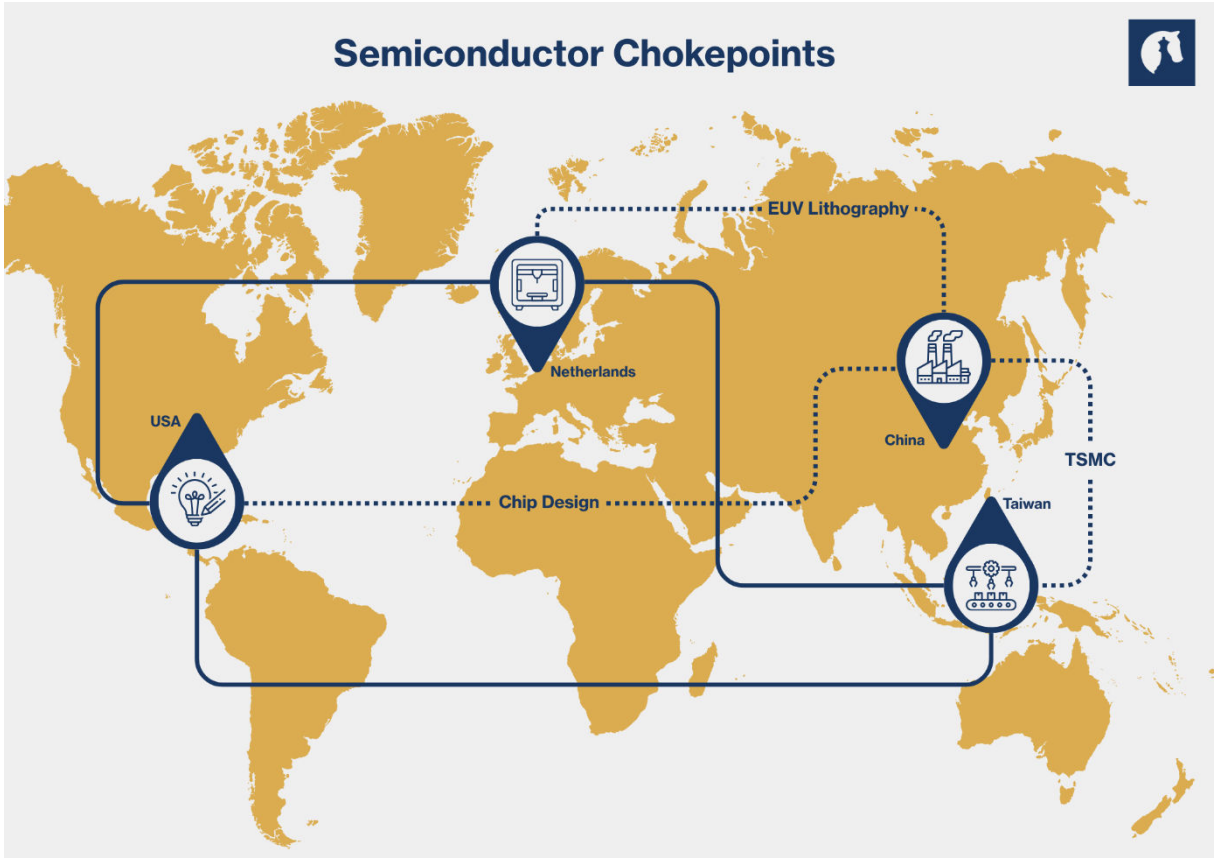
3.1.1 Motivation

The semiconductor industry is the linchpin of Beijing's economic development plan and self-reliance ideology, as it intersects with three key areas: economic growth, national security, and international agenda-setting.[74]

Ensuring that Chinese firms are at the forefront of the semiconductor industry is imperative to achieving the goals set out in Beijing's economic policies.[75] Chief amongst these is Beijing's desire to reduce its "strategic vulnerabilities" or its dependence on foreign core technologies, such as chips and manufacturing equipment, from Japan, the Netherlands, Taiwan, and the US.[76] Several bottlenecks along the supply chain for advanced semiconductor chips prevent China from controlling the entire supply chain.[77] The two most critical chokepoints are perhaps ASML's monopoly on EUV lithography machine production and Taiwan Semiconductor Manufacturing Corporation's (TSMC) dominance in advanced chip manufacturing (see figure 5 below).[78]

[74] Vox, "Why China Is Losing the Microchip War," YouTube, February 7, 2023, https://www.youtube.com/watch?v=Uh4QGey2zTk.
[75] Alexander Chipman Koty, "What Is the China Standards 2035 Plan and How Will It Impact Emerging Industries?," The China Brief, July 2, 2020, https://www.china-briefing.com/news/what-is-china-standards-2035-plan-how-will-it-impact-emerging-technologies-what-is-link-made-in-china-2025-goals/#:~:text=China%20is%20set%20to%20release,operate%20within%20the%20tech%20industry.
[76] *SMIC: China's Main Bet Against TSMC and Samsung | WSJ*, directed by WSJ, The Wall Street Journal, 2025, 5:49, https://www.youtube.com/watch?v=b88mOUwxyJk.
[77] James Lewis, *Learning the Superior Techniques of the Barbarians: China's Pursuit of Semiconductor Independence* (Center for Strategic & International Studies (CSIS), 2019), 8–10, https://www.csis.org/analysis/chinas-pursuit-semiconductor-independence.
[78] Vox, "Why China Is Losing the Microchip War."

Figure 5 Overview of Semiconductor Chokepoints



As a result, China lags behind in terms of semiconductor sophistication.[79] This gap has prevented Beijing from achieving strategic goals, including those set out in the CS35 initiative. This technological gap has prevented Beijing from shaping global standards for emerging technologies, thereby constraining its capacity to translate industrial policy into long-term economic and geopolitical advantage over the West, particularly the US.[80] According to some experts, including Ardi Bouwers, a Dutch Sinologist, this geopolitical advantage is one of Beijing's top domestic priorities. At the same time, China's dependence on advanced foreign semiconductors undermines its ability to weaken Taiwan's "silicon shield," - the deterrent effect created by Taiwan's central role in global advanced semiconductor manufacturing - as any invasion is highly likely to severely disrupt critical supply chains on which China relies.[81]

[79] Min-Yen Chiang, "Restraining China's Chip Rise, Partnering with Taiwan for Global Stability," China Observers, June 24, 2025, https://chinaobservers.eu/restraining-chinas-chip-rise-partnering-with-taiwan-for-global-stability/.
[80] Chris Miller, *Chip War* (2022), https://www.simonandschuster.com/books/Chip-War/Chris-Miller/9781982172015.
[81] Šimov, "The Silicon Shield Erosion: Fortifying Taiwan Against Geopolitical Shocks," Institute for Security and Development Policy, June 5, 2025, https://www.isdp.eu/the-silicon-shield-erosion-fortifying-taiwan-against-geopolitical-shocks/.

Consequently, Beijing remains unable to achieve one of its long-standing goals: reunification with Taiwan.[82]

Crucially, for China to lead the semiconductors' supply chain, it not only needs TSMC's manufacturing capabilities, but also ASML's EUV lithography machines. The Dutch company is the sole producer of the machinery required to produce the most advanced chips at the centre of Beijing's technological development. Beyond ASML, the broader Dutch semiconductor ecosystem provides critical chip design expertise, automotive and industrial semiconductors, and supply-chain know-how that China requires to reduce its dependence on Western technology and move up the value chain.[83] In fact, companies such as NXP and Nexperia play critical roles in the development of key devices across the semiconductor supply chain, including secure connectivity solutions and Metal-Oxide-Semiconductor Field-Effect Transistors (MOSFETs).[84] This provides China with a direct incentive to interfere in the Dutch semiconductor industry.

3.1.2 Entry points

For Beijing, the most prominent entry point to the Dutch semiconductor sector is the concentration of intellectual property (IP) in the Brainport region.[85]

The Netherlands' position in the semiconductor market hinges on either the exclusivity of technology, such as ASML's EUV Lithography, or remaining at the forefront of other technology, such as MOSFETs. China is actively looking to replicate these technologies, albeit with limited success thus far.[86] Were China to succeed in developing its own EUV technology, either through digital and information operations or legal pressure, ASML would likely steadily lose its customer

[82] Joris Teer and Mattia Bertolini, *Reaching Breaking Point: The Semiconductor and Critical Raw Material Ecosystem at a Time of Great Power Rivalry*(The Hague Centre for Strategic Studies, 2022).
[83] Joris Teer and Mattia Bertolini, *Reaching Breaking Point: The Semiconductor and Critical Raw Material Ecosystem at a Time of Great Power Rivalry*.
[84] "A Complete Guide to MOSFET Transistors," RS, February 10, 2023, https://kr.rs-online.com/web/content/discovery/ideas-and-advice/mosfet-guide.
[85] The Brainport region is a hub of technology and innovation in Eindhoven, and houses over 5000 tech companies, including ASML, NXP, and Philips. "About ASML - The World's Supplier for the Semiconductor Industry," ASML, accessed November 20, 2025, https://www.asml.com/en/company/about-asml; "Meet High-Tech Companies and Organisations in Brainport Eindhoven," accessed December 1, 2025, https://brainporteindhoven.com/int/work/companies.
[86] "Breakthroughs or Boasts? Assessing Recent Chinese Lithography Advancements | Strategic Technologies Blog | CSIS," accessed November 20, 2025, https://www.csis.org/blogs/strategic-technologies-blog/breakthroughs-or-boasts-assessing-recent-chinese-lithography.

base and market share, as Chinese firms would almost certainly offer a cheaper alternative. Such a scenario would likely result in job losses, a loss of prestige for ASML, and a decline in the Netherlands' economic stability.[87] Equally, as China gains more Dutch technologies, companies such as NXP and Nexperia also face risks to their global relevance and competitiveness.

In addition to IP theft, another sector-specific vulnerability is China's market leverage over the Dutch semiconductor sector via its economic statecraft tactics. China represents a large market for Dutch semiconductor companies. For example, China accounts for 15%-20% of ASML's sales, despite export controls on certain semiconductor products shipped to the country.[88] China also maintains similar leverage over other parts of the Dutch semiconductor industry, with Nexperia,[89] owned by the Chinese firm Wingtech Technology, which the Chinese government partially owns, and 36% of NXP's exports heading to China in 2024.[90] This gives China notable leverage to apply economic pressure, including restricting market access, demanding technology transfers, or imposing stringent export controls on the raw materials used to produce semiconductors.

3.1.3 Likely interference scenarios

The exploitation of economic dependencies is a highly likely interference scenario for the semiconductor sector and is particularly harmful to global downstream semiconductor production. Europe is almost entirely dependent on Chinese-acquired critical raw materials (CRMs), with 93% of gallium and 84% of germanium – both key to semiconductor production – mined by Chinese companies.[91] As such, China has opted to weaponise this dependency, with Sibylline's Sam Olsen claiming that the withholding of CRM is a key tactic of China and one of the main ways it exerts influence over the West.

[87] Fanny Potkin, "Exclusive: How China Built Its 'Manhattan Project' to Rival the West in AI Chips," China, *Reuters*, December 18, 2025, https://www.reuters.com/world/china/how-china-built-its-manhattan-project-rival-west-ai-chips-2025-12-17/.
[88] "ASML Revenue Worldwide by Region 2024," Statista, accessed November 20, 2025, https://www.statista.com/statistics/789559/sales-revenue-of-asml-by-region/?srsltid=AfmBOorTwkRtm2Kv_Ccivv-Z2aI_bBG_KN54sIzj5f6jpQpY5FTviSrc.
[89] Sarah Shamim, "Why Has Dutch Government Taken Control of China-Owned Chipmaker Nexperia?," Aljazeera, October 14, 2025, https://www.aljazeera.com/news/2025/10/14/why-has-dutch-government-taken-control-of-china-owned-chipmaker-nexperia.
[90] "NXP Embraces 'China-for-China': A Strategic Shift in Semiconductor Manufacturing," Move-x, November 4, 2025, https://www.move-x.ai/news/nxp-embraces-china-for-china-a-strategic-shift-in-semiconductor-manufacturing#:~:text=Global%20chipmaker%20NXP%20Semiconductors%20is,be%20produced%20locally%20by%202025.
[91] Ewa Manthey, "China Strikes Back in the Tech War, Restricting Exports of Gallium and Germanium," ING, July 9, 2023, https://www.ing.com/Newsroom/News/China-strikes-back-in-the-tech-war-restricting-exports-of-gallium-and-germanium.htm.

While such export controls would not directly affect ASML's EUV technology, they would affect the production of other Dutch semiconductor companies, such as Nexperia and NXP, and of critical business partners, such as TSMC and Intel. This would almost certainly have knock-on effects on the Dutch semiconductor industry's profitability by limiting EUV-related business opportunities, increasing overhead costs, and/or preventing companies from producing new chip components, negatively impacting the Netherlands' economic output.

These vulnerabilities create an environment in which China is increasingly incentivised to pursue digital intrusions and targeted information operations. Companies such as ASML, Nexperia, and NXP will likely experience an increase in digital and information operations aimed at IP theft. For example, given that EUV lithography is a 'missing piece' in China's domestic semiconductor production, it is highly likely that ASML will be a specific target for China. There is already a historical precedent of such actions. In 2014, former employees of ASML founded XTAL, a US-based company with strong ties to China, who were accused of stealing source code from ASML before leaving the company. ASML sued XTAL for stealing IP 'for personal gain' and was later awarded $845 million in damages.[92]

Incidents such as the ASML/XTAL case underscore Beijing's use of foreign interference to coerce current and former employees of Dutch semiconductor companies to steal valuable information in exchange for economic benefits in China. In the case of XTAL, its founder now lives and works in Beijing.[93] Given this, the semiconductor sector should anticipate that China will continue to probe for weaknesses to facilitate its corporate espionage operations.

Corporate espionage can also occur via cyber means. In a notable example, the Chinese Advanced Persistent Threat (APT) Chimaera exploited a weakness in NXP's cybersecurity to steal IP between 2017 and 2020.[94] Either through physical or cyber means, the result would be the same: China gaining know-how and accelerating its domestic semiconductor sector.

---

[92] Georgia Butler, *ASML Engineer Who Fled Charges of Stealing Chip Tech Is Living Comfortably in China as CEO of XTAL Inc.*, June 6, 2022, https://www.datacenterdynamics.com/en/news/asml-engineer-who-fled-charges-of-stealing-chip-tech-is-living-comfortably-in-china-as-ceo-of-xtal-inc/.
[93] Georgia Butler, *ASML Engineer Who Fled Charges of Stealing Chip Tech Is Living Comfortably in China as CEO of XTAL Inc.*
[94] Dan Goodin, "Hackers Spent 2+ Years Looting Secrets of Chipmaker NXP before Being Detected," Ars Technica, November 28, 2023, https://arstechnica.com/security/2023/11/hackers-spent-2-years-looting-secrets-of-chipmaker-nxp-before-being-detected/.

It is highly likely that China would not use these tactics in isolation. A mixed-methods approach, incorporating, for example, digital and information operations and economic statecraft, is possible, in which both tactics reinforce the effects of the other. For example, IP theft and cyber espionage become easier following strategic investments in critical infrastructure. The Nexperia case is a good example, where the presence of Chinese ownership in Nexperia caused the Dutch Government to believe that Wingtech Technology was siphoning IP and moving chip production to China.[95] Given the strategic nature of Nexperia's IP, these acts were viewed as potentially eroding the Netherlands' position in the global semiconductor value chain.[96]

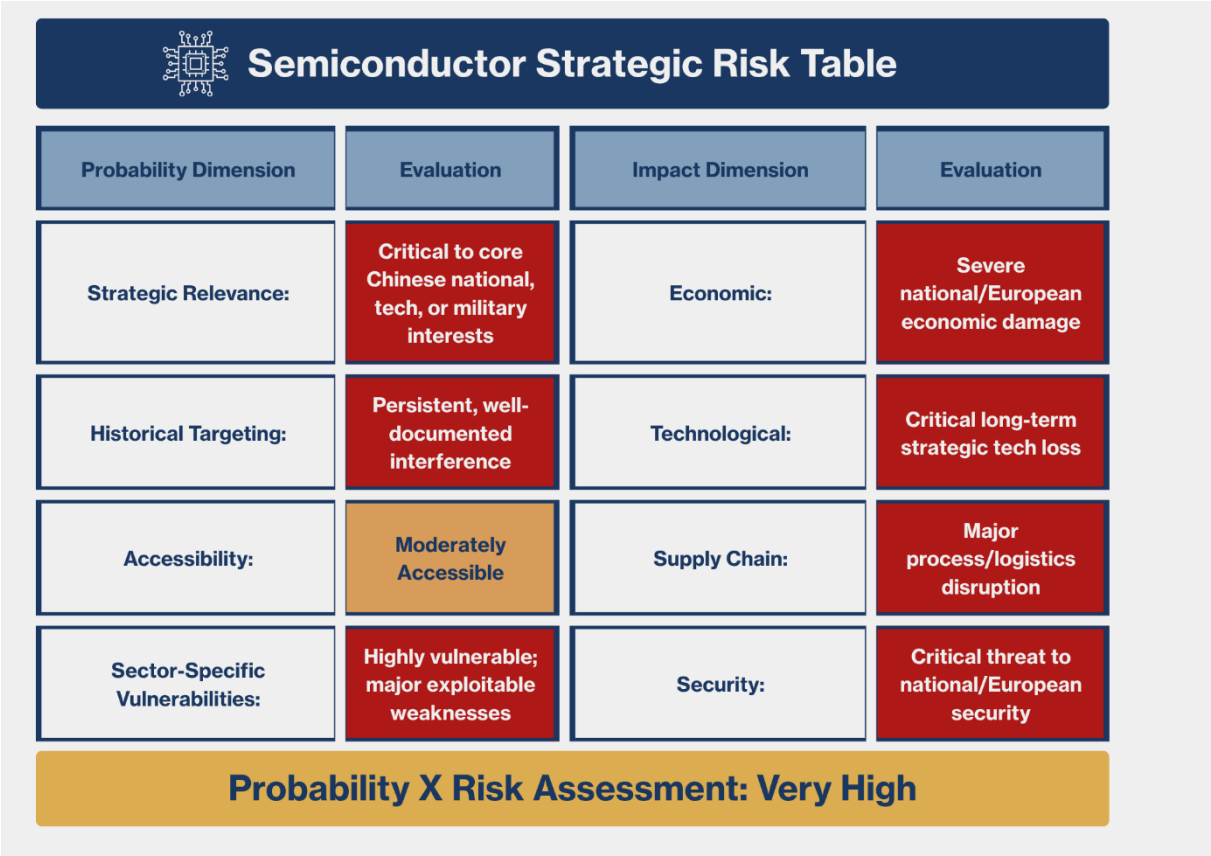
In sum, given the sensitivity of global semiconductor value chains, China is almost certain to pursue persistent interference through a combination of talent-based technological espionage (including human-enabled IP theft linked to talent recruitment, insider coercion, and post-employment technology transfer) alongside cyber-enabled espionage and IP theft targeting design software, process data, and supplier systems, as well as economic statecraft that leverages market access and critical raw material restrictions to induce compliance.

[95] "Dutch Seized Nexperia over Fears Chinese Owners Planned to Move Chip Production to China," South China Morning Post, October 18, 2025, https://www.scmp.com/news/china/diplomacy/article/3329476/dutch-seized-nexperia-over-fears-chinese-owners-planned-move-chip-production-china; Gordon Darroch, "Minister to Brief Parliament on 'Historic' Takeover at Nexperia," *DutchNews.Nl*, October 14, 2025, https://www.dutchnews.nl/2025/10/minister-to-brief-parliament-on-historic-takeover-at-nexperia/.

[96] South China Morning Post, "Dutch Seized Nexperia over Fears Chinese Owners Planned to Move Chip Production to China."

3.1.4 Strategic risk

Table 11 Semiconductor Strategic Risk



Chinese interference in the Dutch semiconductor sector presents a very high overall strategic risk due to the combination of persistent targeting and systemic consequences (see Table 11 above).

In the past, China has demonstrated persistent, sector-specific targeting of the semiconductor industry aligned with its specific industrial policy and foreign policy objectives, making future targeting highly likely, considering that Dutch technology is an essential target in Beijing's push for semiconductor self-sufficiency. For example, Chinese APT Chimaera hacked NXP, and between 2017 and 2020 stole proprietary chip designs from the Dutch company.[97] In 2023, an ex-

[97] Marc Hijink, "Spionage: Chinese hackersgroep zat jarenlang in het netwerk van de Nederlandse chipfabrikant NXP," *NRC*, November 24, 2023, https://www.nrc.nl/nieuws/2023/11/24/spionage-chinese-hackersgroep-zat-jarenlang-in-het-netwerk-van-de-nederlandse-chipfabrikant-nxp-a4182149.

employee of ASML began working for Huawei in China, after being accused of stealing company secrets on his departure.[98]

Chinese interference is further facilitated by a certain degree of accessibility. While the core technological nodes, such as high-precision clean rooms, proprietary algorithms, and restricted engineering environments, are relatively well protected, the broader ecosystem includes suppliers, subcontractors, university research partnerships, and service providers that are far more exposed. These adjacent actors represent potential entry points for economic, digital, or legal influence operations. The reliance on international talent, especially in STEM fields, and frequent global collaboration also create natural interfaces through which influence may be exerted indirectly.

The impact of Chinese interference would also be severe. Semiconductor machinery is one of the Netherlands' highest-value export categories, with extensive spillovers into domestic R&D, high-skilled employment, and supplier networks. Any disruption, whether through cyber sabotage, coercive pressure, or IP compromise, would likely reverberate not only through the Dutch economy but also through global production cycles. Because semiconductor tools are essential to nearly every modern industrial domain, interference would almost certainly undermine competitiveness, delay global chip production, or erode trust in Dutch reliability as a strategic supplier.

If China acquires advanced chipmaking know-how through cases such as XTAL or the Chimera intrusion, it is almost certain Beijing will use it to strengthen its military-industrial base, thereby enabling the development of more advanced weapons, surveillance systems, and cyber capabilities. This erodes Europe's technological edge in defence-critical components and reduces its ability to control the flow of sensitive technologies. Moreover, the loss of Dutch IP would likely allow China to become a dominant supplier of high-end chips, increasing Europe's long-term strategic dependence on a geopolitical competitor and limiting its freedom of action in security and foreign policy.

[98] Marc Hijink, "Opgestapte ASML-medewerker ging naar Huawei – en nam bedrijfsgeheimen mee," *NRC*, October 23, 2023, https://www.nrc.nl/nieuws/2023/10/23/oud-asmler-nam-bedrijfsgeheimen-mee-naar-huawei-a4178222.

Taken together, these factors create an environment in which both the probability and the impact of Chinese interference are structurally elevated. The semiconductor sector's strategic centrality, combined with historical targeting and supply-chain vulnerabilities, places it at the forefront of Dutch industrial exposure, making the strategic risk of Chinese interference systemic.

3.1.5 Gaps and policy actions

The Dutch government has taken several significant steps in recent years to mitigate foreign interference risks in the semiconductor. These measures have strengthened state capacity to intervene in cases of acute concern, yet they remain primarily oriented toward governance failures and discrete transactions, rather than the cumulative dynamics of interference.

The invocation of the Goods Availability Act in September 2025 illustrates this approach. Its use has enabled government intervention in situations where foreign ownership raised serious governance and continuity concerns, most notably in the case of Nexperia, a semiconductor company under Chinese ownership. While this instrument provides an important safeguard against loss of control in critical firms, it is inherently exceptional in nature and does not address more diffuse forms of influence that do not rise to the level of acute governance risk.[99] Similarly, the Wet VIFO (Act on Security Screening of Investments, Mergers and Acquisitions), implemented in 2023, has strengthened scrutiny of foreign investments in a limited set of key technologies deemed vital to national security, including semiconductors.[100] The Act represents a substantial improvement in ex ante risk screening. However, its focus remains largely transaction-driven and firm-specific, leaving limited oversight of long-term access, minority stakes, supplier dependencies, or evolving risk profiles following approval.

Initiatives such as Project Beethoven, a €2.5 billion government-supported effort to strengthen semiconductor production capacity in the Netherlands, signal an emerging awareness of dependency-related vulnerabilities.[101] While such industrial policy measures can reduce

[99] Ministerie van Economische Zaken, "Minister of Economic Affairs Invokes Goods Availability Act - News Item - Government.Nl," nieuwsbericht, Ministerie van Algemene Zaken, October 12, 2025, https://doi.org/10/12/minister-of-economic-affairs-invokes-goods-availability-act.
[100] "Wet veiligheidstoets op investeringen, fusies en overnames | Bureau Toetsing Investeringen," accessed November 17, 2025, https://www.bureautoetsinginvesteringen.nl/het-stelsel-van-toetsen/wet-veiligheidstoets-investeringen-fusies-en-overnames.
[101] Ministerie van Economische Zaken en Klimaat, "The Netherlands to Invest €2.5 Billion to Strengthen Business Climate for Chip Industry in Brainport Eindhoven - News Item - Government.Nl," nieuwsbericht, Ministerie van Algemene Zaken, March 28, 2024,

exposure to external leverage over time, they are not yet fully integrated into a security-oriented framework for assessing foreign interference risks. More broadly, existing measures remain better suited to regulating product and ownership flows than to governing knowledge flows. Export controls and investment screening do not capture human-enabled technology transfer, access to process knowledge, or informal diffusion through supplier relationships and labour mobility. This is particularly relevant in a sector where competitive advantage is increasingly rooted in tacit knowledge and system integration rather than in individual components. While some steps have been taken in this direction, such as the approval in March 2025 of a new law criminalising digital and diaspora espionage, these remain insufficient.[102]

In the private sector, leading companies have taken proactive steps by conducting internal risk assessments that incorporate geopolitical tensions, IP theft, supply-chain disruption, and cyber threats.[103] However, these efforts remain uneven across the broader ecosystem and rely heavily on voluntary action rather than sector-wide standards or coordinated state support.

Taken together, current Dutch policy provides meaningful protection against transactional risks, but remains less effective in addressing attritional threats arising from cumulative knowledge transfer, dependency formation, and sustained foreign access across the semiconductor value chain. Building on existing policy instruments, the next phase of Dutch mitigation efforts should focus on closing the gap between transactional control and systemic resilience. To do so, four main policy actions can be recommended:

1. **Reinforce investment screening mechanisms**
   Expand Wet VIFO's criteria to include downstream IP-transfer risks and mandate post-investment audits for high-risk cases. Increase enforcement transparency to strengthen deterrence.
2. **Develop a national semiconductor continuity strategy**
   Establish public–private financing mechanisms to support domestic fabrication, advanced packaging, and materials production. Reduce reliance on suppliers in high-risk jurisdictions.

https://www.government.nl/latest/news/2024/03/28/the-netherlands-to-invest-%E2%82%AC2.5-billion-to-strengthen-business-climate-for-chip-industry-in-brainport-eindhoven.

[102] "Legislation to Be Broadened to Make More Forms of Espionage a Criminal Offence," nieuwsbericht, Ministerie van Justitie En Veiligheid, Ministerie van Algemene Zaken, March 18, 2025, https://www.government.nl/latest/news/2025/03/18/legislation-to-be-broadened-to-make-more-forms-of-espionage-a-criminal-offence.

[103] "How ASML Manages Risk," ASML, accessed November 17, 2025, https://www.asml.com/en/company/governance/risk.

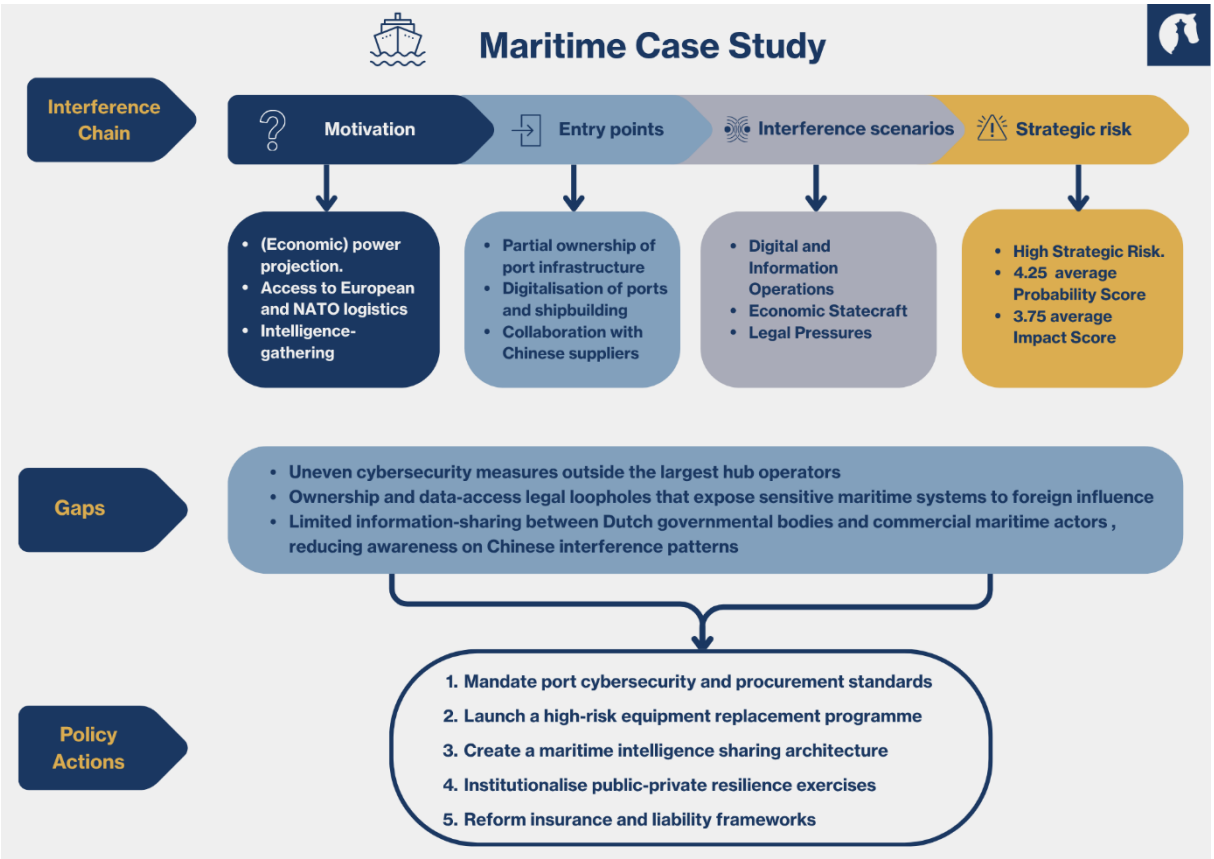
3. **Pursue selective industrial cooperation to shape mutual interdependence**
   Identify narrowly defined areas for continued economic and technological cooperation with China that create reciprocal dependencies without exposing core IP or critical chokepoints. Structured engagement can provide leverage, increase predictability, and reduce incentives for coercive or covert interference while preserving Dutch strategic autonomy.
4. **Introduce high-assurance Operational Security (OpSec) certification**
   Require enhanced cybersecurity, insider-threat mitigation, and supply-chain integrity measures for companies handling advanced nodes or classified production.
5. **Strengthen personnel vetting for sensitive sites**
   Develop risk-based security clearance requirements for key technical and managerial roles, ensuring ethical, non-discriminatory implementation.

Together, these adjustments would strengthen the Netherlands' ability to protect its semiconductor sector not only from immediate disruptions, but from the gradual erosion of strategic advantage that foreign interference is designed to produce.

While several of the vulnerabilities identified in the semiconductor sector are linked to its highly specialised and innovation-driven character, many of the underlying challenges extend beyond this sector. Fragmented intelligence sharing, limited post-investment oversight, and the difficulty of protecting IP recur across Dutch strategic industries. These cross-sectoral dynamics are addressed in section 4, which assesses their broader implications for Dutch national security and outlines systemic policy responses.

3.2 The Maritime Sector

Figure 2 Overview of Maritime Case Study



3.2.1 Motivation

China's interest in the Dutch maritime sector is driven less by technological gaps and more by structural leverage.Interference motivations include maintaining China's economic edge in shipbuilding, controlling key maritime chokepoints, securing access to advanced maritime technologies, and strengthening China's global maritime power projection.

Over the past few decades, China has cemented its position as the world's dominant power in shipbuilding and logistics. In 2024, China produced more commercial ships than the combined output of the next four major shipbuilding hubs (see Figure 7).[104] Chinese firms' strong control over shipbuilding, combined with state-driven capital and strategic port investments through

[104] *Inside the Strategies That Made China a Shipbuilding Powerhouse*, directed by The WSJ, The Wall Street Journal, 2024, 8:20, https://www.wsj.com/video/series/us-vs-china/inside-the-strategies-that-made-china-a-shipbuilding-powerhouse/74DB710C-092F-4473-80FE-AC3D547A82A2.

initiatives such as the "One Belt, One Road", have allowed Beijing to largely circumvent geopolitical volatility and become a driver of global supply chains.

While China currently dominates the maritime and shipbuilding sectors, any potential Western incursions into these sectors will likely be of great interest to Beijing. Countries like the US account for only 0.04% to 1% of the world's commercial ship production. However, the Netherlands was estimated to account for approximately 4% of the volume of built ships in 2023.[105] While nowhere near countries such as South Korea or Japan (26% and 14%, respectively), Dutch maritime firms do represent a more regionally oriented alternative for Western customers to China-manufactured maritime products, albeit at a higher price (see Figure 7 for a further breakdown).

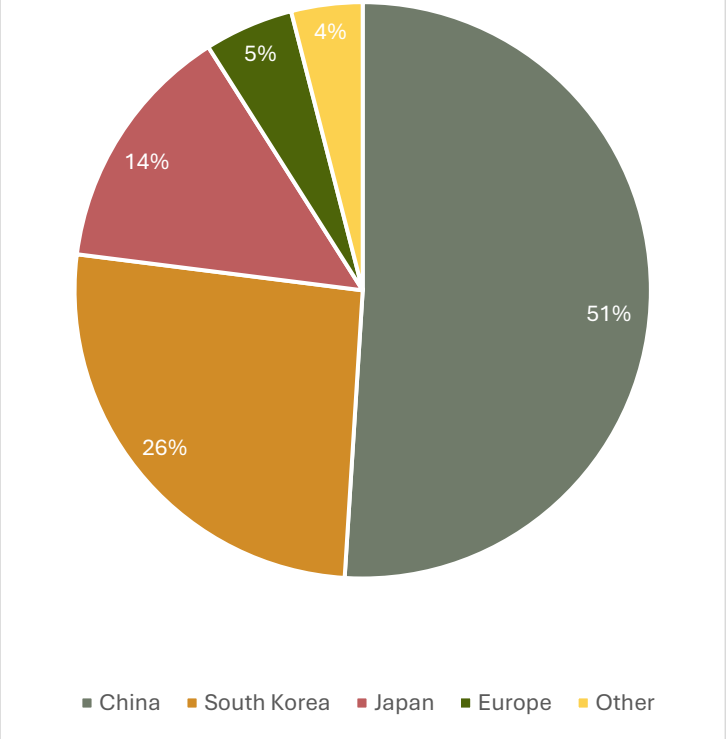


Figure 1: Commercial Shipbuilding Output per country/region

In tandem, China has utilised its strong maritime credentials to build a global network of ports and logistics hubs to strengthen its power-projection capabilities. According to the Council of Foreign Relations' (CFR) "Tracking China's Control over Overseas Ports" dashboard, "China operates or has ownership in at least one port in every continent except Antarctica".[106]

In addition, the CFR found Chinese entities have "acquired varied equity ownership or operational stakes" in at least 129 port projects worldwide, including an alleged 25-37.5% ownership in the

[105] Mariska Buitendijk, "Dutch Govt and Sector Put EUR 60 Million in Innovative Shipbuilding," SWZ Maritime, October 27, 2023, https://swzmaritime.nl/news/2023/10/27/eur-60-million-for-innovative-dutch-shipbuilding/#:~:text=Critical%20lower%20limit%20in%20sight&text=The%20government%20and%20the%20sector,'.
[106] Council on Foreign Relations, "Tracking China's Control of Overseas Ports," Council on Foreign Relations, August 26, 2024, https://www.cfr.org/tracker/china-overseas-ports.

Rotterdam EUROMAX Container Terminal.[107] The port of Rotterdam is the largest in Europe, and among the largest worldwide. Furthermore, the Port of Rotterdam is closely linked to Sino-German trade. President Xi Jinping has personally emphasised the intrinsic link between ports and China's economic development during a 2017 visit to the Tieshan Port in Guangxi Province, where he stated, "We often say that to get rich we must first build roads; but in coastal areas, to get rich we must also first build ports". [108]

Lastly, Beijing's investment in maritime infrastructure, including ports and shipyards, is a valuable source of economic and strategic intelligence gathering operations. For example, access to port data systems, logistics platforms, or maritime sensors can provide strategic insights into NATO military movements, sanctions enforcement, and commercial activity near or at ports in which China has invested, all of which are relevant to China's strategic planning. Dutch firms are world leaders in shipbuilding equipment, maritime robotics, offshore engineering, and autonomous vessel technologies. As such, interfering with or gaining access to these capabilities would be consistent with the objectives set out in the Mic25 or CS35 programmes, which aim to help China advance its naval and commercial fleet modernisation vis-à-vis its Western counterparts and prepare it for potential geopolitical conflicts.[109]

3.2.2 Entry points

China's motivation translates into concrete entry points within the Dutch maritime ecosystem, most notably through the Port of Rotterdam. The port accounts for approximately 6.2% of Dutch GDP and handles over 30% of all EU container traffic, making it a central node not only for the Netherlands but for European supply chains more broadly. [110]

Chinese involvement in Rotterdam, particularly through China Ocean Shipping Corporation (COSCO) and Hutchison Port Holding's stakes in the EUROMAX terminal, creates potential access to sensitive operational data, supply-chain visibility, and, indirectly, NATO-related

[107] Council on Foreign Relations, "Tracking China's Control of Overseas Ports."
[108] Council on Foreign Relations, "Tracking China's Control of Overseas Ports."
[109] Federal Bureau of Investigation, "CHINA: THE RISK TO CORPORATE AMERICA."
[110] "Het Rotterdam-Effect: Economische Betekenis Haven Is Twee Maal Groter Dan Tot Nu Toe Berekend | Port of Rotterdam," accessed November 20, 2025, https://www.portofrotterdam.com/nl/nieuws-en-persberichten/het-rotterdam-effect-economische-betekenis-haven-twee-maal-groter-dan-tot.

logistics.[111] While this investment has delivered economic benefits, it simultaneously creates structural dependencies that China is likely to exploit. Even short-term interference at Rotterdam is almost certain to generate disproportionate economic, reputational, and political effects.[112]

Beyond ownership stakes, digitalisation represents an additional entry point. The Dutch maritime sector is undergoing a "smart transformation," integrating AI asset inspections, automated logistics platforms, and data-driven port management systems.[113] While this enhances efficiency, it also expands the attack surface available for cyber intrusion and espionage. Chinese state-linked firms operating within port ecosystems, such as LOGINK, are subject to coercion under China's National Intelligence Law, increasing the risk that commercial access could be leveraged for intelligence or cyber operations.[114] Dutch ports have been the target of cyberattacks in the past: in 2023, multiple Dutch ports' websites went down following a DDoS attack by NoNames057(16),[115] a pro-Russian hacktivist group.[116] While DDoS attacks are low-level cyberattacks that cause limited damage to IT infrastructure, addressing such incidents drains capacity, resources, and time, which, if timed properly, could allow more overtly destructive or disruptive operations – e.g., wiper malware – to be successfully launched.

Entry points also exist outside ports. As emerged from an interview with a security-focused employee of a Dutch firm operating in the maritime domain, Dutch maritime firms often separate military-related operations from commercial activities through air-gapped systems. However, commercial operations remain exposed due to reliance on collaboration with Chinese suppliers, shipyards, and local workers. The routine sharing of blueprints and operational data increases the risk of technology leakage, particularly of dual-use innovations relevant to the People's Liberation Army Navy (PLAN).[117] As Ardi Bouwers explains, accessibility often arises from

[111] Karin Smit Jacobs, *Chinese Strategic Interests in European Maritime Ports* (European Parliament, 2023), 1.
[112] For a more in-depth analysis on Chinese influence on European and Dutch ports, see: Xiaoxue Martin et al., *China's Strategic Relevance to the Port of Rotterdam* (Clingendael, 2023), https://www.clingendael.org/publication/chinas-strategic-relevance-port-rotterdam.
[113] "Smart Infrastructure," Port of Rotterdam, 2025, https://www.portofrotterdam.com/en/port-future/smart-infrastructure; "How Rotterdam Becomes the Smartest Port in the World," Axians, 2025, https://www.axians.com/use-case/how-rotterdam-becomes-the-smartest-port-in-the-world/.
[114] Tereza Corradi, "China's LOGINK: Securing Maritime Data in European Ports," Articles, *Chinaobservers*, February 22, 2024, https://chinaobservers.eu/chinas-logink-securing-maritime-data-in-european-ports/.
[115] "Dutch Ports' Websites Offline for Hours, Days Due to pro-Russian Cyber Attacks | NL Times," June 14, 2023, https://nltimes.nl/2023/06/14/dutch-ports-websites-offline-hours-days-due-pro-russian-cyber-attacks.
[116] Hacktivists are individuals or groups who utilise their hacking skills for digital political or social activism. They are known to possess less robust technical skills than their state-sponsored counterparts and typically engage in minimally destructive or disruptive cyberattacks, such as DDoS attacks, website defacement, or data breaches.
[117] Ardi Bouwers and Alex Krijger, "The China Challenge Impact of the Politicised Business Environment on Dutch Companies in China."

ignorance of the threat of Chinese interference, which the maritime sector has relatively little experience with.

3.2.3 Likely interference scenarios

Given China's long-term interest in European influence, outright destructive interference in Dutch ports is unlikely during peacetime. Instead, the most plausible scenarios involve intelligence gathering, cyber-enabled espionage, and low-level digital disruption. These will likely include access to logistics databases, monitoring of cargo flows, or manipulation of scheduling and port management systems.

Cyber operations are particularly likely due to the sector's digitalisation and decentralised structure. Chinese state-linked firms operating within ports are likely to be coerced into facilitating intrusive cyber activities, such as data exfiltration, reconnaissance, or disruptive actions like DDoS or ransomware attacks, under provisions such as China's 2017 National Intelligence Law.[118] While such activities would likely remain calibrated to avoid escalation, China has already demonstrated its capabilities in 2024, when the Chinese APT group, Mustang Panda, spied on Dutch vessels, obtaining information about various container shipping companies.[119]

More severe cyber-disruption scenarios become plausible during geopolitical crises, such as a military confrontation over Taiwan. In such contexts, Chinese interference will likely be aimed at delaying or obstructing NATO logistics (e.g., delaying the production of NATO ships produced by Dutch companies), complicating European responses, or obscuring military transport movements. Although China has not historically conducted destructive cyberattacks, it possesses sophisticated APT capabilities that are highly likely to enable operations comparable in impact to Russia's NotPetya attack on Maersk, which disrupted port operations worldwide and caused losses of $200- $ 300 million.[120] It is also plausible that such destructive attacks would be

[118] James Austin et al., *Policy Brief Addressing State-Linked Cyber Threats to Critical Maritime Port Infrastructure* (CCCDCOE NATO Cooperative Cyber Defence Center of Excellence, 2025), 3, https://ccdcoe.org/uploads/2025/07/CCDCOE_Policy_Brief.pdf.
[119] "China-Linked Group Uses Malware to Try to Spy on Commercial Shipping, New Report Says," NBC News, May 14, 2024, https://www.nbcnews.com/news/world/china-linked-group-malware-spy-commercial-shipping-cargo-report-eset-rcna152129; "Dutch Ports' Websites Offline for Hours, Days Due to pro-Russian Cyber Attacks | NL Times," June 14, 2023, https://nltimes.nl/2023/06/14/dutch-ports-websites-offline-hours-days-due-pro-russian-cyber-attacks.
[120] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Tags, *Wired*, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

launched either in tandem with, or after, more disruptive cyberattacks, such as Distributed Denial of Service (DDoS) attacks, as those launched against the Taiwanese government before then-US Speaker of the House of Representatives Nancy Pelosi's trip in 2022.[121] Such attacks would be intended to cause chaos or to limit allies' coordination capabilities during a potential invasion.

Technology and IP theft remain another likely interference vector. As emerged via interviews with maritime sector experts, commercial maritime collaborations provide opportunities for the acquisition of dual-use technologies that are likely to enhance China's naval and commercial capabilities, particularly in autonomous vessels, offshore engineering, and advanced ship systems.

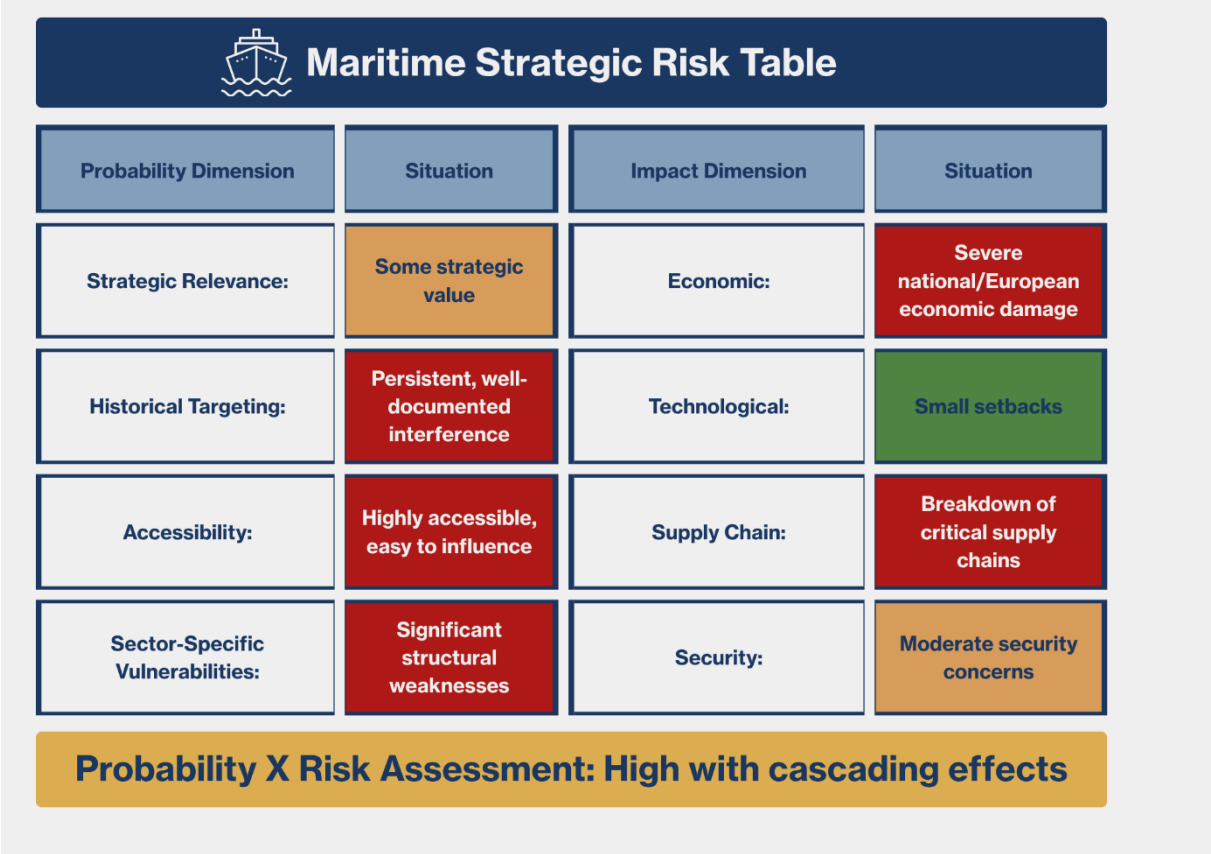
Another likely scenario involves the use of economic statecraft and legal pressures, leveraging China's presence in Dutch ports, maritime infrastructure, and shipbuilding supply chains. It is probable this activity will take the form of informal pressure on Chinese shipping lines, logistics firms, or terminal operators to reduce activity at key ports such as Rotterdam, delay investments, or reconsider long-term commercial commitments. Even limited shifts in cargo flows or port calls are likely to have symbolic and economic effects, given the sector's sensitivity to volume, reliability, and investor confidence. Such measures would likely be calibrated to signal displeasure rather than provoke a full rupture, allowing China to retain access to EU markets while increasing the perceived costs of Dutch policy choices. In parallel, China is likely to exploit existing dependencies on Chinese technology, services, or capital within port operations to amplify uncertainty or resistance to tighter security and sanctions enforcement. [122]

Highly likely scenarios of interference in the Dutch maritime sector therefore include cyber-enabled digital and information operations targeting scheduling, customs, and terminal systems, potentially causing disruption during crises and providing visibility into cargo flows, sanctions enforcement, military logistics, and dual-use technologies, together with economic statecraft that exploits dependencies on materials and supply chains, and legal pressure enabled by ownership stakes in maritime infrastructure, shipping lines, logistics firms, or terminal operators.

[121] AJ Vicens, "Taiwanese Government Sites Hit with DDoS Attacks Ahead of Pelosi's Visit," Cyberscoop, August 2, 2022, https://cyberscoop.com/taiwan-china-ddos-pelosi-visit/.
[122] Xiaoxue Martin et al., *China's Strategic Relevance to the Port of Rotterdam*, 13–15.

3.2.4 Strategic risk

Table 0-12 Maritime Strategic Risk



The Dutch maritime sector constitutes a high strategic-risk domain in the context of potential Chinese interference, primarily due to its structural openness, international embeddedness, and central role in Dutch and European supply chains (see Table 12 above). Unlike sectors such as semiconductors, where strategic vulnerability is driven by technological concentration and intellectual property leadership, the maritime domain derives its exposure from scale, accessibility, and persistent foreign interaction.

¡The probability of interference is high because the maritime sector is inherently open and continuously accessible. Ports require ongoing interaction with foreign shipping lines, terminal operators, equipment suppliers, digital service providers, and logistics platforms. Chinese state-linked firms occupy significant positions across several of these layers, including shipping, port

equipment, and digital logistics technologies.[123] The decentralised and high-throughput nature of port operations and shipbuilding supply chains further complicates oversight, making detection and attribution more difficult than in tightly controlled industrial environments. This creates a complex ecosystem with numerous interfaces -physical, digital, economic- where interference can be exerted.

The sector has also experienced historical targeting attempts, including the 2024 cyber intrusion by the Chinese APT group Mustang Panda, which spied on Dutch vessels and obtained information about various container shipping companies.[124]

Dutch maritime infrastructure depends on global suppliers of cranes, port management systems, navigation equipment, and digital logistics software. In several of these categories, Chinese state-linked firms have strong market positions. The breadth of subcontractors and service providers operating within ports also introduces the possibility of indirect influence through commercial relationships. Moreover, logistics flows passing through Rotterdam often involve Chinese shipping giants, creating regular operational links through which interference might be easily executed and undetected.

The impact of interference would also be high and cascading. The Dutch economy depends heavily on uninterrupted maritime trade, particularly in energy imports, petrochemicals, and industrial inputs. In the Netherlands, the maritime sector employs over 310,000 people and generates more than €94 billion in revenue.[125] Even a limited disruption, such as delays in port operations or manipulation of scheduling systems, is likely to impose substantial costs. Additionally, such disruptions would likely rapidly propagate across interconnected systems. Energy supply chains would almost certainly be affected through delays in oil, LNG, and refined product flows. EU trade would likely face immediate bottlenecks, with knock-on effects for manufacturing, agriculture, and consumer markets. Given Rotterdam's role as a logistical hub,

[123] Karin Smit Jacobs, *Chinese Strategic Interests in European Maritime Ports*.
[124] NBC News, "China-Linked Group Uses Malware to Try to Spy on Commercial Shipping, New Report Says"; "Dutch Ports' Websites Offline for Hours, Days Due to pro-Russian Cyber Attacks | NL Times," June 14, 2023.
[125] Eelco Rietveld, Martijn Streng, Ties de Leijer, Sandra van Putten, et al., *Maritieme Monitor 2025* (Stichting Nederland Maritiem Land, 2025), https://open.overheid.nl/documenten/f5b27ee7-3537-407e-9816-bc8302c36921/file.

disruptions would likely also spill over into road, rail, and inland waterway networks across the Netherlands and neighbouring states, as confirmed by two different interviewees.

Beyond economic and supply-chain effects, interference would carry broader strategic implications. Access to port logistics and cargo data provides visibility into sanctions enforcement, strategic industrial dependencies, and military mobility. Any erosion of data integrity or operational autonomy in Dutch ports would therefore have implications for NATO force movements, EU supply-chain governance, and European strategic autonomy.[126] While the technological and direct security impacts may be less acute than in defence-industrial sectors, the maritime domain's role as a systemic enabler magnifies risk.

Taken together, the combination of high probability and cascading impact places the Dutch maritime sector in a high-risk category with significant strategic consequences.

3.2.5 Gaps and policy actions

The Dutch government and private maritime sector have taken several concrete steps to protect the maritime domain from foreign interference. In late 2024, the Ministry of Infrastructure and Water Management, the National Coordinator for Security and Counterterrorism (NCTV), and the Seaports Trade Organisation (BOZ) jointly launched a Cyber Strategy for Dutch Seaports, evolving the FERM Foundation into a national cybersecurity coordination platform that brings together major port authorities to share threat intelligence, standardise cyber defence practices, and strengthen incident responses across logistics and digital systems essential to maritime operations.[127] Complementing these efforts, the government and industry have launched the Sectoragenda Maritieme Maakindustrie to revitalise Dutch shipbuilding capacity and reduce strategic vulnerabilities, committing €60 million in joint investment in 2024–2025 to secure and sustainably innovate the Dutch shipbuilding sector.[128]

---

[126] Karin Smit Jacobs, *Chinese Strategic Interests in European Maritime Ports*.
[127] Mariska Buitendijk, "Dutch Seaports Launch Nationwide Cyber Security Platform," *SWZ Maritime*, December 13, 2024, https://swzmaritime.nl/news/2024/12/13/dutch-seaports-launch-nationwide-cyber-security-platform/.
[128] "Kabinet en sector versterken scheepsbouw: noodzaak vergroenen en veiligheid," nieuwsbericht, Ministerie van Economische Zaken en Klimaat, Ministerie van Algemene Zaken, October 26, 2023, https://doi.org/10/26/kabinet-en-sector-versterken-scheepsbouw-noodzaak-vergroenen-en-veiligheid?utm.

This effort helps reduce external dependencies and, in turn, the likelihood that China will interfere through economic statecraft. At the same time, port authorities and private actors such as Portbase have advanced secure data-sharing systems and container-processing security to reduce vulnerabilities in digital logistics chains and mitigate credential misuse through the *Secure Chain* system.[129] Industry actors in the maritime manufacturing and shipbuilding sectors, such as the International Association of Classification Services, also increasingly engage with 'cybersecurity by design' practices to ensure resilience is built into vessels, systems, and supply networks from the ground up.[130]

Nonetheless, significant policy gaps persist across the maritime sector, which is highly likely to be exploited by state-linked actors. Cybersecurity adoption remains uneven outside the largest hub operators, with smaller shipyards, logistics firms and connected service providers often lacking enforcement mechanisms or standardised practices to protect operational technology and critical data flows. Regulatory frameworks have yet to close ownership and data-access loopholes that expose sensitive maritime systems to foreign influence, including through third-party cloud services or investment structures.

Additionally, interviews with experts and sectoral employees indicate that current information-sharing between Dutch government bodies and commercial maritime actors is limited, reducing awareness of patterns of Chinese interference across the public and private sectors. Procurement standards in shipbuilding and maritime logistics do not yet systematically integrate geopolitical risk assessments, leaving strategic assets under-protected against coercive economic statecraft and technology transfer. These gaps can be easily exploited by China, whose interference capabilities expertly leverage digital, economic, and legal loopholes.

[129] "Secure Chain," *Portbase*, n.d., accessed January 6, 2026, https://www.portbase.com/en/programs/secure-chain/; "Port of Rotterdam Hits 500,000 Secure Chain Containers, Strengthening Global Import Security," *EuropaWire*, September 18, 2024, https://news.europawire.eu/port-of-rotterdam-hits-500000-secure-chain-containers-strengthening-global-import-security/eu-press-release/2024/09/18/12/27/03/140717/.
[130] "Addressing Cyber Resilience of Ships," IACS International Association of Classification Societies, 2024, https://iacs.flumeserver.co.za/news/iacs-ur-e26-and-e27-press-release/.

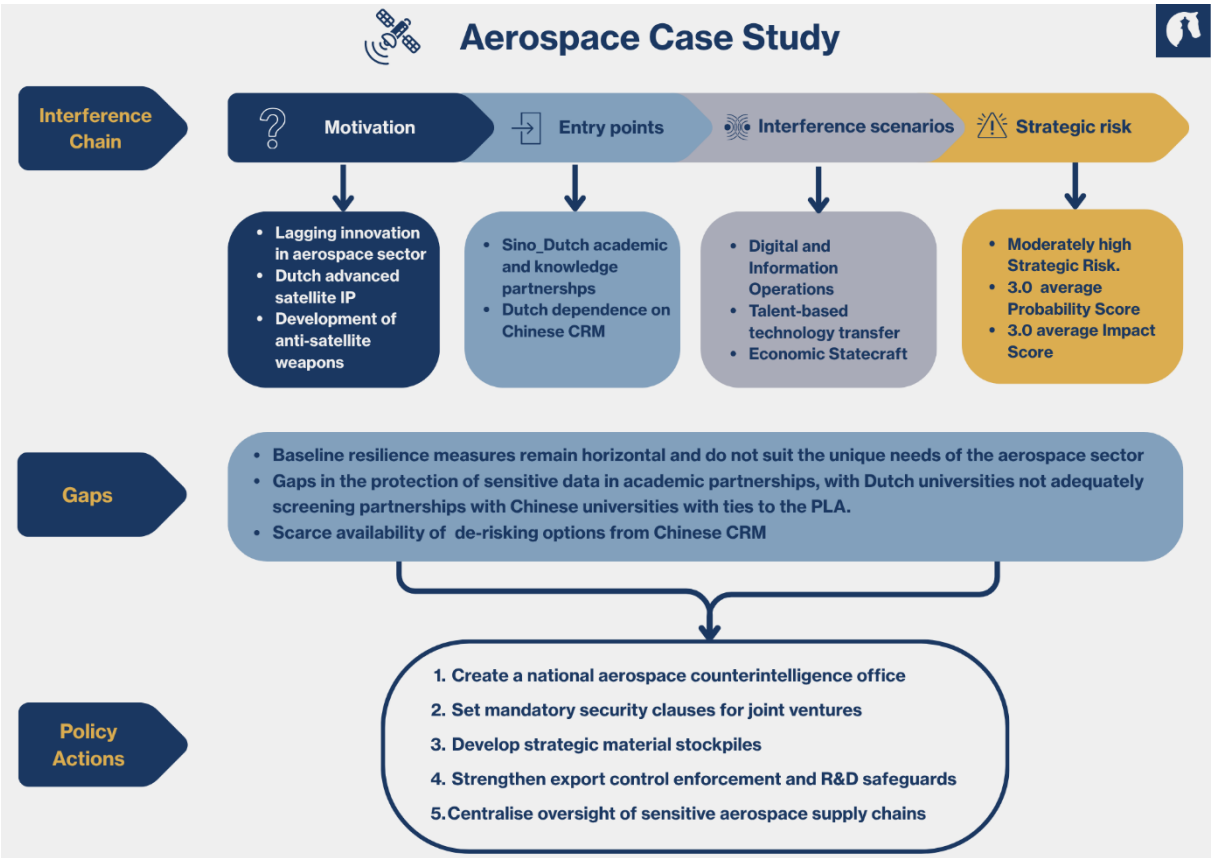
To enhance the protection of the Dutch maritime sector against Chinese interference, a few measures can be taken:

1. **Mandate port cybersecurity and procurement standards**
   Operationalise the "Cyber Strategy for Dutch Seaports" as a compulsory requirement tied to licensing. Establish EU-aligned procurement rules excluding high-risk vendors.
2. **Launch a high-risk equipment replacement programme**
   Provide financial incentives to replace Chinese-built cranes, control systems, and software with trusted domestic or European alternatives.
3. **Create a maritime intelligence sharing architecture**
   Introduce a classified "Trusted Maritime Information Exchange" enabling the AIVD/MIVD to securely share actionable threat intelligence with vetted operators.
4. **Institutionalise public–private resilience exercises**
   Conduct annual national-level exercises simulating cyber disruptions, hardware sabotage, and logistical crises to improve preparedness and cross-sector coordination.
5. **Reform insurance and liability frameworks**
   Incentivise compliance by linking cyber-resilience standards to insurance eligibility and by clarifying liability for operators using high-risk foreign hardware.

The maritime sector's exposure to foreign interference is shaped by its role as a critical infrastructure backbone and global logistical hub. However, the vulnerabilities identified, such as reliance on foreign manufacturers and suppliers, data-intensive operations, and foreign ownership, are not unique to the maritime sector. Similar patterns of dependency and digitalisation of processes are evident in other strategic sectors. The maritime case, therefore, underscores the need for coordinated, national-level approaches to interference risk management, which are further developed in section 4.

3.3 The Aerospace Sector

Figure 8 Overview of Aerospace Case Study



3.3.1 Motivation

China's interest in the Dutch aerospace sector is driven by a combination of technological lag, dual-use sensitivity, and strategic dependence. Unlike the maritime and semiconductor industries, Beijing has not yet succeeded in transforming its domestic aerospace organisations into global industry leaders, particularly in the commercial aircraft segment. Chinese firms continue to face a structural disadvantage relative to Western incumbents such as Boeing and Airbus, particularly in technological sophistication and global market penetration.

As with other state priorities, the commercial aircraft sector has received substantial state-directed funding from Beijing to accelerate its catch-up. China's largest commercial aircraft

manufacturer, the Commercial Aircraft Corporation of China (COMAC), has received at least USD 45 billion in state funding since its inception in 2008. This level of support exceeds the approximately USD 22 billion received by Airbus during the same period, according to data from the World Trade Organisation (WTO) and the Centre for Strategic and International Studies (CSIS).[131] Despite this investment, Chinese commercial aircraft manufacturers remain heavily reliant on Western component suppliers, particularly those based in the United States and Europe.

The case of COMAC's C919 aircraft illustrates this dependency clearly. As seen in the table below, of the 82 components, materials, and other items (e.g., avionics and airframes) used in the production of the C919, 48 and 26 are sourced entirely or partially from U.S.- and Europe-based firms, respectively (see table 13 below).[132] These include critical subsystems such as avionics, power systems, airframes, and specialised materials. While China dominates upstream rare earth production (accounting for 59% of global mining, 91% of refining, and 94% of permanent magnet manufacturing), it remains dependent on Western firms for high-value aerospace components and systems integration.[133]

Table 13 Production location of C919 components

	US	Europe	Asia-Pacific	China	Total
Airframe	9 (1)	6 (3)	3 (1)	8 (3)	22 (4)
Avionics	12 (2)	1	1	2 (2)	14 (2)
Power Systems	10 (3)	11 (4)	2 (2)	2 (1)	20 (5)
Components	14	4 (1)	0	2 (1)	19 (1)
Materials	3	4	0	0	7
Total	48 (6)	26 (8)	6 (3)	14 (7)	82 (12)

[131] Scott Kennedy, "China's Stalled Aircraft Dreams," CSIS, December 7, 2020, https://www.csis.org/programs/chinese-business-and-economics/chinas-stalled-aircraft-dreams.
[132] Scott Kennedy, "China's COMAC: An Aerospace Minor Leaguer," CSIS, December 7, 2020, https://www.csis.org/blogs/trustee-china-hand/chinas-comac-aerospace-minor-leaguer.
[133] Holly Ellyatt, "Europe Has Rare Earths but, for Now, It's at China's Mercy like Everyone Else," CNBC, November 19, 2025, https://www.cnbc.com/2025/11/19/europe-has-rare-earths-but-for-now-its-at-chinas-mercy.html#:~:text=China%20dominates%20the%20rare%20earths,its%20vulnerabilities%20to%20geopolitical%20disruptions

This configuration has produced a relationship of mutual dependence between China and the West in aerospace: Western manufacturers rely on Chinese rare earths and materials, while Chinese aircraft programmes depend on Western technology. From Beijing's perspective, this dependency represents a strategic vulnerability that it seeks to reduce. Aerospace technologies are deeply intertwined with military aviation, space systems, and power projection capabilities, making them central to China's long-term geopolitical objectives, including potential military operations in the Indo-Pacific.

As a result, Beijing has a strong incentive to monitor, access, and, where possible, acquire sensitive aerospace know-how from leading Western ecosystems. The Netherlands, with its concentration of specialised aerospace manufacturing, avionics expertise, and defence-adjacent research institutions, occupies a particularly attractive position within this landscape. The Dutch space ecosystem is particularly of interest to China. The Netherlands hosts over 200 organisations, including companies, research institutes, and government entities, operating in the space sector. This includes Airbus Defence & Space Netherlands (a producer of satellite solar arrays and launcher structures), ISISPACE (a Delft-based smallsat builder), and research institutions such as SRON (Space Research Organisation of the Netherlands) and TNO.[134] The Netherlands excels at the development of earth observation and satellite components and has recently signed an agreement with ISISPACE to develop the first Dutch military satellite constellation, PAMI-I.[135] China, which is looking into expanding its (military) satellite capabilities and at the same time reducing its dependence on Western companies in the aerospace sector, has thus a concrete motivation to interfere with the Dutch aerospace sector, namely to acquire newly-developed, cutting-edge space technology.[136]

3.3.2 Entry points

China's motivations translate into several concrete entry points within the Dutch aerospace ecosystem. A defining vulnerability of the sector lies in the prevalence of dual-use technologies that are directly applicable to both civilian and military aerospace platforms. This is often

[134] Remco Timmermans, "Space Industry Map of The Netherlands 2022," *Groundstation*, January 24, 2022, https://www.groundstation.space/business/space-industry-map-of-the-netherlands-2022/.
[135] "Nieuwe satelliet van Nederlandse makelij," nieuwsbericht, Ministerie van Defensie, Ministerie van Defensie, November 22, 2024, https://www.defensie.nl/actueel/nieuws/2024/11/22/nieuwe-satelliet-van-nederlandse-makelij.
[136] "China Seeking Dutch Space Technology -Military Intelligence Agency," Space, *Reuters*, April 19, 2023, https://www.reuters.com/technology/space-seeking-dutch-space-technology-military-intelligence-agency-2023-04-19/.

concentrated in a few key Dutch companies, such as Fokkers or Airbus NL, making this type of dual-use IP particularly vulnerable to foreign interference through digital operations.[137]

The openness of research and innovation networks further amplifies exposure. The Netherlands hosts multiple academic and research partnerships with Chinese institutions, resulting in over 90 Chinese researchers gaining access to Dutch aerospace-related knowledge environments.[138] This creates sustained opportunities for technology transfer, with China already persistently targeting Dutch knowledge institutions, firms, and scientists in this field as it seeks to develop anti-satellite weapons.[139] IP theft in the Dutch aerospace sector is not new: in 2023, the head of Aratos group, a Dutch-Greek Satellite Technology firm, was arrested and charged with spying for Russia and smuggling military and dual-use technology to Russia.[140]

According to our interview with a Netherlands-based sinologist, some universities are unaware of the Chinese threat. Particularly worrying are the connections with the 'Seven Sons of National Defence', a group of seven Chinese universities with close links to China's military-industrial complex. The Australian Strategic Policy Institute (ASPI) recommended in 2019 that Western universities should terminate collaborations with the Seven Sons, which show 'indications of research going towards a military end use'.[141] In the same year, HCSS and the Leiden Asia Centre published "Checklist for Collaboration with Chinese Universities," which highlighted the risks of knowledge transfer in aerospace technology.[142] Despite such advice and the Seven Sons' links to the PLA, Dutch university TU Delft, for example, has entered into cooperation agreements with four of them over the last 15 years.[143] Extensive cooperation agreements of this kind facilitate

[137] "Defence Projects," *Airbus Defence & Space Dutch Technology*, n.d., accessed November 20, 2025, https://airbusdefenceandspacenetherlands.nl/activities/defence/; "DEFENSE AND GOVERNMENT | Fokker Services Group," Fokker Services Group, accessed November 20, 2025, https://fokkerservicesgroup.com/markets/defense.
[138] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, "Threat Assessment of State Actors 2025 - Publication - AIVD," publicatie, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, September 26, 2025, 41, https://english.aivd.nl/publications/publications/2025/09/26/threat-assessment-of-state-actors-2025.
[139] "China Pursuing Netherlands Aerospace Tech, Says Dutch Report; Beijing Says 'Unfair, Untrue,'" ANI News, April 22, 2023, https://www.aninews.in/news/world/europe/china-pursuing-netherlands-aerospace-tech-says-dutch-report-beijing-says-unfair-untrue20230422165321/.
[140] "Owner of Noord-Brabant Defense Business Arrested in Paris at U.S. Request | NL Times," accessed January 13, 2026, https://nltimes.nl/2023/05/18/owner-noord-brabant-defense-business-arrested-paris-us-request.
[141] Alex Joske, *The China Defence Universities Tracker* (Australian Strategic Policy Institute, 2019), https://www.aspi.org.au/report/china-defence-universities-tracker/.
[142] Frank Bekkers, *Collaboration with Chinese Universities and Other Research Institutions* (2019), https://hcss.nl/report/checklist-for-collaboration-with-chinese-universities-and-other-research-institutions/.
[143] Annebelle de Bruijn, *How TU Delft Unintentionally Helps the Chinese Army - Delta*, Science, March 26, 2021, https://delta.tudelft.nl/en/article/how-tu-delft-unintentionally-helps-chinese-army.

Chinese extraction of valuable IP and know-how from Dutch research institutions through talent-based technological espionage.

Beyond technology transfer, the Dutch aerospace sector is also vulnerable to China's economic statecraft tactics, including targeted trade restrictions on key materials used in the aerospace sector, such as graphite, gallium, and germanium.[144] Sibylline's China Analyst Sam Olsen stated in an interview that China can readily "turn the tap off" to these CRMs, which would make it difficult for the Netherlands (and other NATO countries) to repair or produce military aircraft, such as the F-35, as well as satellite capabilities. In peacetime, this implies production delays and procurement bottlenecks. In times of crisis, strategic Chinese restrictions on CRMs would severely limit the Netherlands' ability to repair and maintain its air force and space capabilities. Dependencies once again provide entry points for Chinese economic statecraft.

3.3.3 Likely interference scenarios

Given these entry points, highly likely Chinese interference scenarios in the Dutch aerospace sector involve a combination of talent-based technological espionage, cyber-enabled espionage and technology transfer, and economic statecraft.

Technology and IP theft remain the most persistent risk. Aerospace is one of the few remaining critical sectors in which China continues to lag behind Western competitors. According to Sibylline's Sam Olsen, Chinese IP theft is decreasing across many critical sectors due to the success of China's economic development policies, which have enabled Chinese firms to achieve technological parity or superiority. However, aerospace remains a target, as China still lags behind in this sector. Corporate espionage targeting firms such as Airbus NL or Fokker, alongside cyber intrusions into engineering systems, design software, and supplier networks, would allow China to accelerate its domestic aerospace development.

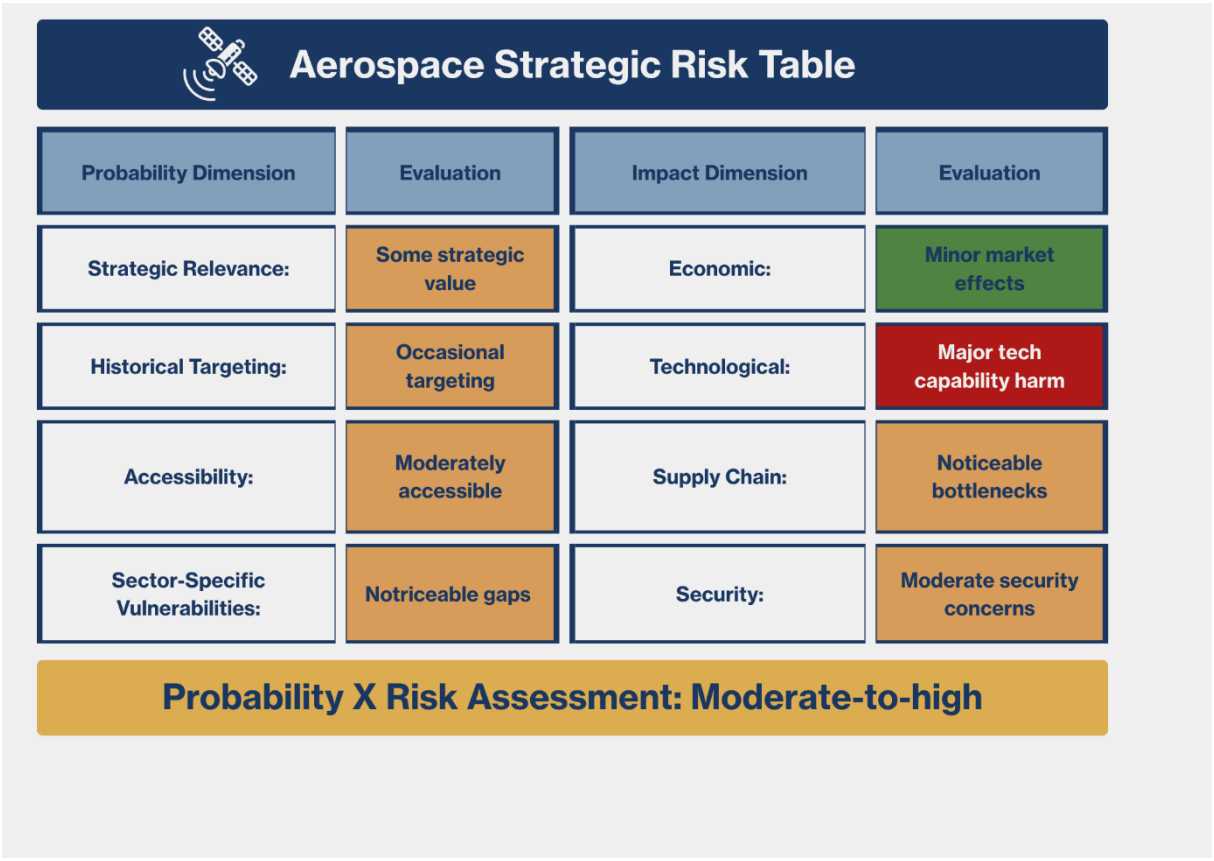
[144] Benedetta Girardi et al., *Strategic Raw Materials for Defence | Mapping European Industry Needs* (2023), 15–18, https://hcss.nl/report/strategic-raw-materials-for-defence/.

Academic collaboration constitutes a parallel interference channel that enables talent-based espionage. Chinese research institutions are likely to continue to exploit the liberal approach adopted by Dutch academia to conduct talent-based technology espionage by infiltrating research institutes and universities.

In the Dutch aerospace sector, China is likely to employ a combination of cyber-enabled digital and information operations, including IP theft targeting aerospace firms and research institutions; talent-based technology transfer through academic exploitation and long-term partnerships linked to military end use; and economic statecraft in the form of supply-chain coercion, leveraging restrictions on CRMs essential for aircraft production and maintenance, particularly during periods of heightened geopolitical tension.

3.3.4 Strategic risk

Table 14 Aerospace Strategic Risk



Chinese interference in the Dutch aerospace sector represents a moderate-to-high strategic risk (see Table 14 above). Its vulnerabilities are less centralised than those of the semiconductor sector and less extensive than the maritime domain. Still, the sector contains multiple high-value nodes where interference would likely yield significant returns for China.

The probability of interference is elevated by China's continued technological lag in the sector and the presence of accessible entry points through academic collaboration, multinational supply chains, and dual-use R&D environments. While core aerospace manufacturing sites are relatively well protected, adjacent ecosystems (e.g., universities, suppliers, maintenance contractors, and digital systems) offer pathways for sustained influence and intelligence collection.

The impact of successful interference would be most acute in the technological and security dimensions. Loss of sensitive aerospace IP, in particular, when it comes to satellite developments, is highly likely to erode Dutch competitiveness and weaken the Netherlands' participation in collaborative aviation and space programmes. In the defence domain, interference affecting avionics, satellite systems, or CRM availability would directly undermine military readiness and strategic resilience, with implications extending beyond the Netherlands to NATO and the EU.

The economic impact, while not irrelevant, would likely be less immediately systemic than in semiconductors or maritime trade, considering the less prominent position of the aerospace sector in the Dutch economy (the sector has a total revenue of ~€4.7 billion, compared to the ~€30 billion of the semiconductor and ~€94 billion of the maritime sectors).[145]

Overall, the aerospace sector occupies a middle position in the Dutch risk landscape: not the most exposed, but strategically significant enough that cumulative Chinese interference is likely to produce long-term consequences, particularly for innovation and technology development.

[145] "Aerospace Industry," Holland International Distribution Council, 2025, https://hollandinternationaldistributioncouncil.com/en/key-sectors/aerospace/; *Semicon in NL* (PWC and Strategy&, 2024), https://www.hightechnl.nl/wp-content/uploads/2024/05/2024-pwc-strategy-semicon-study-nl.pdf; Eelco Rietveld, Martijn Streng, Ties de Leijer, Sandra van Putten, et al., *Maritieme Monitor 2025*.

3.3.5 Gaps and policy actions

The Dutch government has taken several steps to protect the aerospace sector from Chinese interference. These include the Wet VIFO investment-screening regime, which allows the state to block or condition foreign acquisitions in dual-use and defence-relevant technologies;[146] strict EU export controls on aerospace and dual-use items, limiting sensitive technology transfers to China; and the application of NIS/NIS2 cybersecurity obligations to airports and aviation infrastructure, supported by threat intelligence and incident response from the National Cyber Security Centre (NCSC).[147]

In parallel, the government has advanced knowledge-security initiatives, notably the National Knowledge Security Programme, which issues guidance to universities and research institutions on managing high-risk foreign collaborations, and has strengthened the legal framework by criminalising digital and diaspora-based espionage in 2025. Intelligence services (AIVD/MIVD) have expanded outreach to aerospace firms and academic institutions regarding risks associated with Chinese talent programmes and military-affiliated universities, while simultaneously developing legislation to criminalise industrial espionage.[148]

Together, these measures improve the baseline resilience of the sector, but they remain largely horizontal, i.e. applicable across multiple industries and not designed specifically for the unique risk profile, technologies, supply chains, and interference patterns of the aerospace sector. While the risk of this sector remains lower than that of maritime and semiconductors, it is still possible to formulate policy recommendations to enhance sectoral resilience:

1. **Create a national aerospace counterintelligence office**
   Establish a dedicated capability to support private-sector threat detection, vet foreign partners, and provide training on espionage risks.

[146] "Wet veiligheidstoets op investeringen, fusies en overnames | Bureau Toetsing Investeringen."
[147] "Cybersecurity Assessment Netherlands 2025," NCTV, December 2, 2025, https://english.nctv.nl/latest/news/2025/12/02/cybersecurity-assessment-netherlands-2025.
[148] "Knowledge Security," Ministerie van Algemene Zaken, Ministerie van Algemene Zaken, April 7, 2025, https://www.government.nl/topics/science/knowledge-security; Ministerie van Algemene Zaken, "Legislation to Be Broadened to Make More Forms of Espionage a Criminal Offence."

2. **Set mandatory security clauses for joint ventures**
   Require standardised JV agreements that restrict data access, control sensitive tooling, and enable government-mandated reviews of foreign participation.
3. **Develop strategic material stockpiles**
   Coordinate with EU partners to stockpile rare earths and speciality alloys, mirroring U.S. DLA practices to reduce vulnerability to trade coercion.
4. **Strengthen export control enforcement and R&D safeguards**
   Tighten monitoring of dual-use research, personnel mobility, and publication pathways. Condition government R&D funding on adherence to high-security standards.
5. **Centralise oversight of sensitive aerospace supply chains**
   Establish unified procurement oversight, similar to Japan's ATLA model, to improve visibility of risks across both military and civilian aerospace production.

In the aerospace sector, Chinese interference risks are closely linked to long-term innovation pathways, supply-chain dependencies, and the development of dual-use technologies. While these risks manifest differently from those in semiconductors or the maritime sector, they reveal comparable vulnerabilities related to knowledge protection, workforce mobility, and supply chain dependence. The aerospace case demonstrates how Chinese interference can undermine industrial resilience through knowledge infiltration and the leveraging of dependencies, reinforcing the need for systemic resilience measures that extend beyond sector-specific controls. These implications are synthesised and addressed in section 4.

3.4 Cross-Sectoral Synthesis: Patterns of Vulnerability and Governance Challenges

A comparative assessment of the three case studies reveals several recurring patterns that are central to understanding Chinese interference as a national security challenge for the Netherlands (see Table 15 below).

First, Chinese interference exploits structural openness, digitalisation, and economic interdependencies. In semiconductors, knowledge diffusion threatens technological leadership;

in the maritime sector, layered dependencies on foreign equipment and data systems increase operational risk; and in aerospace, progressive erosion of innovation capacity undermines long-term competitiveness and defence readiness.

Second, interference tactics are not operated in isolation but rather as concerted efforts pursuing an overarching objective. Across all three sectors, China employs a layered, multi-domain approach that targets different aspects of the industry. These dynamics suggest that assessing interference risks on a case-by-case or transaction-by-transaction basis is insufficient.

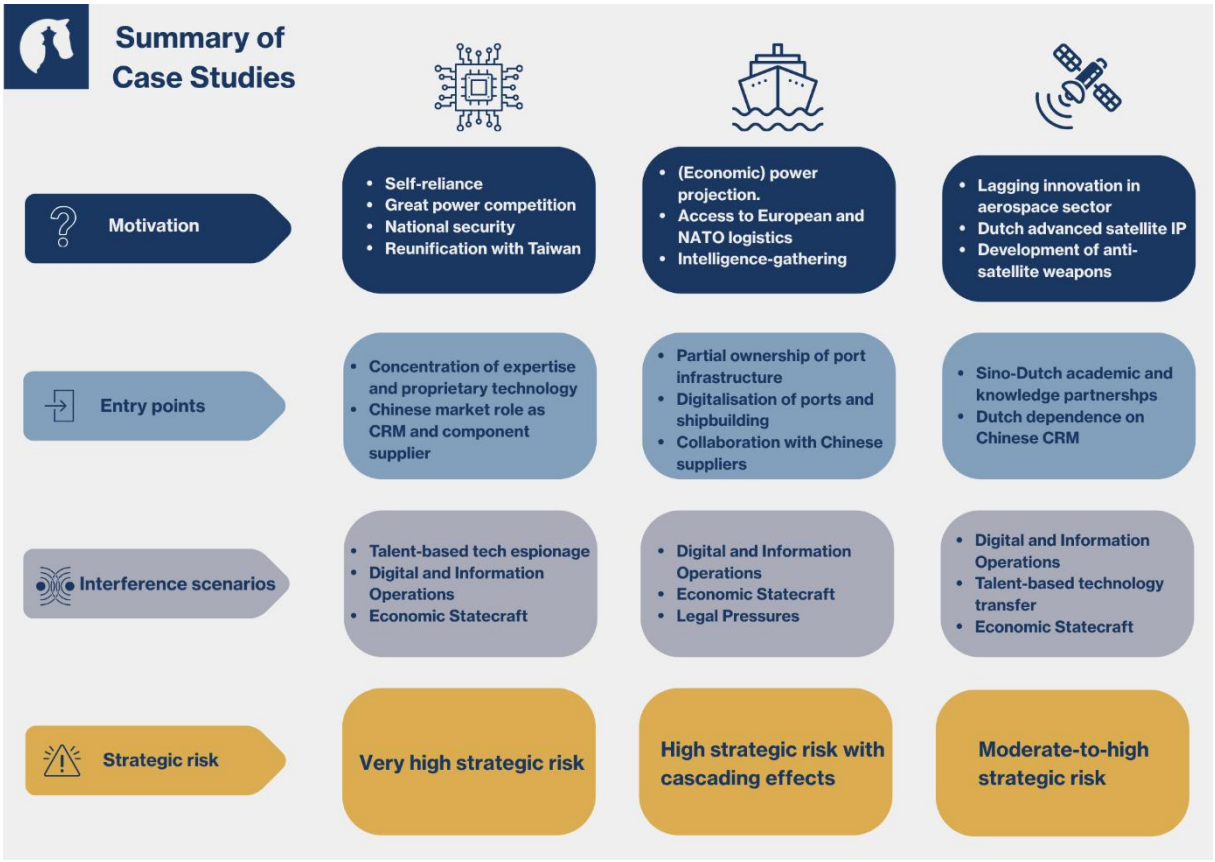
Third, governance fragmentation consistently limits effective risk management. Across all sectors, responsibilities for addressing interference are distributed across multiple ministries, regulators, companies, and knowledge institutions, with limited mechanisms for aggregating insights or coordinating responses. This fragmentation creates blind spots that adversarial actors can exploit across sectors.

Chinese interference in Dutch strategic industries increasingly targets the interfaces among industry, innovation, and talent, rather than formal ownership or exports alone. In all three sectors examined, competitive advantage and strategic relevance are rooted in sensitive IP, systems digitalisation, and research processes based on talent and innovation. These are precisely the domains in which existing policy instruments, such as export controls and investment screening, provide only partial protection.

For the Dutch industrial base, this implies a growing risk of a gradual loss of critical capabilities, competitiveness, and strategic relevance. Even in the absence of large-scale acquisitions or overt technology transfers, sustained access to Dutch ecosystems through research collaboration, supplier relationships, personnel mobility, and minority stakes can gradually reduce the Netherlands' technological lead. Over time, this weakens the country's position in global value chains and diminishes its ability to shape technology standards, control critical chokepoints, and act as a trusted supplier to allies.

These findings indicate that foreign interference in Dutch strategic industries constitutes a systemic challenge requiring coordinated, cross-sectoral policy responses. While sector-specific measures remain necessary, they are insufficient in themselves and should be complemented by a national security approach. The broader national security consequences of these patterns, and the policy options available to address them, are analysed in section 4.

Table 15 Overview of all case studies



4.Implications for Dutch National Security and Building Resilience Against Foreign Interference

4.1 Strategic implications for Dutch national security

The case studies demonstrate that Chinese foreign interference in Dutch strategic industries does not constitute a series of isolated sectoral risks, but rather a systemic challenge that, in the long run, has the potential to erode three core pillars of Dutch national security: strategic autonomy, national governance model, and the Netherlands' role in the EU and NATO.

Chinese interference directly affects the Netherlands' strategic autonomy. In sectors such as semiconductors, maritime, and aerospace, Chinese interference targets capabilities that underpin not only economic competitiveness, but also defence readiness, crisis response, and alliance obligations. The gradual loss of technological edge, combined with increased dependence on high-risk suppliers, limits the Netherlands' freedom of action during periods of geopolitical tension. In a scenario of heightened confrontation, such as a crisis involving Taiwan, these dependencies are highly likely to be activated as leverage, constraining Dutch policy choices and increasing exposure to coercion.

Additionally, Chinese interference exploits precisely those features that characterise the Dutch economic and innovation model: openness, decentralised governance, strong public–private collaboration, and international integration and trade. Historically, these have been the Netherlands' strategic strengths. However, with increasing Chinese interference, they risk creating governance fragmentation across government, industry, and research institutions.

Lastly, Chinese interference carries implications for the Netherlands' role within European and transatlantic security architectures. Dutch strategic industries function as critical nodes in EU and NATO systems. Interference that undermines the integrity, reliability, or security of these sectors therefore carries alliance-level consequences, potentially affecting trust, interoperability, and collective resilience. At a time when the transatlantic relationship is undergoing a process of transformation, and Europe focuses on rearming, foreign interference in

Dutch industries should be understood not only as a national issue but as a challenge to broader Euro-Atlantic security.

Taken together, these dynamics indicate that Chinese foreign interference constitutes a long-term, systemic risk that extends beyond the Dutch industrial ecosystem and spills over into national security. Addressing this challenge requires a shift from predominantly transactional risk management toward a resilience-oriented national security approach.

4.2 Policy Recommendations

From a policy perspective, these findings underline the need to integrate national, knowledge, and economic security more systematically. Protecting Dutch strategic industries from Chinese interference is not solely a matter of defensive regulation, but also of ensuring that long-term industrial and innovation policies actively reduce structural vulnerabilities. The analysis shows that China employs a broad toolkit of interference measures, used in a multi-layered manner, to target Dutch strategic industries in pursuit of its foreign policy and economic objectives. China analyst Sam Olsen argues that this multifaceted approach to interference makes China's potential to affect the Netherlands effective. While the Netherlands has so far avoided significant disruptive consequences of Chinese interference, Beijing's activities targeting Dutch strategic industries have intensified, as noted by Dutch Minister of Defence Ruben Brekelmans in May 2025.[149]

The Netherlands has the capacity to enhance its resilience to Chinese interference by strengthening public-private cooperation and adopting a comprehensive, national-security-oriented strategy that treats Chinese interference as a systemic challenge. To achieve this, there are five key policy recommendations that can be implemented in the short-to-medium term:

[149] "Chinese Spying on Dutch Industries 'Intensifying': Dutch Defence Minister," *Reuters*, May 31, 2025, https://www.reuters.com/business/aerospace-defense/chinese-spying-dutch-industries-intensifying-dutch-defence-minister-2025-05-31/.

4.2.1 Establish a national coordination and intelligence-sharing architecture for foreign interference

The Netherlands should establish a permanent national coordination and intelligence-sharing architecture dedicated to foreign interference in strategic industries with the purpose of closing the information gap between public and private actors and enabling timely, coordinated responses to foreign interference.

This architecture should combine two mutually reinforcing elements:

- A cross-sector Foreign Interference Council under the guidance of the NCTV, bringing together government, industry, academia, and civil society. The council should operate at the strategic level, with industry-specific subgroups (e.g. semiconductors, maritime, aerospace) to address sectoral risk profiles and vulnerabilities.
- A secure intelligence-sharing platform or mechanism, enabling structured, two-way information exchange between public intelligence services (AIVD/MIVD), relevant ministries, and trusted private-sector actors.

This recommendation builds directly on the whole-of-society approach to hybrid threats articulated in the *Defensienota 2024* and aligns with the NCTV's coordination role in a specific sub-field of foreign interference, as outlined, for instance, in the *Cybersecuritybeeld Nederland 2025*.[150] Furthermore, it addresses current capacity constraints within AIVD/MIVD by enabling companies to supplement state intelligence with vetted private intelligence capabilities, while ensuring government oversight and contextualisation.

4.2.2 Implement mandatory, risk-based sector-wide security standards

Develop baseline requirements for cybersecurity, supply chain integrity, foreign investment screening, and insider threat management across all sensitive industries. Chief among these should be the standardisation of a tiered employee screening process. This process will focus on

[150] inisterie van Defensie, “Defensienota 2024”; Ministerie van Algemene Zaken, “Cybersecuritybeeld Nederland 2025.”

ensuring that employees and researchers with affiliations with institutions known to be used by Beijing for espionage-related activities are not hired.

This tiered process should move beyond the Ministry of Justice's standard "Verklaring Omtrent Het Gedrag" (VOG or Certificate of Behaviour). This is because such VOG background checks do not account for applicants' actions, behaviours, and connections outside of the Netherlands or the European Union, which those operating at the behest of the Chinese government will have. Applicants may not be subject to a screening process solely on the basis of their ethnicity, as this would constitute discrimination under Dutch labour law. Instead, a company's tiered system should critically assess what its organisation's "crown jewels"[151] are and who has access to them.

Based on this crown jewel assessment, a tiered screening system is created, whereby those with the most direct access to these crown jewels (e.g., IT workers, C-Suite, mid-level managers, etc.) undergo a more stringent screening process based on several factors (e.g., an applicant's susceptibility to blackmail or bribery, given personal ties or financial health). In contrast, less high-profile applicants (e.g., working students or contractors) will undergo a background check that adequately reflects their seniority and level of access to the company's crown jewels.

Such policies could build on the Netherlands' *Knowledge Security Screening Bill* proposal, which is aimed primarily at academia.[152] Standards should be co-designed with the representatives from the concerned industries to balance practicality, resilience, and industry-specific needs. Such assessments could be conducted in-house or via specialised private sector firms, given the Dutch government's limited capacity to conduct such screenings on the scale needed.

[151] A company's most valuable, profitable, or strategically critical assets.
[152] Ministerie van Algemene Zaken, "Screening for Researchers Wising to Handle Sensitive Knowledge."

4.2.3 Embed foreign interference risk into industrial and innovation policy via a public–private resilience fund

Develop a funding mechanism, in coordination with the EU and NATO, to support the replacement of high-risk foreign equipment. For example, equipment such as server motherboards, Baseboard Management Controller, or large ship-to-shore (STS) cranes,[153] should be replaced with European-made equivalents. Moreover, the supply base for these products should be diversified, with greater reliance on Europe-based organisations, and domestic capacity-building for critical technologies in the Netherlands (e.g., cybersecurity and infrastructure upgrades) should be strengthened.

This funding mechanism should be monitored and maintained by an independent subcommittee structure that includes representation from relevant ministries and industry stakeholders (e.g., Domestic Affairs, Defence), as well as intelligence and security services.

This funding mechanism should also build on the previous two recommendations by using the threat assessments to identify where structural vulnerabilities exist and where money can be most effectively invested. Moreover, it should, as far as possible, align with EU- and NATO-level initiatives (e.g., the EU Chips Act and CRM strategies) to ensure Europe-wide resilience and to ensure that the Netherlands maintains interoperability with its EU and NATO partners.

Given the rapidly shifting geopolitical landscape, a surge capacity function should be included that activates during crises (e.g., trade sanctions, severe cyber campaigns). A predefined set of escalation triggers would unlock accelerated procedures and additional tranches of funding to help prevent significant economic damage to the Netherlands' strategic industries.

The fund's independent governing body should regularly review (e.g., every 1-2 years) strategic priorities and adjust funding priorities based on factors such as the pace of technological change, geopolitical conditions, and risk appetites.

[153] Lori Ann LaRocco, "A Look inside the Chinese Cyber Threat at the Biggest Ports in US," CNBC, March 13, 2024, https://www.cnbc.com/2024/03/13/a-look-inside-the-true-nature-of-chinese-cyber-threat-at-us-ports.html.

This mechanism would complement existing initiatives such as Project Beethoven and the Defence Industrial Strategy. A built-in surge capacity should allow accelerated funding and procedures during crises (e.g. sanctions escalation, severe cyber campaigns).

4.2.4 Promote transparency, accountability, and international alignment

To reinforce democratic oversight and international coherence, the Netherlands should publish regular non-classified assessments of foreign interference trends, building on the model of the Cybersecuritybeeld Nederland.[154] These assessments should also build upon the EU and NATO's standards (e.g., Articles 2 and 3), programmes, and resilience efforts (e.g., the NATO Resilience Reference Curriculum or the European Preparedness Union Strategy). Moreover, these reports should inform public debate without compromising sensitive sources.

At the international level, the Netherlands should actively promote coordination within the EU and NATO on investment screening, critical technology procurement, supply-chain security, and incident response and sanctions alignment. This can be achieved by furthering existing cooperation between the Dutch government and industry with multilateral dedicated fora such as the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

Domestically, compliance with resilience measures should be incentivised through procurement preferences, insurance mechanisms, and recognition schemes, rather than relying solely on enforcement. These measures would complement existing initiatives and Dutch societal and military resilience policies, such as the December 2025 Letter to the House of Representatives on the Netherlands' resilience and preparedness against hybrid and military threats (e.g., de Wet weerbaarheid kritieke entiteiten or Cyberbeveiligswet).[155]

[154] NCTV, "Cybersecuritybeeld Nederland 2025."
[155] Brekelmans et al., "Kamerbrief Weerbaarheid En Militaire Paraatheid Tegen Hybride En Militaire Dreigingen."

4.2.5 Strategically manage interdependence through selective, reciprocal & leverage-based engagement

The Netherlands should complement its defensive resilience measures with a strategy of *managed interdependence* vis-à-vis China, aimed at preserving economic benefits while reducing asymmetric dependencies and coercion risks. In addition, the Netherlands, in combination with the EU, should also look to move beyond viewing this relationship as one-sided in nature and seek to be more proactive in its approach towards China. Indeed, as highlighted in the case studies, China still maintains numerous dependencies on Dutch and EU businesses in sectors such as aerospace and semiconductors, allowing these players to act from a position of strength instead of weakness. This approach builds directly on existing Dutch policy that recognises both the necessity of engagement with China and the risks associated with unmitigated dependence.[156]

Operationally, this two-fold approach would entail:

- Identifying and explicitly delineating "safe-to-engage" domains where cooperation with Chinese actors poses limited national security risk, such as climate mitigation technologies, basic research with low dual-use potential, public health, and international standards-setting. Providing clarity on these domains would reduce uncertainty for industry and academia and prevent over-securitisation.
- Embedding reciprocity and risk-awareness into economic and innovation policy. Engagement should be conditional on minimum standards regarding market access, IP protection, data governance, transparency of ownership, and the absence of state-directed interference.
- Actively manage dependencies by mapping and controlling critical nodes in value chains. Dutch and European actors should retain control over key stages such as system integration, design, certification, software, and servicing, even when Chinese inputs are involved. Systematic mapping of sectoral dependencies and vulnerabilities should inform investment screening, procurement policy, export control calibration, and diplomatic

[156] *Kamerbrief Open Strategische Autonomie*.

engagement, ensuring that security and economic objectives are coherent and mutually reinforcing.

- In tandem, the Netherlands and its EU partners would:
- Maintain its reverse dependencies vis-à-vis China by improving their strategic sectors, such as aerospace or semiconductors, launching programmes to support the further development of skills, such as engineering in high-technology, and the business environment required to maintain their competitive edge over Chinese businesses.
- Instituting an export measurement control for technology, components or other aspects related to these actors' critical sectors. In contrast to an export control mechanism, which would restrict trade to Chinese partners, this trade mechanism should be targeted at maintaining a strict overview of which critical technologies or components, including dual-use technology, are being sent to Chinese actors and/or their known partners. Such a mechanism would allow the Hague and Brussels to maintain an overview and track record of where Beijing's interests currently are vis-à-vis Europe's strategic innovations, how this is evolving, and act as an early warning signal if Beijing is becoming less dependent on them. For the success of this mechanism, the Hague and Brussels would need to either limit or maintain a similar overview process for key technologies that Beijing acquires through other trade mechanisms, such as "Greenfield Investments".[157]

By embedding reciprocal and leverage-based engagement with China within a structured framework of reciprocity, transparency, and dependency management, the Netherlands can move from a reactive posture to a more confident and strategic proactive approach. This approach reinforces national resilience not only by reducing exposure to interference, but also by preserving room for manoeuvre and leveraging the Netherlands' economic strengths in an increasingly competitive geo-economic environment.

The strategic consequences and policy recommendations outlined in this section underscore that Chinese foreign interference in Dutch strategic industries should be understood as a structural and long-term national security challenge, rather than as a collection of isolated risks or incidents. The Netherlands' openness, technological sophistication, and deep integration into

[157] Canton and Solera, *Greenfield Foreign Direct Investment and Structural Reforms in Europe: What Factors Determine Investments?*

global value chains remain core strategic assets, but they also require active protection in an increasingly contested geopolitical environment.

Strengthening resilience against foreign interference, therefore, does not imply abandoning openness, but rather recalibrating it through coordinated governance, risk-based safeguards, and sustained public-private cooperation. By adopting a systemic, resilience-oriented approach anchored in national coordination, sector-wide standards, targeted investment, preparedness, and international alignment, the Netherlands can preserve its strategic autonomy, uphold its governance model, and continue to function as a reliable partner within the EU and NATO, even under conditions of intensified geopolitical competition.