



Research Papers

October 2026

High-Risk ICT Vendors and Critical Infrastructure: European Approaches

Jamie MacColl, Pia Hüscher, Natasha Buckley and Sophie Williams-Dunning

Disclaimer

The content in this publication is provided for general information only. It is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action based on the content in this publication.

The views expressed in this publication are those of the authors, and do not necessarily reflect the views of RUSI or any other institution.

To the fullest extent permitted by law, RUSI shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising from or in connection with the reproduction, reliance on or use of the publication or any of the information contained in the publication by you or any third party. References to RUSI include its directors, trustees and employees.

© 2026 The Royal United Services Institute for Defence and Security Studies



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

RUSI Research Papers, October 2026

ISSN 2977-960X

Publications Team

Editorial

Director of Publications: Alice Trouncer

Managing Editor: Sarah Hudson

Assistant Editor: Sophie Boulter

Assistant Editor: Liz Ottosson

Design

Graphic Designer: Lisa Westthorp

Research Editorial

Head of Research Governance
and Editorial: Elias Forneris

Cover image: Courtesy of Yurii Maslak /
Alamy

Get in touch

 www.rusi.org

 enquiries@rusi.org

 +44 (0)207 747 2600

The Royal United Services Institute for Defence and Security
61 Whitehall, London
SW1A 2ET
United Kingdom

Follow us on



Contents

iv	Disclaimer
1	Executive Summary
1	Key Findings
3	Introduction
5	What is a ‘High-Risk’ ICT Vendor?
5	Geopolitical and Security Risks
7	Technical Risks
8	Economic Risks
9	The Evolution of the EU’s Approach to High-Risk Vendors
12	Germany
12	Strategic Context
14	Policy, Legislation and Regulation
16	Policy Implementation Approach, Gaps and Challenges
20	Spain
20	Strategic Context
21	Policy, Legislation and Regulation
23	Policy Implementation Approach, Gaps and Challenges
27	The UK
27	Strategic Context
29	Policy, Legislation and Regulation
31	Policy Implementation Approach, Gaps and Challenges
35	Cross-Cutting Themes and Implications for EU and UK Policy
35	Absence of a Common Definition of a High-Risk Technology Vendor
36	Persistence of Economic Considerations for National Policy on High-Risk Vendors
37	Visibility Gap and the Importance of State Capacity
38	The Role of US Technology Companies in Debates on High-Risk Vendors

38	The Impact of Designations and Exclusions of High-Risk Vendors on Europe's Cyber Security
39	Addressing Gaps in the UK's Approach to High-Risk ICT Vendors
41	Conclusion
42	About the Authors
43	Annex 1
44	Annex 2
45	Annex 3

Methodology

This paper draws on primary and secondary research conducted between February 2025 and February 2026. The paper was submitted on 4 June 2026 and approved for copy-editing on 21 August 2026. Secondary qualitative research involved a rapid evidence assessment to review relevant open source academic and grey literature. The research team also conducted 27 interviews with UK, Spanish and German stakeholders in the public, private, academic and civil society sectors. The majority of these interviews took place online, but some interviews with German stakeholders took place in Berlin in June 2025. All interview data was anonymised to protect participants' confidentiality, in accordance with standard research ethics protocols. The research team then held a validation roundtable in Brussels in February 2026 with stakeholders from the European Commission, the European Parliament, member state officials, the private sector and civil society.

Disclaimer

The content in this publication is provided for general information only. It is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action based on the content in this publication.

The views expressed in this publication are those of the authors, and do not necessarily reflect the views of RUSI or any other institution.

This document has been prepared by RUSI for informational purposes only (the 'Permitted Purpose'). While all reasonable care has been taken by RUSI to ensure the accuracy of material in this report (the 'Information'), it has been obtained primarily from interviews and open source literature and RUSI makes no representations or warranties of any kind with respect to the Information.

You should not use, reproduce or rely on the Information for any purpose other than the Permitted Purpose. Any reliance you place on the Information is strictly at your own risk. If you intend to use the Information for any other purpose (including, without limitation, to commence legal proceedings, take steps or decline to take steps or otherwise deal with any named person or entity), you must first undertake and rely on your own independent research to verify the Information. To the fullest extent permitted by law, RUSI shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising from or in connection with the reproduction, reliance on or use of any of the Information contained in the publication by you or any third party. References to RUSI include its directors, trustees and employees.

Executive Summary

Since the debate on excluding Huawei from 5G cellular infrastructure peaked around five years ago, Europe has continued to seek ways to effectively manage the risks posed by Chinese ICT vendors. This paper explores how three European countries – Germany, Spain and the UK – have taken different approaches to balance the risks and opportunities presented by Chinese technology vendors. It analyses how differences at the national level could be reconciled by a common European approach, and how the EU's efforts to create such an approach may be perceived and shaped by key member states.

Key Findings

- **Germany, Spain and the UK have developed different approaches, shaped by their respective economic relationships with China, perceptions of national security risk, institutional structures and relationships with the US and the EU.** Germany has historically prioritised economic considerations and adopted a cautious, narrowly focused approach that means Chinese vendors remain in significant swathes of its 5G infrastructure, although recent legislative changes give the government broader powers to intervene across critical national infrastructure (CNI). Spain adheres to EU policy where the law is explicit, for example with respect to 5G security, but exploits legislative ambiguity where it exists to enable Chinese ICT vendors to continue to expand their footprint in several sensitive sectors. The UK has developed the most interventionist framework in telecommunications (telecoms) and public procurement to protect itself from these vendors, supported by dedicated legislation and institutional capacity, but still lacks a coherent framework covering its remaining CNI.
- **There is no common European definition of a 'high-risk ICT vendor'.** Germany, Spain and the UK use different, often sector-specific frameworks to assess risks relating to foreign state influence, technical vulnerability and strategic dependence. This flexibility allows for national differences in risk appetite and a difference in approach to national security but also produces inconsistent implementation and leaves procurement officials and operators to make judgements for which they may be poorly equipped.

- **The EU's approach, to allow member states to participate in restrictions on a voluntary basis, has failed to produce a coherent European response.** Although most member states have established some legal powers to assess suppliers, only a minority have fully implemented restrictions under the EU Toolbox for 5G Security. Divergent economic interests, political priorities and perceptions of China have created significant differences between national approaches.
- **Economic considerations remain central to national decision-making.** Germany's industrial exposure to China has contributed to delayed and narrowly defined restrictions, while Spain's interest in Chinese investment and its green transition discourages more interventionist policies. The longer that high-risk vendors remain embedded in infrastructure, the greater the financial and operational costs of removing them. Economic considerations also mean that Germany and Spain are likely to push back against the EU's efforts to designate and exclude Chinese ICT vendors from critical sectors.
- **Institutional capacity and supply-chain visibility are as important as formal legal powers.** Governments frequently lack accurate information about installed technology, subcontractors and dependencies further down supply chains. The UK's National Security Unit for Procurement provides a useful model of a dedicated institution able to assess vendors, advise contracting authorities and monitor implementation.

Introduction

Over the last decade, Europe has grappled with the risks posed by Chinese ICT to CNI, with mixed success. In January 2026, the European Commission announced its latest effort to manage the security and economic risks associated with so-called ‘high-risk suppliers’, proposing a new set of amendments to the EU’s Cyber Security Act (CSA).¹ One such amendment aims to create a ‘trusted ICT supply chain framework’ that will give the Commission broad powers to designate and exclude high-risk vendors from 18 critical sectors across EU countries. The proposal follows several years of frustration within the Commission and many European governments about the slow progress and uneven implementation of the EU’s voluntary 5G security framework, the EU Toolbox for 5G Security.²

Concerns about the risks posed by Chinese ICT vendors are well-founded. National security legislation in China enables Chinese authorities to exercise control and influence over technology vendors, such as Huawei. China has also demonstrated its willingness and capability to hack European CNI to serve strategic goals.³ The country’s industrial capacity also positions it to dominate supply chains – and by extension, create unwelcome dependencies – for certain strategic technologies. At the same time, the strength of China’s economy and its role in global technology supply chains pose challenges for reducing dependencies. In some technologies, Chinese companies have surpassed their Western counterparts and sell superior products at lower prices. For many European countries, therefore, the cost of not doing business with China outweighs the potential security risks.

1. European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European Cybersecurity Certification Framework, and ICT Supply Chain Security and Repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)’, 20 January 2026, <<https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act>>, accessed 13 February 2026.
2. European Commission, *The EU Toolbox for 5G Security* (Brussels: EU, 2020), <<https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security>>, accessed 13 February 2026.
3. Council of the EU, ‘Cyber-Attacks Against the EU and its Member States: Council Sanctions Three Entities and Two Individuals’, 16 March 2026, <<https://www.consilium.europa.eu/en/press/press-releases/2026/03/16/cyber-attacks-against-the-eu-and-its-member-states-council-sanctions-three-entities-and-two-individuals/>>, accessed 16 July 2026; Raphael Minder, ‘Chinese Cyber Threat to Europe on Par With Russia’s, Warns Czech President’, *Financial Times*, 20 June 2025.

Given this tension, governments in Europe – and globally – have interpreted, prioritised and enforced concerns about Chinese ICT vendors in a variety of ways. This paper examines those differences through a comparative analysis of three European countries – Germany, Spain and the UK – chosen primarily because of their varied postures and approaches towards China, relations with the US and managing 5G vendors such as Huawei.⁴

The first chapter explores common drivers that shape perceptions of high-risk vendors in Europe and provides an overview of the EU’s policy towards high-risk vendors. The second chapter examines the national approaches of Germany, Spain and the UK to high-risk ICT vendors in CNI. In each case, the analysis considered: the strategic context shaping perceptions of foreign technology risks; the policies, laws, regulations, institutions and frameworks that govern those risks; and efforts to implement policies aimed at high-risk ICT vendors. The final section looks at the implications of these differing national approaches to policy.

Table 1: Breakdown of Interviewees

Country	Number of interviewees
Germany	7
Spain	7
UK	13
Total	27

Sources: The authors.

The primary research was designed to surface and stress-test expert perspectives on high-risk ICT vendors, not to measure the prevalence of opinion across the EU. Interviewees and roundtable participants were selected for their direct experience in the relevant public, private, academic and civil society settings, with a deliberate focus on three states: Germany, Spain and the UK. The resulting evidence is qualitative and illustrative, capturing how informed practitioners understand the challenges and where their assessments converge or diverge, and is triangulated throughout against secondary literature. In turn, interview and roundtable findings are reported as the considered views of those consulted rather than as measures of how widely a given position is held in any of the countries studied for the paper.

4. See Roxana Radu and Cedric Amon, ‘The Governance of 5G Infrastructure: Between Path Dependency and Risk-Based Approaches’, *Journal of Cyber Security* (Vol. 7, No. 1, 2021); Alanna Krolikowski and Todd H Hall, ‘Non-Decision Decisions in the Huawei 5G Dilemma: Policy in Japan, the UK, and Germany’, *Japanese Journal of Political Science* (Vol. 24, No. 2, 2023), pp. 171–89; Tim Rühlig, ‘The “Huawei Saga” in Europe Revisited: German Lessons for the Rollout of 6G’, IFRI, 2 June 2025, <<https://www.ifri.org/en/publications/huawei-saga-europe-revisited-german-lessons-rollout-6g>>, accessed 5 August 2026.

What is a ‘High-Risk’ ICT Vendor?

A high-risk ICT vendor is not a fixed legal category. Applying this label involves a judgement about trust, dependency and exposure. As the EU and European governments have evaluated foreign ICT vendors, decision-makers have been required to balance three types of risk: geopolitical, technical and economic.

Geopolitical and Security Risks

First, there are concerns among many European policymakers and cyber security practitioners that dependencies on some vendors may be exploited in moments of geopolitical tension. It has been argued that China may use its ability to control and influence state-owned or private ICT vendors to spy on foreign governments or disrupt CNI during crises.⁵

The body of evidence supporting concerns about Chinese ICT vendors is sufficient to establish the risk as real. The legal mechanisms are not in dispute. Analysis of China’s data-governance architecture documents that the National Intelligence Law (2018)⁶ and the Counter-Espionage Law (2014, revised 2023)⁷ require private firms to submit data to the state on request, and that China’s Company Law obliges firms to host internal Chinese Communist Party (CCP) representatives.⁸ One analysis found that companies such as Alibaba, Huawei and Tencent maintain hundreds of CCP representatives between them, leaving the conduct of China’s largest technology platforms difficult to

-
5. Alexander Martin, ‘EU Parliament Expresses “Deep Concern” About China and Use of Huawei Equipment’, *Sky News*, 13 March 2019; Ken Dilanian, ‘U.S. Officials: Using Huawei Tech Opens Door to Chinese Spying, Censorship’, *NBC News*, 14 February 2020.
 6. China Law Translate, ‘PRC National Intelligence Law (as Amended in 2018)’, 27 June 2017, <<https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>>, accessed 2 August 2026.
 7. China Law Translate, ‘China: Counter-Espionage Law of the P.R.C. (2023 Ed.)’, 26 April 2023, <<https://www.chinalawtranslate.com/en/counter-espionage-law-2023/>>, accessed 2 August 2026.
 8. Scott Livingston, ‘The New Challenge of Communist Corporate Governance’, Center for Strategic and International Studies (CSIS), 15 January 2021, <<https://www.csis.org/analysis/new-challenge-communist-corporate-governance>>, accessed 1 June 2026.

disentangle from those of the CCP.⁹ The same analysis notes that the National Security Law (2015)¹⁰ obliges citizens and entities to report activity endangering national security and to assist state agencies, a provision they read as potentially permitting government access to digital communications within Chinese jurisdiction, while noting that strict enforcement remains sparsely evidenced.¹¹ This is a statutory capability the Chinese state has built deliberately and continues to widen.

Additionally, the 2021 Regulation on the Management of Network Product Security Vulnerabilities¹² compels firms operating in China to report software flaws to the Ministry of Industry and Information Technology within 48 hours of discovery, while prohibiting disclosure to overseas parties other than the product's own vendor. This converts China's private sector security research into a state-controlled pipeline that grants intelligence services privileged early access to exploitable vulnerabilities.¹³ Alongside this, the parallel practices of compelled cooperation, CCP influence within firms, and a demonstrated record of Chinese intrusions into European and Western CNI have been documented.¹⁴

It has been noted that the National Intelligence Law's cooperation clause lacks a formal enforcement mechanism.¹⁵ However, where the state can already secure cooperation without needing to invoke a law, the absence of enforcement could be considered a feature of an opaque system. What remains unobservable from open sources is the scale, frequency and extent of actual covert exploitation. The convergence of confirmed legal capability, an operational pipeline for vulnerability collection and a

-
9. Oscar Borgogno and Michele Savini Zangrandi, 'Chinese Data Governance and Trade Policy: From Cyber Sovereignty to the Quest for Digital Hegemony?', *Journal of Contemporary China* (Vol. 33, No. 148, 2024), pp. 578–602.
 10. Rogier Creemers, 'National Security Law of the People's Republic of China', DigiChina, Stanford University, 1 July 2015, <<https://digichina.stanford.edu/work/national-security-law-of-the-peoples-republic-of-china/>>, accessed 5 August 2026.
 11. Borgogno and Savini Zangrandi, 'Chinese Data Governance and Trade Policy'.
 12. Cyberspace Administration of China, 'Notice from the Ministry of Industry and Information Technology, the State Internet Information Office, and the Ministry of Public Security on Issuing Regulations on the Management of Network Product Security Vulnerabilities', 13 July 2021, <https://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm>, accessed 5 August 2026.
 13. Dakota Cary and Kristin Del Rosso, 'Sleight of Hand: How China Weaponizes Software Vulnerabilities', Atlantic Council, 6 September 2023, <<https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/>>, accessed 5 August 2026; Catalin Cimpanu, 'Chinese Government Lays Out New Vulnerability Disclosure Rules', *The Record*, 14 July 2021, <<https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules>>, accessed 5 August 2026.
 14. James Andrew Lewis, 'Securing Communications Networks from Foreign Adversaries', Statement before the House Energy and Commerce Subcommittee on Communications and Technology, CSIS, 15 February 2024, <<https://www.csis.org/analysis/securing-communications-networks-foreign-adversaries>>, accessed 4 August 2026.
 15. Jeremy Daum, 'What China's National Intelligence Law Says, and Why It Doesn't Matter', China Law Translate, 22 February 2024, <<https://www.chinalawtranslate.com/en/what-the-national-intelligence-law-says-and-why-it-doesnt-matter/>>, accessed 4 August 2026.

demonstrated intrusion record, however, should raise questions about the risk of dependence on Chinese ICT.

As a recent Australian Strategic Policy Institute report notes, while these concerns are not unique to China, China's lack of legal checks and balances and track record of cyber operations and economic coercion set it apart.¹⁶

Technical Risks

Considerations of technical vulnerabilities and dependencies underpin the geopolitical concerns above. During earlier debates about the security of Chinese 5G vendors, there was serious concern about the existence of 'backdoors' or 'kill switches' that would allow Huawei – and by extension, Chinese authorities – to access user data or affect network functionality.¹⁷ In April 2025, reporting by Reuters raised similar apprehensions about solar panel inverters¹⁸ manufactured by Chinese companies.¹⁹ Yet, in both cases, there is no clear evidence that Chinese vendors have deliberately installed backdoors. Following extensive testing, the UK National Cyber Security Centre assessed that none of the vulnerabilities uncovered in Huawei's equipment were the result of state control or influence.²⁰ In February 2026, a review by the US Department of Energy reportedly found no evidence of backdoors in Chinese solar power inverters.²¹

However, backdoors are not the only technical risks. Dependence on ICT vendors for hardware and software maintenance, network management and managed services also constitute a potential risk. Such vendors may withhold updates or maintenance for key services during geopolitical crises or conflict, as when some US technology vendors stopped providing updates and cloud services for Russian customers after Russia's 2022 full-scale invasion of Ukraine.²²

-
16. Justin Bassi et al., 'In Whose Tech We Trust: Part 1 – Mapping Indo-Pacific Security Approaches to Foreign Owned, Controlled or Influenced Technology', Australian Strategic Policy Institute (ASPI), 11 November 2025, <<https://www.aspi.org.au/report/in-whose-tech-we-trust-part-i-mapping-indo-pacific-security-approaches-to-foreign-owned-controlled-or-influenced-technology/>>, accessed 6 July 2026.
 17. Jason Healey, 'Five Jeez: Five Security Arguments Against Huawei 5G', Council on Foreign Relations, 4 September 2019, <<https://www.cfr.org/articles/five-security-arguments-against-huawei-5g>>, accessed 2 September 2026.
 18. Solar panel inverters convert raw direct current electricity generated by solar panels into useable electricity for home appliances and the national grid.
 19. Sarah McFarlane, 'Rogue Communication Devices Found in Chinese Solar Panel Inverters', *Reuters*, 14 May 2025.
 20. National Cyber Security Centre, 'Sixth Huawei Cyber Security Evaluation Centre Oversight Board Report Published', 1 October 2020, p. 24, <<https://www.ncsc.gov.uk/information/hcsec-ob-report>>, accessed 6 August 2026.
 21. Nichola Groom, 'US Probe Finds No Evidence of Spyware in Chinese Power Inverters', *Reuters*, 10 February 2026.
 22. Alexander Martin, 'Microsoft to Suspend All Sales and Services in Russia', *Sky News*, 4 March 2022.

Economic Risks

Some European and Indo-Pacific policymakers and analysts are concerned about China's ability to distort markets, including the sale of some ICT equipment, through state subsidies and industrial capacity. They see restricting the involvement of Chinese vendors in domestic markets as necessary to protect sovereign capabilities and nurture national alternatives.²³

Other economic pressures, however, pull in the opposite direction. Huawei and other Chinese vendors offer competitive pricing, which is attractive for countries focused on economic growth and development. Furthermore, once vendors have a foothold, reducing dependence by replacing 'high-risk' equipment is costly, an argument that has been emphasised through lobbying by industry groups and Chinese vendors.²⁴

The threat of economic retaliation has also shaped national decision-making. During Germany's 5G debate, Chinese officials warned of 'consequences' for Germany's economic relationship with China if it excluded Huawei.²⁵ Sweden offers a fully developed example of how such restrictions could be contested. In 2020, the Swedish telecoms regulator excluded Huawei and ZTE from the country's 5G networks on national security grounds and ordered existing Huawei equipment to be removed from core functions.²⁶ After failing to overturn the decision in the Swedish courts, Huawei escalated the matter to international arbitration, filing a claim against Sweden at the World Bank's International Centre for Settlement of Investment Disputes in January 2022 under the 1982 China–Sweden bilateral investment treaty,²⁷ reportedly seeking damages of SEK 5.2 billion.²⁸ The case, still pending, can be regarded as a test that will

-
23. Sander Tordoir and Brad Setser, 'China Shock 2.0: The Cost of Germany's Complacency', Centre for European Reform, 20 May 2026, <<https://www.cer.eu/publications/archive/policy-brief/2026/china-shock-20-cost-germanys-complacency>>, accessed 2 September 2026; Bassi et al., 'In Whose Tech We Trust: Part 1'.
 24. Philip Blenkinsop, 'EU Plan to Phase Out Chinese Tech Could Cost Bloc Over \$400 Billion, Chinese Study Says', *Reuters*, 6 May 2026. This is an ongoing debate, however. See GSMA Intelligence, 'The Cost of Removing Designated Third-Country Vendors from EU Telecoms Networks', July 2026, <<https://www.gsmainelligence.com/research/the-cost-of-removing-designated-third-country-vendors-from-eu-telecoms-networks>>, accessed 15 August 2026; Strand Consult, 'Fact-Check: GSMA Intelligence's Report "The Cost of Removing Designated Third-Country Vendors from EU Telecoms Networks"', 23 July 2026, <<https://strandconsult.dk/fact-check-gsma-intelligences-report-the-cost-of-removing-designated-third-country-vendors-from-eu-telecoms-networks/>>, accessed 15 August 2026.
 25. Tony Czuczka and Steven Arons, 'China Threatens Retaliation Should Germany Ban Huawei 5G', *Bloomberg*, 14 December 2019, <<https://www.bloomberg.com/news/articles/2019-12-14/china-threatens-germany-with-retaliation-if-huawei-5g-is-banned>>, accessed 5 August 2026.
 26. Annie Turner, 'Sweden Bans Use of Huawei and ZTE Equipment in 5G Networks', *Mobile Europe*, 21 October 2020, <<https://www.mobileeurope.co.uk/sweden-bans-use-of-huawei-and-zte-equipment-in-5g-networks/>>, accessed 4 September 2026.
 27. UN Trade & Development, 'China - Sweden BIT (1982)', <<https://investmentpolicy.unctad.org/international-investment-agreements/treaties/bit/976/china---sweden-bit-1982->>, accessed 2 September 2026.
 28. *Euronews*, 'Huawei is Taking Sweden to Court After the Country Banned Its 5G Products', 31 January 2022, <<https://www.euronews.com/next/2022/01/31/huawei-is-taking-sweden-to-court-after-the-country-banned-its-5g-products>>, accessed 2 September 2026.

shape how other states can lawfully exclude Chinese vendors from gaining access to foreign CNI on security grounds, illustrating that Chinese firms increasingly meet such exclusions not only with diplomatic and economic pressure but also with formal legal challenges to host states' security decisions.²⁹

As the profiles of Germany, Spain and the UK illustrate in this paper, different states have weighted these three categories of risk differently, depending on their broader strategic priorities and economic exposure to China.

The Evolution of the EU's Approach to High-Risk Vendors

In recent years, the European Commission has taken a more central role in managing high-risk ICT vendors in Europe. The EU's approach has developed in stages: initial voluntary, non-binding measures that were formally country-neutral have given way to more interventionist policies that explicitly seek to designate and exclude Chinese vendors from critical technology supply chains.

In 2020, the EU introduced its voluntary Toolbox for 5G Security,³⁰ which sought standardised approaches for assessing and managing high-risk telecommunications vendors. The Toolbox recommends that member states use a combination of 'strategic' and 'technical' measures to assess vendor risks and exclude them from 'critical or sensitive' parts of 5G infrastructure. Although the Toolbox is ostensibly neutral towards country of origin, in 2023 the Commission stated explicitly how the Toolbox should be implemented, saying that 'Huawei and ZTE represent ... materially higher risks than other 5G suppliers' as a result of 'their likelihood of being influenced by specific third countries which have security laws and corporate governance that are a potential risk for the security of the Union'.³¹ There has been an inconsistent approach to adoption of the Toolbox across EU member states. Only 10 of 27 have fully implemented it and Austria, Bulgaria, Hungary and Cyprus apparently have no plans to adopt the measures.³² At the start of 2025, the European Commission's Executive Vice-President for Tech Sovereignty, Security and Democracy, Henna Virkkunen, reportedly rebuked EU member states that had yet to

29. Ming Du, 'Huawei Strikes Back: Challenging National Security Decisions before Investment Arbitral Tribunals', *Emory International Law Review* (Vol. 37, No. 1, 2022), pp. 1–54.

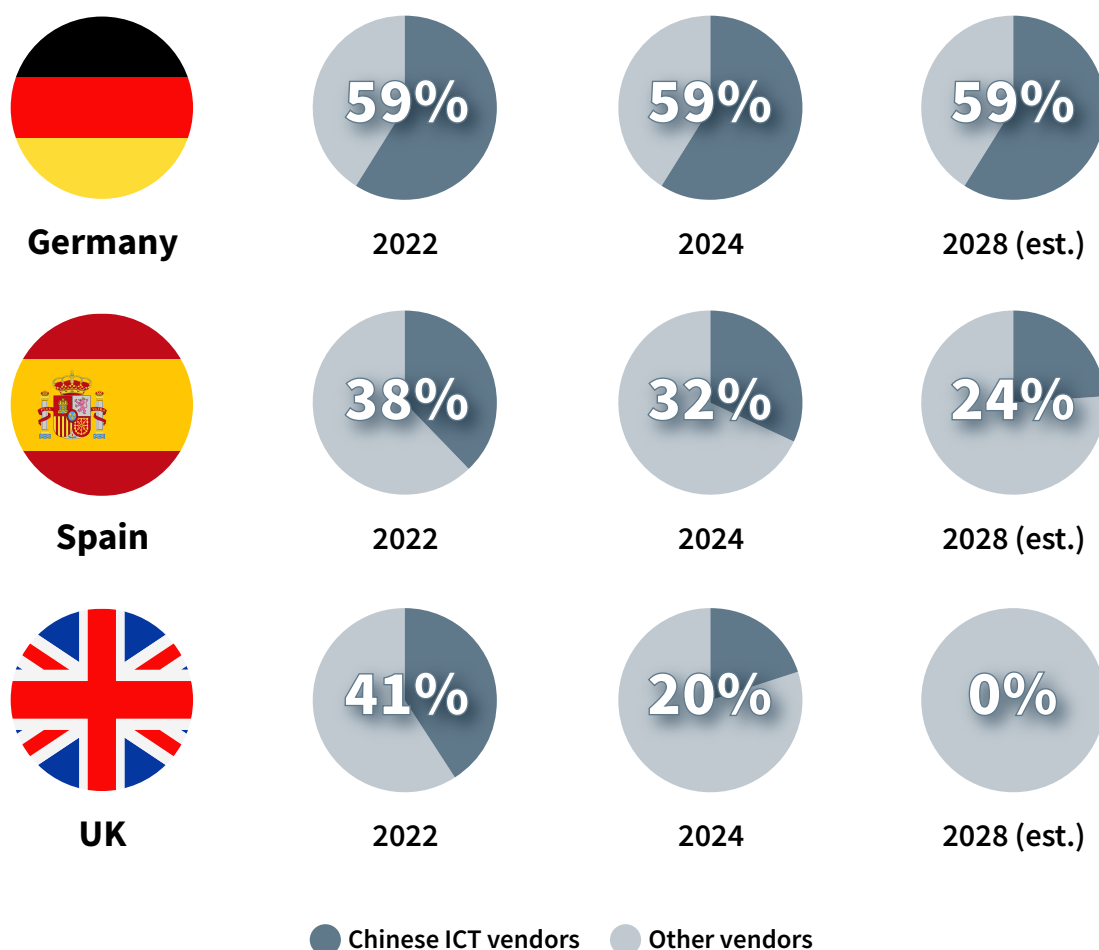
30. European Commission, *The EU Toolbox for 5G Security*.

31. European Commission, 'Communication from the Commission: Implementation of the 5G Cybersecurity Toolbox', 15 June 2023, <<https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox>>, accessed 4 June 2026.

32. Théophane Hartmann, 'Seventeen EU Countries Not Ready to Cut China 5G Dependence', *Euractiv*, 19 March 2025, <<https://www.euractiv.com/news/seventeen-eu-countries-not-ready-to-cut-china-5g-dependence/>>, accessed 2 September 2026.

implement the measures during a panel event.³³ Chinese vendors' share of 5G RAN in Germany, Spain and the UK is shown in Figure 1.

Figure 1: Chinese ICT Vendors' Share of 5G RAN



Source: Strand Consult, 'The Market for 5G RAN in 2024: Share of Chinese and Non-Chinese Vendors in Europe', 10 January 2025, <<https://strandconsult.dk/get-your-free-copy-of-strand-consults-new-study-the-market-for-5g-ran-in-2024-share-of-chinese-and-non-chinese-vendors-in-europe/>>, accessed 2 September 2026.

33. Iain Morris, 'European Threatens "Further Measures" Against Huawei as Trump Returns', *Light Reading*, 20 January 2025, <<https://www.lightreading.com/5g/europe-threatens-further-measures-against-huawei-as-trump-returns>>, accessed 2 September 2026.

In January 2026, the European Commission articulated a shift in its approach towards high-risk vendors when it proposed amendments to the EU CSA.³⁴ The amendments will give the Commission the power to assess, designate and restrict high-risk vendors from 18 CNI sectors. EU member states must then phase out designated vendors within 36 months. The Commission has signalled that if the amendments pass, it will start by suggesting European telecoms operators remove Huawei and ZTE from 5G networks. All vendors designated as ‘high-risk’ will also be prohibited from participating in European standards development, receiving EU funding or holding an EU cyber security certification.³⁵ These prohibitions may effectively exclude some vendors from the EU market.

Prior to the announcement, there was speculation in industry that the amendments might form part of a broader push to advance European technological sovereignty and decrease its dependence on US technology giants.³⁶ However, the detail of the proposed legislation indicates the measures are aimed at Chinese companies. It states that the Commission’s risk assessments will consider a vendor’s links to countries that ‘carry out malicious cyber activities or campaigns against the Union or Member States’, but which also do not have ‘independent and democratic control mechanisms’³⁷ – language that could be taken to be clearly, if diplomatically, aimed at China.

At the time of writing, the amendments have not yet passed and it is likely that there will be pushback from some EU member states. Nevertheless, this move suggests a significant shift towards a more interventionist, cross-European approach to managing high-risk vendors.

The following three country case studies explore how three different European countries – Germany, Spain and the UK – have tried to manage the risks associated with Chinese ICT vendors.

-
34. European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European Cybersecurity Certification Framework, and ICT Supply Chain Security and Repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)’; Foo Yun Chee, ‘EU Plan to Phase-Out High-Risk Tech Draws Fire from China’s Huawei’, *Reuters*, 21 January 2026.
 35. European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European Cybersecurity Certification Framework, and ICT Supply Chain Security and Repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)’.
 36. This risk was raised in interviews with stakeholders from the cyber security industry in Spain, Germany and the UK.
 37. European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European Cybersecurity Certification Framework, and ICT Supply Chain Security and Repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)’, pp. 52, 53.

Germany

Strategic Context

Germany has historically taken a slow and cautious approach to reducing exposure to high-risk ICT vendors. Germany's close economic relationship with China has contributed to a political-level reluctance to take decisive actions against potential security risks posed by dependence on Chinese technology. Geopolitical and legislative developments, however, have contributed to a shift in Germany's strategic posture and its approach towards high-risk vendors since mid-2025. This may yet translate into the development and implementation of more robust policy to reduce exposure to high-risk vendors, both in telecoms and other sectors.

Germany's foreign policy relationship with China is shaped by its large and growing trade dependence. In 2025, China was Germany's most important trading partner, with the annual bilateral trade turnover between the two states totalling €251.8 billion.³⁸

This strategic context has shaped Germany's historically cautious approach to restricting the exposure of various sectors to Chinese or other high-risk ICT vendors, exemplified by Germany's longstanding hesitance to remove Huawei from its 5G telecoms network.³⁹ Only in 2024 did the German government ultimately opt to phase out Chinese vendors from the 'core' of its 5G network, several years after various other key EU member states.⁴⁰ Furthermore, despite the gradual emergence of debate on vendor risks to sectors besides telecoms – most notably renewable energy – a cross-sector, strategic and transparent discussion of high-risk ICT vendors was absent from German policy discussions when research interviews for this paper were conducted in summer and autumn 2025.⁴¹

38. Destatis, 'China is Germany's Most Important Trading Partner Once Again in 2025', 20 February 2026, <https://www.destatis.de/EN/Press/2026/02/PE26_056_51.html>, accessed 11 August 2026.

39. Rühlig, 'The "Huawei Saga" in Europe Revisited'.

40. Federal Ministry of the Interior and Community (BMI), 'Greater Security and Technological Sovereignty for the German 5G Mobile Network: The Federal Government Concludes Contracts with Telecommunications Companies', 11 July 2024, <<https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2024/07/5g-en.html>>, accessed 14 August 2026.

41. Authors' interview with civil society representative, Berlin, 5 June 2025.

There are now signs, however, that Germany's approach may become more robust. Germany moved towards a more pragmatic and competitive approach to China under Chancellor Olaf Scholz – as documented by Germany's 2023 China Strategy.⁴² Since becoming Chancellor in May 2023, Friedrich Merz has gone further, adopting a 'de-risking' approach towards relations with China. Once again, the hard edge of Germany's foreign policy posture towards China is demonstrated by restrictions in the telecoms sector. In November 2023, Merz announced that Germany 'will not allow components from China in [its] 6G network'.⁴³ Although the integration of 6G technology into telecoms networks is still several years away, this announcement has signalled a more proactive approach to reducing Germany's exposure to high-risk vendors in the telecoms sector.

These changes should also be considered in their broader context. Amid the current climate of heightened global risk of conflict and deteriorated Euro-Atlantic relations, Merz has adopted a more assertive posture on defence and security.⁴⁴ These circumstances are clearly having an impact on the debate on high-risk vendors. In Germany, concerns about the reliability of Euro-Atlantic ties have reframed understandings of vendor risks in the context of dependence on US technology and an emerging emphasis on European tech sovereignty.⁴⁵ Over-reliance on US vendors – particularly in the public sector – is a clear anxiety for Germany policymakers and wider society.⁴⁶

The debate on high-risk vendors has also widened in terms of the sectors under consideration. Foreign cloud providers face particular scrutiny considering Germany's heightened sensitivity around data protection (which stems from both historical and recent concerns⁴⁷). This has caused considerable pushback against the roll-out of cloud

42. Federal Foreign Office, 'The 2023 Federal Government Strategy on China', 24 January 2023, <<https://www.auswaertiges-amt.de/en/ausserpolitik/regionaleschwerpunkte/asien/strategy-on-china-2608618>>, accessed 14 August 2026.

43. *Heise Online*, 'Chancellor Merz: "Will Not Allow Components from China in 6G Network"', 15 November 2023, <<https://www.heise.de/en/news/Chancellor-Merz-Will-not-allow-components-from-China-in-6G-network-11080056.html>>, accessed 18 June 2026.

44. Matteo Villa, 'Leader to Watch in 2026: Friedrich Merz', Italian Institute for International Political Studies (ISPI), 24 December 2023, <<https://www.ispionline.it/en/publication/leader-to-watch-in-2026-friedrich-merz-226485>>, accessed 14 August 2026.

45. Élysée, 'Summit on European Digital Sovereignty Delivers Landmark Commitments for a More Competitive and Sovereign Europe', press release, 18 November 2023, <<https://www.elysee.fr/en/emmanuel-macron/2023/11/18/summit-on-european-digital-sovereignty-delivers-landmark-commitments-for-a-more-competitive-and-sovereign-europe>>, accessed 18 June 2026.

46. Authors' interview with think tank researcher, Berlin, 3 June 2025.

47. Alvar C H Freude and Trixy Freude, 'Echoes of History: Understanding German Data Protection', *Bertelsmann Foundation* (1 October 2016), <<https://www.bfna.org/politics-society/echoes-of-history-4tdtdjes5l/>>, accessed 27 August 2026.

computing infrastructure, with some German states, for example, Schleswig-Holstein, actively moving away from US cloud providers in pursuit of greater digital sovereignty.⁴⁸

Despite this noticeable shift in the strategic context, it remains to be seen whether these changes in rhetoric will translate into a step change in Germany's approach to high-risk Chinese ICT vendors. This will depend on debate leading to tangible policy changes and new security-focused legislation being implemented effectively.

Policy, Legislation and Regulation

Germany lacks a unified or statutory definition of a high-risk vendor. The most relevant terminology recurring in the German policy and industry debate surrounding this issue is 'untrustworthy vendors' for 'critical components'.⁴⁹

The first major legislative intervention introduced in the German context to deal with the risks posed by high-risk ICT vendors was the IT Security Law 2.0 (IT-Sicherheitsgesetz 2.0) passed by the Bundestag in April 2021.⁵⁰ Under this law, CNI carriers were required to notify the Ministry of the Interior (Bundesministerium des Innern, BMI) of the components they intended to use for technical and security assessment by Germany's Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI). The law also included provisions for geopolitical assessment of components (as detailed below) to be led on by the BMI.⁵¹ Ultimately, it allows the BMI to exclude components based on these technical, security and geopolitical assessments.

The law is sector-agnostic. In practice, however, it was understood as a response to the Huawei debate and to concerns about security in the telecoms sector in particular. One German official noted that it has not been applied substantively outside this sector.⁵² In fact, the technical assessment that the BSI made under this provision was not even referenced in the final agreement the BMI made with Germany's main telecoms

48. SecurEnvoy, 'German State Moves Beyond Microsoft? Exploring the Rise of Open-Source Alternatives', 22 May 2025, <<https://securenvoy.com/blog/german-state-moves-beyond-microsoft/>>, accessed 18 June 2026.

49. Authors' interview with German government official, Berlin, 6 June 2025. These are the terms used in the IT Security Act 2.0. See Federal Office for Information Security (BSI), 'Second Act on Increasing the Security of IT Systems (German IT Security Act 2.0)', <https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html>, accessed 2 September 2026. For an English language explainer to the terms, see Gleiss Lutz, 'IT Security Act 2.0 – Prohibition on the Use of Critical Components to Protect Public Security', 31 May 2021, <<https://www.gleisslutz.com/en/know-how/it-security-act-20-prohibition-use-critical-components-protect-public-security>>, accessed 14 September 2026.

50. Federal Office for Information Security (BSI), 'Second Act on Increasing the Security of IT Systems (German IT Security Act 2.0)', <https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html>, accessed 2 September 2026.

51. Fabian Niemann, 'The German IT Security Act 2.0 Comes into Force – Overview of the Most Significant Changes to the BSI Act', Bird and Bird, 26 May 2021, <<https://www.twobirds.com/en/insights/2021/germany/the-german-it-security-act-2-0-comes-into-force>>, accessed 2 September 2026.

52. Authors' interview with German government official, Berlin, 6 June 2025.

providers in 2024 to exclude certain parts and software by Chinese providers ZTE and Huawei, which it implies are not ‘trustworthy’.⁵³

The law also takes a vendor-centric – as opposed to state-centric – approach to assessing high-risk suppliers. It is the trustworthiness of individual companies, rather than the countries of origin, which is evaluated.⁵⁴ The BMI’s geopolitical assessment of what constitutes an untrustworthy vendor takes into account factors such as direct or indirect state control,⁵⁵ and a vendor’s involvement in activities that have an impact on the public order or security aims of Germany, the EU or NATO. In practice, however, geopolitical considerations bear heavily on these assessments, and the gap between the formal country-neutral framing and the underlying geopolitical logic has made Germany’s approach appear inconsistent.

More recent shifts in strategic context have prompted further legislative and regulatory changes relevant to the challenge posed by high-risk technology vendors. First, in November 2025, the Federal Network Agency (Bundesnetzagentur) published a draft of new requirements to enhance protective measures of telecoms service providers against cyber threats under the Telecommunications Act.⁵⁶ The draft was seen by commentators as ‘the technical and regulatory implementation of the political decision to significantly increase the security of German 5G networks’.⁵⁷

New legislation now seeks to expand the ability of the BMI to exclude vendors beyond both federal agencies and outside the telecoms context. Despite previous delays, Germany has now passed new legislation to implement the EU’s NIS2 Directive, effective December 2025.⁵⁸ This implementation law also updates the IT Security Law 2.0. It increases the cyber security requirements for federal agencies and expands

53. Bundesministerium des Innern (BMI), ‘Stärkung der Sicherheit und technologischen Souveränität der deutschen 5G-Mobilfunknetze’ [‘Strengthening the Security and Technological Sovereignty of Germany’s 5G Mobile Networks’], 11 July 2024, <<https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2024/07/5g.html>>, accessed 18 June 2026. Author translation.

54. Federal Office for Information Security (BSI), ‘Second Act on Increasing the Security of IT Systems (German IT Security Act 2.0)’.

55. Bundesministerium des Innern (BMI), ‘Stärkung der Sicherheit und technologischen Souveränität der deutschen 5G-Mobilfunknetze’ [‘Strengthening the Security and Technological Sovereignty of Germany’s 5G Mobile Networks’]. Author translation.

56. Bundesnetzagentur, ‘Überarbeitung des Kataloges von Sicherheitsanforderungen’ [‘Revision of the Catalog of Safety Requirements’], October 2025, <<https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/Konsultation/start.html>>, accessed 2 September 2026. Author translation.

57. Stefan Krempel, ‘Federal Network Agency Tightens Security for Telecom Providers’, *Heise Online*, 3 November 2025, <<https://www.heise.de/en/news/Federal-Network-Agency-tightens-security-for-telecom-providers-10996857.html>>, accessed 18 June 2026.

58. The NIS2 Directive establishes a unified legal framework to uphold cybersecurity in 18 critical sectors across the EU. Germany is implementing this via the following legislation: Bundesgesetzblatt, ‘Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung’ [‘Law Implementing the NIS-2 Directive and Regulating Essential Principles of Information Security Management in the Federal Administration’], 5 December 2025, <<https://www.recht.bund.de/bgbl/1/2025/301/VO.html>>, accessed 2 September 2026. Author translation.

the scope of the legislation to cover not only CNI operators but also other ‘important entities’ (companies of a certain size or turnover).⁵⁹

In this sense, Germany’s NIS2 implementation law goes beyond EU-mandated minimum standards, as do those of other member states, such as Belgium and Italy.⁶⁰ It grants the BMI additional powers to determine what qualifies as a ‘critical component’ and prohibits or limits the use of critical components in all CNI sectors, including the energy sector. The renewable energy sector is likely to be of particular concern for Germany, as the debate around Chinese vendors has been more advanced in the context of solar panels⁶¹ and wind turbines.⁶² Components fulfilling critical functions had already been defined for energy networks and power stations under paragraph 11 of the Energy Industry Act (ENWG, Gesetz über die Elektrizitäts- und Gasversorgung); in December 2025 these provisions were relocated and expanded by the NIS2 implementation law.⁶³

Policy Implementation Approach, Gaps and Challenges

In practice, Germany’s regulatory and legislative tools for managing risk posed by certain IT vendors often remain unused. The foremost German case study for the actual enforcement of high-risk vendor policy remains the eventual exclusion of Chinese vendors from German telecoms infrastructure.

As previously suggested, Germany was slower than many European counterparts to regulate or exclude Chinese vendors. Only in July 2024 did the BMI and three main telecoms operators reach an agreement to phase out components made by Huawei and

59. *Ibid.*, p. 3.

60. Curtis McCluskey and Joseph Ndep, ‘Navigating NIS2: What Organisations Need to Know as EU Implementation Unfolds’, Goodwin, 23 October 2025, <<https://www.goodwinlaw.com/en/insights/publications/2025/10/insights-practices-dpc-navigating-nis2-what-organisations-need-to-know>>, accessed 2 September 2026.

61. Julius Baumeister, Herbert Kordes and Falk Steiner, ‘Solaranlagen: Gefahr aus China?’ [‘Solar Panels: Danger from China?’], *Tagesschau*, 14 August 2025, <<https://www.tagesschau.de/investigativ/monitor/solar-anlagen-sabotage-china-100.html>>, accessed 18 June 2026. Author translation.

62. Kathrin Witsch and Sabine Gusbeth, ‘Windräder aus China: Militärexperten warnen vor Spionage’ [‘Wind Turbines from China: Military Experts Warn of Espionage’], *Handelsblatt*, 28 February 2025, <<https://www.handelsblatt.com/unternehmen/energie/windraeder-aus-china-militaerexperten-warnen-vor-spionage/100109846.html>>, accessed 18 June 2026. Author translation.

63. Bundesministerium der Justiz für Verbraucherschutz and Bundesamt für Justiz, ‘Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG)’ [‘Law on Electricity and Gas Supply (Energy Industry Act – EnWG)’], 7 July 2005, <https://www.gesetze-im-internet.de/enwg_2005/BJNR197010005.html>, accessed 18 June 2026. Author translation; Bundesgesetzblatt, ‘Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung’ [‘Law Implementing the NIS-2 Directive and Regulating Essential Principles of Information Security Management in the Federal Administration’]. Author translation.

ZTE from Germany's 5G network.⁶⁴ Under this agreement, 'critical components' made by Huawei and ZTE must be removed from the core of 5G networks by the end of 2026, while mobile phone operators must remove these components from the 'critical function of 5G network management systems' (referring to software) by 2029. ZTE and Huawei can continue to sell hardware to Germany's telecoms providers except for 'critical components', which must be security certified by the BSI from 2026 onwards.

Some have questioned Germany's prospects for ensuring timely or impactful enforcement of this regulation. As of 2024, Chinese vendors still provided 58% of Germany's 5G sites,⁶⁵ including software for 5G base stations. Under the new agreement, Huawei's and ZTE's network management software will be phased out by 2029, yet experts remain sceptical whether large telecoms providers such as Deutsche Telekom will be able to replace Chinese software with European alternatives.⁶⁶ Some commentators have seen the compromise as 'a significant step toward bolstering technological sovereignty and national security'.⁶⁷ However, the agreement's scope is still narrow and focused solely on the software 'core' of Germany's 5G infrastructure, as a result of successful industry lobbying.⁶⁸ This illustrates Germany's difficulty balancing network modernisation with economic and security concerns.⁶⁹

A second case study of Germany's approach to managing high-risk ICT vendors is provided by the BSI's warning, in March 2022, about Kaspersky, a Russian anti-virus application. One month after the full-scale invasion of Ukraine, the BSI published a warning directed at users and industry, recommending that they switch from Kaspersky to other providers under paragraph 7 of the IT Security Act 2.0.⁷⁰ The BSI's accompanying press release explicitly mentioned the actions of Russian forces and Russian threats against the EU, NATO and Germany as context for the BSI's doubts

-
64. BSI, 'BSI ermöglicht effizientere Zertifizierung sicherheitskritischer 5G-Komponenten' ['BSI Enables More Efficient Certification of Security-Critical 5G Components'], press release, 10 July 2025, <https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250710_Zertifizierung_5G-Komponenten.html>, accessed 18 June 2026. Author translation.
 65. Strand Consult, 'Fact-Check: GSMA Intelligence's Report "The Cost of Removing Designated Third-Country Vendors from EU Telecoms Networks"'.
 66. Iain Morris, 'German Telcos Pool Efforts to Retain More "Open" Huawei – Sources', *Light Reading*, 5 March 2025, <<https://www.lightreading.com/5g/german-telcos-pool-efforts-to-retain-more-open-huawei-sources>>, accessed 18 June 2026.
 67. Aparna Divya, 'Germany is Phasing out Chinese Tech from 5G Networks. Is It the Right Call?', *The Diplomat*, 26 July 2024, <<https://thediplomat.com/2024/07/germany-is-phasing-out-chinese-tech-from-5g-networks-is-it-the-right-call/>>, accessed 18 June 2026.
 68. Authors' interview with civil society representative, Berlin, 5 June 2025.
 69. Heise Online, 'Huawei Ban: Early "Assurances", Delays and Lobby Pressure', 3 August 2024, <<https://www.heise.de/en/news/Huawei-ban-Early-assurances-delays-and-lobby-pressure-9822560.html>>, accessed 18 June 2026.
 70. Alex Scroxton, 'German Authorities Warn on Kaspersky but Stop Short of Ban', *Computer Weekly*, 16 March 2022, <<https://www.computerweekly.com/news/252514679/German-authorities-warn-on-Kaspersky-but-stop-short-of-ban>>, accessed 18 June 2026.

about Kaspersky's 'reliability' and the warning more broadly.⁷¹ The BSI's assessment was criticised by Kaspersky on the grounds that it was 'political'⁷² rather than focused on technical assessments that the BSI typically prioritised.⁷³ Ultimately, this led to legal pushback from Kaspersky comprising requests for injunctions, appeals and ultimately a constitutional complaint, all of which were declined.⁷⁴ This example demonstrates not only Germany's reluctance to take binding measures to exclude high-risk vendors – the BSI's response fell short of a ban⁷⁵ – but also the potential risks of backlash or legal repercussions when governments target interventions against specific vendors on criteria that are deemed political or only selectively implemented.

Beyond 5G and Kaspersky, there were no other publicly known examples of vendor exclusions in Germany at the time of writing. Until the NIS2 regulation came into force in December 2025, Germany did not impose regulations with respect to the private sector's risk management of high-risk ICT vendors. One government official stressed that there was 'very much a "private sector own risk" approach' and that the German government generally does not interfere in these matters.⁷⁶ The official explicitly mentioned the integration of Huawei products in a German chemical producer's (part of Germany's CNI) intranet.

Under the new NIS2 regulation, the BMI now enjoys extended powers and could, in theory, implement vendor exclusions in the private sector. Implementation is, however, a separate and largely political question. The 5G phasing out agreement and the Kaspersky decisions were made under Germany's former centre-left government. While Merz has signalled a renewed emphasis on security and championed the idea of European digital sovereignty, his government has also committed state modernisation and digitalisation as a key mission (via its new Digital Ministry).⁷⁷

-
71. BSI, 'BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten (archiviert)' ['BSI Warns Against the Use of Kaspersky Antivirus Products (Archived)'], 5 March 2022, <https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/Presse-Archiv/220315_Kaspersky-Warnung.html>, accessed 01 June 2026. Author translation.
 72. BBC News, 'Germany Warns Against Russian Anti-Virus Use', 15 March 2022.
 73. Jochen Michels, 'Call for More Evidence in Cybersecurity: Clear Assessment Criteria for a Secure Digital Future in Germany, Europe, and the World', Kaspersky, 16 December 2025, <<https://www.kaspersky.com/about/policy-blog/call-for-more-evidence-in-cybersecurity-clear-assessment-criteria-for-a-secure-digital-future-in-germany-europe-and-the-world>>, accessed 18 June 2026.
 74. Dennis-Kenji Kipker, 'War die Warnung vor Kaspersky politisch motiviert?' ['Was the Kaspersky Warning Politically Motivated?'], *Legal Tribune Online*, 5 August 2022, <<https://www.lto.de/recht/hintergruende/h/kaspersky-software-virenschutz-warnung-bsi-it-sicherheit-rechtswidrig-neue-erkenntnisse-recherche>>, accessed 14 September 2026. Author translation.
 75. Scropton, 'German Authorities Warn on Kaspersky but Stop Short of Ban'.
 76. Authors' interview with German government official, Berlin, 6 June 2025.
 77. Euronews, 'Merz's Government Decree Gives German Digital Ministry Extensive Powers', 7 May 2025, <<https://www.euronews.com/next/2025/05/07/merz-s-government-decree-gives-german-digital-ministry-extensive-powers>>, accessed 2 September 2026.

If Merz indeed has the political will to implement and enforce new legislation and policies, some sectors will be of higher priority than others, as several private sector industries have already received critical attention for relying on potentially high-risk vendors. These include the growing green energy sector, especially with respect to solar panels and wind turbines. Germany's rail network still heavily relies on Huawei technologies – despite criticism from the BMI, which the Ministry of Transport rejects.⁷⁸ Vendors in these sectors could be next to face further scrutiny and more rigorous enforcement under Merz's revived commitment to addressing the risks posed by certain ICT vendors.

78. Sarah Marsh, 'Exclusive: Deutsche Bahn Bets on Huawei for Railway Digitalisation Despite Security Concerns', *Reuters*, 10 March 2023.

Spain

Strategic Context

Spain's strategic approach to high-risk ICT vendors is anchored in pragmatism, prioritising economic opportunity and legal compliance over geopolitical risk considerations. Unlike some members of the Five Eyes or northern European counterparts, Spain does not consistently single out Chinese vendors as a national security threat. Stakeholders in security-focused institutions such as Centro Criptológico Nacional (CCN) – the cyber security arm of the National Intelligence Centre (Centro Nacional de Inteligencia) – do, however, consistently assess that China represents a risk,⁷⁹ comparable in intent to Russia or North Korea due to its national intelligence legislation requiring companies to cooperate with state security services. However, this high-risk assessment is not shared uniformly across Spain's government departments. Interviewees noted that debates around high-risk vendors are increasingly filtered through a broader digital sovereignty lens, in which US vendors are also viewed with caution.⁸⁰

Spain's broader foreign and economic policy remains focused on the EU, NATO and the Americas, with China occupying a sporadic rather than strategic position. Economic exposure to China is limited compared with the UK and Germany. However, specific trade dependencies do exist. Spain is the EU's largest pork exporter to China, for instance, with exports valuing approximately €2.6 billion in 2021.⁸¹ Spain is also actively pursuing Chinese investment in strategic sectors such as electric vehicles and renewable energy, for instance via the Chery–Ebro partnership for electric vehicle production in Spain,⁸² and a \$1-billion hydrogen energy project developed with the Chinese company Envision.⁸³ These initiatives align with Spain's broader goals for the

79. Authors' interview with academic, online, 11 August 2025.

80. Authors' interview with US tech company executive, online, 21 July 2025; authors' interview with academic, online, 11 August 2025.

81. Merics, 'Country Profile: Spain', <<https://merics.org/en/country-profile-spain>>, accessed 14 September 2026.

82. Catalonia Trade & Investment, 'Chinese Company Chery Chooses Barcelona for Its First Electric Car Plant in Europe', 19 April 2024, <<https://catalonia.com/w/chinese-company-cheri-chooses-barcelona-for-its-first-electric-car-plant-in-europe>>, accessed 2 July 2026.

83. Inti Landauro, 'China's Envision to Invest \$1 bln in Spain to Make Green Hydrogen Machinery', *Reuters*, 10 September 2024.

green transition but deepen its economic entanglement with China. The more Spain relies on Chinese investment, the costlier it becomes to restrict Chinese vendors, since policymakers believe such measures risk provoking retaliation, making protective policies less attractive even where security concerns would favour them.

Experts interviewed for this paper repeatedly noted that senior Spanish political leaders view China through a transactional diplomatic and commercial lens, underestimating the ideological role of the CCP and Beijing's strategic use of technology exports.⁸⁴ One participant further argued that Spain's response to high-risk vendor concerns is marked more by a reactive focus on technical compliance with a set of standards (detailed in the next section) than by a coherent, strategic geopolitical approach.⁸⁵

In its approach to high-risk vendors, Spain appears to adhere to EU policy where it is explicit but to exploit legislative ambiguity where it exists. Consequently, high-risk vendors continue to retain a presence in significant components of Spain's public sector ICT environment.

Policy, Legislation and Regulation

Spain lacks a unified statutory definition of a high-risk vendor. The designation exists only in the 5G sector under Royal Decree-Law 7/2022 and Royal Decree 443/2024 (ENS5G), which allow authorities to assess and restrict vendors based on EU 5G Toolbox criteria such as foreign state influence and transparency.⁸⁶ No supplier has yet been publicly designated under these mechanisms. For all other digital systems, governance relies on the Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC),⁸⁷ Spain's national allowlist of technology products approved for public sector procurement. It is compiled and maintained by the CCN in coordination with the Instituto Nacional de Ciberseguridad (INCIBE, National Cyber Security Institute).⁸⁸ The CPSTIC operates as a positive selection mechanism. Only products that pass certification appear on the allowlist, while those that are not

84. Authors' interview with academic, online, 11 August 2025; authors' interview with think tank researcher, online, 28 July 2025.

85. Authors' interview with academic, online, 11 August 2025.

86. 'Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación' ['Royal Decree-Law 7/2022, of 29 March, on Requirements to Guarantee the Security of Fifth Generation Electronic Communications Networks and Services'], 30 March 2022, <<https://www.boe.es/eli/es/rdl/2022/03/29/7>>, accessed 2 September 2022. Author translation; 'Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G' ['Royal Decree 443/2024, of April 30, Approving the National Security Framework for 5G Networks and Services'], <<https://www.boe.es/buscar/act.php?id=BOE-A-2024-8715>> accessed 2 September 2026. Author translation.

87. Centro Criptológico Nacional, 'Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC)' ['CPSTIC: Catalogue of Information and Communication Technology Security Products and Services'], <<https://cpstic.ccn.cni.es/en/>>, accessed 18 June 2026.

88. Instituto Nacional de Ciberseguridad (INCIBE), 'INCIBE', <<https://www.incibe.es/en>>, accessed 18 June 2026.

submitted for assessment or fail evaluation are absent. There is no blocklist by vendor or country of origin as such; any supplier – Chinese, American or European – may appear on the CPSTIC if it clears the technical bar.

Spain's decentralised administrative structure grants regional and municipal authorities significant discretion over technology procurement. National cyber security bodies demonstrate high levels of risk awareness and EU alignment in areas considered critical, such as defence networks and 5G cores; yet at a local level, procurement is shaped primarily by budget and availability.⁸⁹ Several regions continue to actively engage with Chinese firms.⁹⁰ Catalonia stands out with initiatives such as a dedicated China Investment Desk⁹¹ and the development of a new Port of Barcelona terminal for Chinese electric vehicle imports.⁹² The overall result is a two-speed security culture in Spanish digital infrastructure – selective risk aversion at the national level combined with permissiveness at the local level.

Spain's National Cybersecurity Strategy⁹³ equips the government with soft regulatory levers, such as risk assessment requirements, certification and supply-chain obligations. In the case of domains such as privately owned CNI, these levers can strongly influence procurement decisions, but stop short of giving direct authority to the state, again reflecting Spain's broader preference for technical compliance over geopolitical exclusion. The National Cybersecurity Strategy is currently under review as part of a larger 2026 España Digital (Digital Spain) plan.⁹⁴

Spain is slowly transposing NIS2 into legislation,⁹⁵ with only draft legislation created so far,⁹⁶ despite the EU's mandate that the directive be transposed into national law by 18

89. Authors' interview with cyber security consultant, online, 20 May 2025.

90. Qian Zhou, 'China-Spain Relations: Trade, Investment, and Industry Opportunities', *China Briefing*, 11 September 2024, <<https://www.china-briefing.com/news/china-spain-relations-trade-investment-and-industry-opportunities/>>, accessed 18 June 2026.

91. Government of Catalonia, 'Government of Catalonia Creates China Desk to Boost Chinese Investment in Catalonia', press release, 18 January 2023, <<https://catalangovernment.eu/catalangovernment/news/573082/government-of-catalonia-creates-china-desk-to-boost-chinese-investment-in-catalonia>>, accessed 2 September 2026.

92. *Catalan News*, 'Port of Barcelona Breaks Ground on New Vehicle Terminal to Attract Chinese Cars', 9 April 2026, <<https://www.catalannews.com/business/item/port-of-barcelona-breaks-ground-on-new-vehicle-terminal-to-attract-chinese-cars>>, accessed 2 September 2026.

93. National Security Department of Spain, 'Estrategia Nacional de Ciberseguridad 2019' ['National Cybersecurity Strategy 2019'], <<https://www.dsn.gob.es/es/publicaciones/estrategias-sectoriales/ENC2019>>, accessed 7 September 2026.

94. La Moncloa (official website of the president of the government of Spain), 'Pedro Sánchez Announces the Creation of the National Cybersecurity Centre, Attached to the Presidency of the Government', 16 October 2025, <<https://www.lamoncloa.gob.es/lang/en/presidente/news/paginas/2025/20251016-information-security-meeting.aspx>>, accessed 2 September 2026.

95. Álvaro Gutiérrez Serrano, 'NIS2: Strengthening Europe's Digital Resilience and Reviewing Its Impact', Telefónica blog, 3 June 2025, <<https://www.telefonica.com/en/communication-room/blog/nis2-strengthening-europes-digital-resilience-reviewing-impact/>>, accessed 18 June 2026.

96. David Galindo, 'NIS2 Directive: Transposition in Spain and Draft Law', iSEC Auditors blog, 28 November 2025, <<https://blog.isecauditors.com/en/nis2-directive-transposition-in-spain-and-draft-law>>, accessed 18 June 2026.

October 2024.⁹⁷ This represents more than administrative delay; it underscores a deeper policy misalignment between EU strategic intent and Spain's established cyber security governance model. Spain's current framework remains anchored in technology-neutral certification (National Security Framework, ENS / CPSTIC) and procurement laws prioritising cost and market openness.⁹⁸ While the government has publicly reaffirmed its commitment to cyber security, including plans for a new National Cybersecurity Centre,⁹⁹ a number of northern European states have moved beyond this baseline to restrict specific high-risk vendors on security grounds. Spain has not. This inaction has enabled the widespread deployment of Chinese-supplied infrastructure across non-telecoms public services¹⁰⁰ and heightened reputational and alliance risks, as illustrated by the recent example of Huawei being contracted to provide cloud storage for Spain's judicial wiretap infrastructure.¹⁰¹

Against this backdrop, interviewees characterised the cumulative regulation as burdensome, discussing 'framework fatigue',¹⁰² with small to medium-sized enterprises struggling to implement the required changes. In the authors' analysis, Spain's policy model draws a sharp regulatory boundary between telecoms and other ICTs, with origin-based security only codified for the former.

Policy Implementation Approach, Gaps and Challenges

Spain's approach to high-risk vendor governance is defined by an implementation gap: robust where legal authority and political will converge, but more permissive elsewhere. In areas where legal authorities and political incentives converge, most visibly in 5G, Spain demonstrates some alignment with EU and NATO expectations. At the end of 2022, around 38% of Spain's 5G network was based on Huawei equipment, placing Spain among the highest users of Chinese 5G vendors in Europe. However, this is now modestly declining as Spanish telecoms operators have committed to removing

97. European Commission, 'NIS2 Directive: Securing Network and Information Systems', <https://www.nis-2-directive.com/NIS_2_Directive_Transposition.html>, accessed 2 September 2026.

98. Authors' interview with cyber security executive, online, 21 July 2025; authors' interview with academic, online, 11 August 2025.

99. La Moncloa, 'Pedro Sánchez Announces the Creation of the National Cybersecurity Centre, Attached to the Presidency of the Government'.

100. Authors' interview with academic, online, 11 August 2025.

101. Natasha Buckley, Pia Hüscher and Jamie MacColl, 'European Critical Infrastructure Still Struggles with Chinese ICT Vendors', *The Strategist* blog, 22 July 2025, <<https://www.aspistrategist.org.au/european-critical-infrastructure-still-struggles-with-chinese-ict-vendors/>>, accessed 18 June 2026.

102. Authors' interview with cyber security consultant, online, 20 May 2025.

them from most core 5G networks.¹⁰³ Defence ICT networks prohibit Chinese equipment entirely. These successes show that Spain can apply robust high-risk vendor controls.

Telefónica demonstrates a successful example of the removal of Huawei from 5G core network functions in Spain.¹⁰⁴ Rather than implementing an abrupt ban, Telefónica progressively reduced Huawei's role in security-sensitive areas, shifting new core deployments and government-facing services to European suppliers such as Nokia and Ericsson. At the same time, it has retained some Huawei equipment in non-core or legacy segments where replacement costs are high and regulatory pressure is lower. This phased approach reflects Telefónica's effort to balance security and compliance with operational and commercial considerations, aligning with Spain's broader pattern of de facto exclusion without explicit designation of Huawei as a high-risk vendor.

Unlike 5G and telecoms, most Spanish public digital infrastructure sits outside the scope of origin-based risk management. In these sectors – education, healthcare, municipal administration, transport and mobility systems – it is likely that Huawei maintains a substantial installed base.¹⁰⁵ Interviewees identified three converging forces sustaining this outcome:

1. Spain's National Security Framework (ENS) certifies ICT products against technical security criteria but provides no mechanism to weigh a vendor's country of origin or its exposure to a foreign state – so equipment from a Chinese vendor can be certified and deployed in public systems on the same terms as any other, regardless of the geopolitical considerations that concern security institutions.
2. Spanish public procurement law requires contracts to be awarded on neutral, competitive grounds, principally cost and technical merit. Combined with Huawei's competitive pricing, this tends to favour it rather than exclude it.
3. While national security bodies such as the CCN assess China as a risk, that awareness is not widely shared among the regional and sectoral authorities that make many day-to-day procurement decisions, leaving a gap between strategic assessment and operational practice.¹⁰⁶

103. Strand Consult, 'The Market for 5G RAN in 2024: Share of Chinese and Non-Chinese Vendors in Europe (2024/2025)', <<https://strandconsult.dk/the-market-for-5g-ran-in-europe-share-of-chinese-and-non-chinese-vendors-in-31-european-countries/>>, accessed 2 September 2026. For the 2022 Spain figure, see Javier Torre de Silva, '5G Regulation and Law in Spain', CMS, 3 March 2025, <<https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/spain>>, accessed 9 September 2026. For the European aggregate and country trends, see Iain Morris, 'Huawei has Hardly Been Weakened in European 5G, Data Shows', *Light Reading*, 2 January 2025, <<https://www.lightreading.com/5g/huawei-has-hardly-been-weakened-in-european-5g-data-shows>>, accessed 2 September 2026.

104. Jesús Maturana, 'Huawei's Paradox in Spain: No to 5G, Yes to Wiretaps', *Euronews*, 13 July 2025, <<https://www.euronews.com/next/2025/07/13/huaweis-paradox-in-spain-no-to-5g-but-yes-to-wiretap-storage>>, accessed 18 June 2026.

105. Authors' interview with US technology vendor executive, online, 21 July 2025.

106. Authors' interview with cyber security consultant, online, 20 May 2025; authors' interview with technology vendor executive, online, 21 July 2025; authors' interview with academic, online, 11 August 2025.

The procurement of Huawei's OceanStor data storage¹⁰⁷ solution for judicial wiretap recordings exemplifies these structural issues. The agreement was primarily concerned with backend data-storage infrastructure rather than telecommunications equipment and thus fell outside the scope of ENS5G restrictions. Once the product passed CPSTIC evaluation and emerged as the lowest-cost bid, it was deemed acceptable under Spanish open procurement requirements. Officials argued that the associated security risk was manageable through technical and procedural controls.¹⁰⁸ However, the subsequent international reaction, particularly from US policymakers,¹⁰⁹ exposed the reputational and diplomatic consequences of Spain's approach. The issue only gained domestic political salience following this backlash, underscoring the government's underestimation of the geopolitical implications of technology procurement.¹¹⁰ It could be argued that the case confirmed that Spain's current regime governs for compliance rather than strategic assurance, constraining its ability to align procurement practice with allies' national security expectations.

Spain's national ministries and major financial institutions possess mature high-risk vendor management capabilities, while regional and local authorities struggle to operationalise supply-chain risk mapping, business criticality analysis or incident response planning for third- and fourth-party dependencies.¹¹¹ Interviewees highlighted uncertainty over who holds liability when a connection to a compromised vendor must be severed, impeding decision-making.¹¹² These gaps are compounded by the international footprint of major Spanish firms. Banks such as Santander and BBVA, and operators such as Telefónica, run extensive financial, 5G and digitalisation operations across Latin America, where security controls are often weaker and Chinese vendors face few of the restrictions applied in Europe. This extends Spanish corporate supply chains into higher-risk environments – Telefónica's continued use of Huawei in Brazil being one example¹¹³ – meaning that exposure managed out of the domestic market can re-emerge through overseas operations. Coordination among cyber security authorities remains limited. CCN focuses on certification and direct support to national bodies, while INCIBE, despite its wider responsibility, was described as reactive,¹¹⁴ with insufficient capacity to provide national scale coordination similar to the UK's National Cyber Security Centre (NCSC). This shortcoming may be mitigated by

107. Antoaneta Roussi, 'Spain Under Fire for Contracting Huawei to Store Judicial Wiretaps', *Politico*, July 2025, <<https://www.politico.eu/article/spain-huawei-contract-judicial-wiretaps/>>, accessed 18 June 2026.

108. *Ibid.*

109. Martin Matishak, 'Lawmakers Call on DNI to Review Intel Sharing with Spain over Huawei Revelations', *The Record*, 17 July 2025, <<https://therecord.media/lawmakers-call-on-dni-to-review-spain-intel-huawei>>, accessed 18 June 2026.

110. Authors' interview with academic, online, 11 August 2025.

111. *Ibid.*

112. Authors' interview with public sector cyber security consultant, online, 20 May 2025.

113. *Reuters*, 'Telefonica Ditches Huawei's 5G Gear in Spain and Germany; Keeps It in Brazil', 30 July 2025, <https://www.tradingview.com/news/reuters.com,2025:newsml_L8N3TR1ZR:0-telefonica-ditches-huawei-s-5g-gear-in-spain-and-germany-keeps-it-in-brazil/>, accessed 2 September 2026.

114. *Ibid.*

new provisions – as of October 2025 – to strengthen cyber security and inter-institutional coordination, including the creation of a new National Cybersecurity Centre attached to the Office of the Prime Minister.¹¹⁵

An additional structural factor shaping Spain's procurement posture beyond 5G and telecoms is the limited availability of politically 'neutral' alternatives to Chinese technology. Across enterprise IT and cloud services, the only global competitors to Huawei and other Chinese vendors are predominantly US firms. Participants acknowledged other European tech options, but their prices were considered uncompetitive.¹¹⁶ While US cloud vendors dominate the Spanish market, interviewees highlighted that anti-US sentiment and residual scepticism of US surveillance practices shape a desire for strategic autonomy and limit the appetite to exclude Chinese vendors from procurement.¹¹⁷ One participant even noted that some officials view US legal instruments such as the Patriot Act as creating equivalent sovereignty risks to China's National Intelligence Law, a narrative that is flawed when exploring the legislation, but politically convenient.¹¹⁸ Combined with the fact that European alternatives often lack the price competitiveness or technical depth required for large-scale deployments, this perception reinforces Spain's default position. While China poses a risk, US technology is not viewed as risk-free either, and Spain currently sees few viable options that fully reconcile cost, capability and strategic comfort.

Spain therefore implements some high-risk vendor controls effectively only in the narrow spaces where regulatory authority, political will and organisational maturity align. Elsewhere, decisions default to national economic considerations and budgetary constraints, producing reactive, rather than preventive, risk governance.

115. La Moncloa, 'Pedro Sánchez Announces the Creation of the National Cybersecurity Centre, Attached to the Presidency of the Government'.

116. Authors' interview with technology vendor executive, online, 21 July 2025.

117. *Ibid.*; authors' interview with think tank researcher, online, 28 July 2028.

118. Authors' interview with technology vendor executive, online, 21 July 2025.

The UK

Strategic Context

The UK's approach to high-risk ICT vendors is shaped by two key broader strategic considerations: China's importance in both the global and UK economy, and the UK's commitment to its security partnership with the US. The dilemma of balancing economic opportunity and national security risk – along with an increasing focus on national resilience and sovereignty – has forced successive UK governments to make high-profile, often contentious decisions about foreign-owned or foreign-influenced ICT vendors in strategic sectors. These competing priorities have resulted in legislative, regulatory and institutional tools for managing high-risk ICT vendors in the UK, but without the kind of proactive approach required to employ them at scale across critical sectors.

Parts of UK government and business have long framed engagement with China as an economic opportunity. China is the UK's fourth-largest trade partner and has been a source of a significant amount of foreign investment. Cumulative Chinese investments into the UK from 2000 to 2024 total €84.3 billion, more than for any other European country.¹¹⁹ Although the 2021 National Security and Investment Act gave the government the power to screen and block investments and acquisitions in strategic sectors,¹²⁰ investment and capital from Chinese companies is still sought after. The UK also has significant upstream dependencies on Chinese technology and manufacturing that is not reflected in trade and investment metrics. This is particularly true of technologies that will be crucial if the UK is to meet its net-zero commitments.

At the same time, the UK national security community has consistently highlighted the risks posed by foreign-controlled or foreign-influenced ICT vendors. The NCSC has assessed that 'China is investing huge sums ... in advanced technologies, which it almost certainly intends to export worldwide. Success will enable China to project its

119. Esther Goreichy, Grezgorz Stec and Abigaël Vasselier, 'Profiling European Countries' Resilience Towards China – 2025 Update', Merics, 29 October 2025, <<https://merics.org/en/report/profiling-european-countries-resilience-towards-china-2025-update>>, accessed 2 September 2026.

120. Cabinet Office, 'National Security and Investment Act 2021', 22 August 2026, <<https://www.gov.uk/government/collections/national-security-and-investment-act>>, accessed 2 September 2026.

economic, military and political power globally'.¹²¹ Perceptions of Chinese ICT vendors have also become increasingly politicised within Parliament, particularly among Conservative parliamentarians who have been sanctioned by China for criticising China's human rights record.¹²²

Concerns about foreign influence and espionage risks from ICT vendors are also shaped by the UK's very close intelligence and defence partnership with the US. This relationship has meant the UK government is susceptible to pressure from US administrations that have actively sought to influence its policies towards strategic technologies such as 5G.¹²³

This close security partnership with the US also means that the UK is generally less concerned about digital sovereignty than many other European countries, such as Germany and Spain. While government officials acknowledge the concentration risks posed by cloud hyperscalers such as Microsoft and AWS, officials and politicians largely do not share the current scepticism towards US tech vendors that is commonplace in a number of EU members.¹²⁴ As such, the UK debate about high-risk ICT vendors typically focuses on adversaries like Russia and China.

As the UK's experience with Huawei and its telecommunications infrastructure shows, balancing these competing interests has not been straightforward. In 2005, British Telecom gave Huawei its first significant European contract.¹²⁵ This foothold allowed the company to establish a strong position in 3G and 4G networks. As concerns grew about the potential role of Huawei in the UK's 5G networks, the government adopted a pragmatic risk management approach, including testing and assurance of Huawei's products.¹²⁶ However, the UK's attempt to go its own way on Huawei was eventually abandoned after sustained pressure from President Donald Trump's first administration and US sanctions against Huawei.¹²⁷

121. Intelligence and Security Committee of Parliament, *China*, HC 1605 (London: The Stationery Office, 2023), p. 123.

122. Patrick Wintour, 'China Imposes Sanctions on UK MPs, Lawyers and Academics in Xinjiang Row', *The Guardian*, 26 March 2021. Since the time of writing, China has lifted these sanctions. See Pippa Crerar, 'China Has Lifted Sanctions from Six Serving British MPs and Peers, Starmer Says', *The Guardian*, 30 January 2026.

123. Toby Helm, 'Pressure from Trump Led to 5G Ban, Britain Tells Huawei', *The Guardian*, 18 July 2020.

124. Authors' interview with government officials, online, 25 April 2025; authors' interview with government official, online, 1 May 2025.

125. Juliette Garside, 'Huawei's Relationship with BT Under Investigation by MPs', *The Guardian*, 10 October 2012.

126. Ian Levy, 'Security, Complexity and Huawei; Protecting the UK's Telecoms Networks', National Cyber Security Centre, 22 February 2019, <<https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks>>, accessed 2 September 2026.

127. Conrad Prince and James Sullivan, 'The UK's New Way on Huawei', *RUSI Commentary*, 14 July 2020, <<https://www.rusi.org/explore-our-research/publications/commentary/uks-new-way-huawei>>, accessed 2 September 2026; Radu and Amon, 'The Governance of 5G Infrastructure'.

Policy, Legislation and Regulation

Since its decision to replace Huawei in its 5G networks, the UK has established a more formal approach to managing high-risk vendors, underpinned by legislation, regulation and dedicated government units. This has created a robust policy framework for managing risks in the telecoms sector and the public sector, albeit with potential gaps in other areas of CNI. To implement these mechanisms, the UK government has also increased state capacity.

The Telecommunications Security Act (TSA) 2021 and associated regulation is the primary legal instrument for managing high-risk vendors in the UK's telecoms infrastructure. The Act, which came into force in October 2022, imposes security obligations on telecoms operators and gives government powers to intervene against vendors.¹²⁸ Under the TSA, the Secretary of State for the Department for Digital, Culture, Media and Sport (DCMS) issues Designation Notices for vendors whose presence in UK telecoms networks poses national security risks, and Designated Vendor Directions to telecoms providers. The latter place controls on the use of a designated vendor's goods and services. Although the TSA does not define a high-risk vendor, it does set out several criteria that will inform the government's assessments, such as national security laws in the jurisdiction in which the vendor is based, the relationship between the vendor and the vendor's domestic state apparatus, and the strategic position of the vendor in UK telecoms networks. The Electronic Communications (Security Measures) Regulations 2022 also set detailed, mandatory security measures for telecoms operators.¹²⁹ Failure to comply can lead to fines from Ofcom, the UK's telecoms regulator.

The UK has also developed a more robust, interventionist framework to manage high-risk vendors in the public sector. The Procurement Act 2023, which came into force in February 2025, introduced a specific exclusion ground for national security and expanded powers to terminate contracts and exclude suppliers that pose risks.¹³⁰ A national security exclusion or termination requires agreement from a Minister of the Crown (a member of the government appointed on the advice of the prime minister to lead a department or hold a senior executive office). This gives the government a legal route to bar or remove high-risk ICT vendors from individual procurements or from whole categories of sensitive contracts.

128. HM Government, 'Telecommunications (Security) Act 2021', <<https://www.legislation.gov.uk/ukpga/2021/31/contents>>, accessed 2 September 2026.

129. HM Government, 'The Electronic Communications (Security Measures) Regulations 2022', <<https://www.legislation.gov.uk/uksi/2022/933/contents>>, accessed 2 September 2026.

130. Cabinet Office, 'Guidance: Exclusions Annex 2: National Security Grounds', updated 24 June 2026, <<https://www.gov.uk/government/publications/procurement-act-2023-guidance-documents-procure-phase/guidance-exclusions-annex-2-national-security-grounds-html>>, accessed 2 September 2026.

To operationalise these powers, the UK government has also created a dedicated National Security Unit for Procurement within the Cabinet Office¹³¹ which receives referrals from public sector authorities and assesses suppliers that may pose a national security risk. It also monitors the market and can ‘self-refer’ suppliers for investigation.¹³² The risk assessments carried out by the unit use a three-pillar framework:

- Jurisdictional hazard and control
- Technical vulnerability
- Customer sensitivity.¹³³

Interviewees highlighted that, although in theory the risk arises from a combination of all three, in practice jurisdictional hazard and control is the most important determinant.¹³⁴ At the same time, interviewees stressed that this does not mean there is a blanket ban on Chinese vendors, but instead that the government takes a flexible approach, accounting for varying sensitivity across the public sector.¹³⁵ A chief information security officer (CISO) in a central government department emphasised that the Procurement Act is a ‘much better framework’ than prior ones and there is now ‘more direction from Cabinet Office’.¹³⁶

Besides telecoms and the public sector, the UK’s policy for managing high-risk vendors is more limited. The Network and Information Systems Regulations (NIS) 2018 is currently the main regime for managing the cyber security and resilience of the UK’s privately operated CNI.¹³⁷ However, neither the NIS nor the government’s Cyber Assessment Framework (a tool that helps CNI operators comply with NIS) has any dedicated requirements for managing suppliers associated with national security risk.¹³⁸

The current set-up therefore risks creating a two-tier approach with a robust assessment and enforcement mechanism for the public sector and telecoms, but not for other parts of CNI. This raises broader questions about the coherence of the UK’s strategy for managing foreign-owned, foreign-controlled, or foreign-influenced ICT vendors in key areas of CNI and the UK economy. Research interviews consistently highlighted that the UK government does not have a cross-government definition of a

131. Cabinet Office, ‘The National Security Unit for Procurement’, updated 24 June 2026, <<https://www.gov.uk/guidance/the-national-security-unit-for-procurement>>, accessed 2 September 2026.

132. Authors’ interview with government official, online, 1 May 2025; authors’ interview with government official, online, 25 April 2025.

133. Cabinet Office, ‘Guidance: Exclusions Annex 2’.

134. Authors’ interview with government official, online, 1 May 2025; authors’ interview with government official, online, 25 April 2025.

135. Authors’ interview with government official, online, 1 May 2025; authors’ interview with government official, online, 9 April 2025.

136. Authors’ interview with UK government chief information security officer (CISO), online, 27 June 2026.

137. Department for Digital, Culture, Media and Sport, ‘The NIS Regulations 2018’, <<https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018>>, accessed 2 September 2026.

138. National Cyber Security Centre, ‘Cyber Assessment Framework’, <<https://www.ncsc.gov.uk/collection/cyber-assessment-framework>>, accessed 2 September 2026.

high-risk vendor nor a national framework for reviewing risks in a broader range of sectors and supply chains.

However, this may change in the future. The forthcoming Cyber Security and Resilience Bill, the UK's first dedicated legislation for managing cyber risk in CNI, will give the secretary of state for DCMS the power to issue binding directions to regulated entities in response to national security threats.¹³⁹ Although the original draft of the proposed legislation did not include a dedicated framework for excluding specific suppliers to CNI operators based on risks associated with foreign ownership, control or influence, a recent proposed amendment to the Bill seeks to give the government powers to ban technology vendors on national security grounds.¹⁴⁰ The amendment would give the government the ability to issue 'vendor-related directions', which would restrict affected CNI operators from using a particular supplier's products or services. Unlike designations under the Telecoms Act, however, the government would not have to publicly designate a vendor as a national security risk.¹⁴¹ However, at the time of writing, it is uncertain if the amendment will be included in the final draft of the Bill.

Policy Implementation Approach, Gaps and Challenges

There are two main cases in which the UK government has intervened against high-risk ICT vendors. The most high-profile is the removal of Huawei from the UK's 5G telecoms network. Following the decision to remove Huawei in July 2020, the UK government created a phased timeline for telecoms operators to remove the vendor's equipment from their networks. In October 2022, the government issued a designation notice to Huawei under the TSA, making the restrictions legally binding.¹⁴² The deadline for removing all Huawei equipment from 5G networks is 31 December 2027.¹⁴³

The other primary case study is the presence of Chinese surveillance equipment on UK government sites. In November 2022, following pressure from several MPs, the Cabinet Office instructed central government departments to remove visual

139. Department for Science, Innovation and Technology, 'Policy Paper: Cyber Security and Resilience Policy Statement', April 2025, <<https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement/cyber-security-and-resilience-bill-policy-statement>>, accessed 2 September 2026.

140. 'Cyber Security and Resilience Bill: Running List of All Amendments in Grand Committee Tabled Up to and Including 24 August 2026', p. 25, <<https://bills.parliament.uk/publications/67470/documents/8691>>, accessed 2 September 2026.

141. Alexander Martin, 'UK Government Seeks Powers to Secretly Block Risky Tech Suppliers', *The Record*, 25 August 2026, <<https://therecord.media/uk-technology-national-security>>, accessed 2 September 2026.

142. Department for Digital, Culture, Media and Sport, 'Huawei Legal Notices Issued', 13 October 2022, <<https://www.gov.uk/government/news/huawei-legal-notices-issued>>, accessed 2 September 2026.

143. HM Government, 'Huawei to be Removed from UK 5G Networks by 2027', 14 July 2020, <<https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027>>, accessed 2 September 2026.

surveillance systems sold by companies subject to the National Intelligence Law of China.¹⁴⁴ Although the directive applied primarily to ‘sensitive sites’ such as government buildings or military bases, other public sector authorities were also advised to make ‘risk-based’ decisions about the use of such equipment.¹⁴⁵ In April 2024, the UK government revealed that 50% of sensitive sites that deployed such surveillance systems had removed them,¹⁴⁶ and interviewees indicated that the process had essentially been completed by summer 2025.¹⁴⁷ While some government cyber security officials questioned the necessity or proportionality of this decision,¹⁴⁸ it highlights the ability of the UK central government to assess and remove high-risk ICT vendors when it is politically, economically and technically viable to do so.

In other areas of the public sector’s ICT supply chains, there is less certainty among policymakers and practitioners about potential dependencies on high-risk ICT vendors. On the one hand, there is no evidence of large-scale public sector IT and cloud contracts, as in some European countries. UK government CISOs, procurement officials and cyber security consultants that specialise in the public sector all emphasised that Huawei equipment plays an insignificant role in government IT estates and that Chinese enterprise IT vendors do not bid for UK government contracts.¹⁴⁹ One former UK government CISO suggested that Huawei has ‘decimated its UK presence ... the market for them is absolutely dead in the public sector’.¹⁵⁰ This assessment aligns with Huawei UK’s financial reporting (see Figure 2), which highlights a drop in revenue from €1479.45 million in 2019 to €226.12 million in 2024.¹⁵¹

On the other hand, the research for this paper suggests a significant visibility gap that makes it difficult for government to assess the extent of its dependence on high-risk ICT vendors. The public sector lacks centralised risk registers for vendors,¹⁵² while asset management is, according to one senior government cyber security official, ‘poor across government’.¹⁵³ As a consequence, if a vendor is designated as high-risk in the

144. Oliver Dowden, ‘Security Update on Surveillance Equipment: Statement Made on 24 November 2022’, 24 November 2022, <<https://questions-statements.parliament.uk/written-statements/detail/2022-11-24/hcws386>>, accessed 2 September 2026.

145. Authors’ interview with government official, online, 1 May 2025.

146. Sarah Young, ‘Chinese-Made Surveillance Kit to be Removed from Sensitive Sites by 2025, Says UK’, *Reuters*, 29 April 2024.

147. *Ibid.*; authors’ interview with government officials, online, 25 April 2025.

148. Authors’ interview with government CISO, online, 27 June 2025; authors’ interview with government official, online, 1 May 2025.

149. Authors’ interview with government IT manager, online, 4 June 2025; authors’ interview with government CISO, online, 27 June 2025; authors’ interview with public sector cyber security consultant, online, 15 May 2025; authors’ interview with government officials, online, 25 April 2025.

150. Authors’ interview with public sector cyber security consultant, online, 25 February 2025.

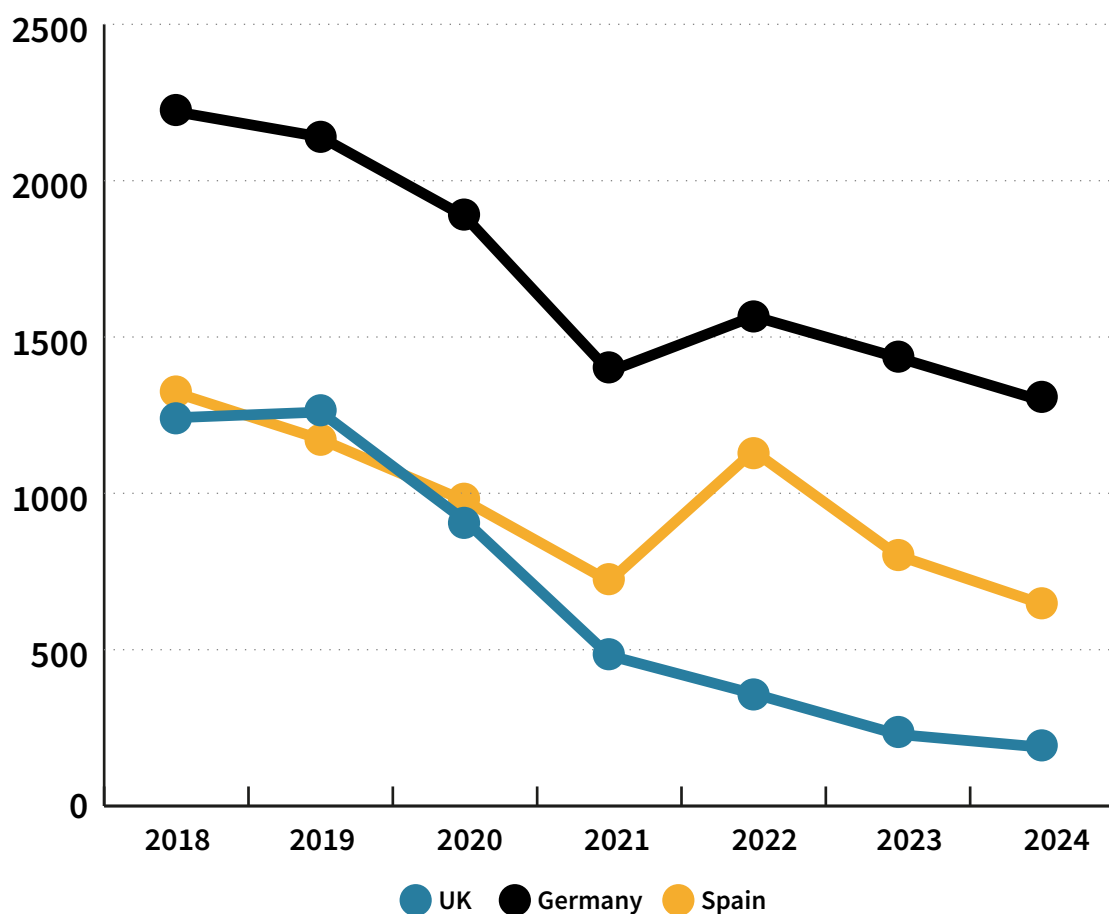
151. Paul Kunert, ‘Huawei Counts Cost of Western Bans As UK Business Withers’, *The Register*, 2 September 2025, <<https://www.theregister.com/on-prem/2025/09/02/huawei-counts-cost-of-western-bans-as-uk-business-withers/304768>>, accessed 2 September 2026.

152. National Audit Office, ‘Government Cyber Resilience’, 29 January 2025, <<https://www.nao.org.uk/reports/government-cyber-resilience/>>, accessed 1 June 2026.

153. Authors’ interview with senior government cyber security official, online, 9 April 2025.

future, the government cannot reliably map pre-existing exposure and is reliant on ad hoc audits to collect and assess relevant data points. The visibility gap also applies to supply chain management. For most public sector organisations, it is challenging to assess risk down a supply chain, as suppliers may use high-risk subcontractors or manufacturers. A recurring theme in the interviews with UK government officials and practitioners was that even ‘trusted’ Western vendors rely on manufacturing supply chains based in China.¹⁵⁴

Figure 2: Huawei Annual Revenue by Country (in € million)



Source: Annual company filings from Huawei Deutschland GMB, Huawei Espana and Huawei Technologies (UK) Ltd.

Note: Huawei Technologies (UK) Ltd statements have been converted to euros.

154. Authors' interview with intelligence official, online, 3 April 2025; authors' interview with government CISO, online, 27 June 2025.

As noted previously, the UK's approach to managing high-risk vendors outside telecoms and the public sector is less mature. At present, there are few examples of government interventions to assess and remove high-risk ICT vendors from the supply chains of other CNI sectors. CNI operators cannot reference government assessment frameworks or assurance regimes, which are specifically designed to address cyber risks posed by ICT vendors linked to foreign ownership, control or influence. One relatively recent exception is the energy sector, which is reportedly the subject of a government review to assess risks posed by Chinese suppliers.¹⁵⁵ In March 2026, the government blocked a Chinese wind turbine manufacturer from building a factory in Scotland on national security grounds.¹⁵⁶ The factory will now reportedly be built in Spain.¹⁵⁷ However, the absence of clear policy or enforcement mechanisms for managing vendors in the energy sector, combined with the complexity of energy supply chains and China's growing dominance within them, means that excluding Chinese vendors in this sector is likely to be more challenging than for the telecoms sector.

In summary, the UK's approach to high-risk ICT vendors remains a work in progress. Successive governments have developed legal, regulatory and institutional tools for managing foreign-owned, foreign-controlled or foreign-influenced vendors in the country's telecoms infrastructure and public sector, but without the kind of coherent, systematic framework required for the rest of CNI and the UK economy. It is likely that this lack of coherence reflects the broader limitations of the government's China strategy and the hesitance to answer fundamental questions about the acceptability of concentrated dependence on any external strategic supplier for the UK's CNI.

155. Jim Pickard et al., 'MI5 Investigates Use of Chinese Green Technology in UK', *Financial Times*, 15 February 2025.

156. The government did not reveal which legal instrument it used to block the project. See Paris Gourtsyannis and Steven McKenzie, 'Why was a £1.5 Billion Chinese Plan to Invest in a Highland Yard Blocked?', *BBC News*, 26 March 2026.

157. Susanna Twidale, 'China's Ming Yang Plans Europe Factory After UK Wind Turbine Snub', *Reuters*, 14 May 2026.

Cross-Cutting Themes and Implications for EU and UK Policy

The three country case studies point to a central tension in European approaches to high-risk technology vendors. Germany, Spain and the UK all recognise, to varying degrees, that some foreign ICT vendors create risks that cannot be managed through ordinary cyber security controls alone. Yet they differ significantly in how they define those risks, which sectors they prioritise and how far government intervene to manage the risks.

The analysis of these three countries raises several specific challenges that have implications for EU and UK policy on high-risk ICT vendors. A full breakdown of the key policy measures of the three countries to managing high-risk vendors is shown in Annex 3.

Absence of a Common Definition of a High-Risk Technology Vendor

There is no consensus on what constitutes a high-risk vendor or a standardised assessment framework across Germany, Spain and the UK. Instead, each country has developed partial, sector-specific and often politically sensitive ways of describing the same underlying set of risks. The UK has developed the broadest framework and is more willing than Spain and Germany to publicly designate Chinese vendors as high risk, but even it lacks a single cross-government definition or assessment framework that can be used beyond telecoms and public procurement.

Definitional ambiguity has some advantages. It allows each government to avoid crude bans based entirely on country of origin and preserve space for proportionate, case-by-case decision-making. It also allows national authorities to account for differences

between sectors, technologies and deployment models. A cloud platform, a 5G RAN, a solar panel inverter, a data-storage system and a surveillance camera do not create identical risks. However, this ambiguity also creates inconsistency for implementation. Where governments have not clearly specified how geopolitical, technical and economic risks should be weighed, decisions are often pushed down to regulators, procurement officials, operators or local authorities that are ill-placed to account for strategic risk.

The EU's proposed trusted ICT supply chain framework is therefore an important step towards harmonising definitions and criteria. At the same time, it should retain the sectoral flexibility that some governments have allowed for at a national level. Telecoms should remain the reference model, but the framework should not assume that other technology supply chains have the same set of risks, dependencies and exposures. A credible framework will therefore specify common criteria but allow asset taxonomies, mitigations and timelines to vary by sector.

Persistence of Economic Considerations for National Policy on High-Risk Vendors

To varying degrees, all three case studies also highlight the ongoing salience of economic considerations in how national governments make policy towards high-risk ICT vendors and how they justify and implement action. Even when geopolitical and national security risks are acknowledged, many European policymakers have been reluctant to take steps that might impose high costs or provoke economic retaliation.

Fears about the potential high cost of ripping and replacing Chinese ICT equipment, particularly for 5G networks, have been amplified by highly publicised (and disputed) cost estimates made by interest and lobbying groups. In the wake of the proposed amendments to the EU CSA, for instance, the Chinese Chamber of Commerce to the EU commissioned a study by KPMG that claimed the cost of implementing the Act would be €367.8 billion over the next five years.¹⁵⁸ In July 2026, the GSMA, a global trade body representing the telecom industry, assessed that implementing the Act for the telecoms sector would cost €30–40 billion.¹⁵⁹ This estimate is significantly higher than the EU's own estimate of €10–13 billion.¹⁶⁰ In reality, these estimates are not that far apart as the GSMA's assessments include costs that would be implied without the new regulations

158. Euractiv, '€367.8 Billion Question: Guardrails or Blockade?', 6 May 2026, <<https://www.euractiv.com/opinion/e367-8-billion-question-guardrails-or-blockade/>>, accessed 2 September 2026.

159. GSMA Intelligence, 'The Cost of Removing Designated Third Country Vendors from EU Telecoms Networks', July 2026, p. 3, <<https://www.gsmainelligence.com/research/the-cost-of-removing-designated-third-country-vendors-from-eu-telecoms-networks>>, accessed 16 August 2026.

160. European Commission, 'Proposal for a Regulation for the EU Cybersecurity Act', January 2026, <<https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act>>, accessed 5 August 2026.

(gross costs) and the EU's assessments do not (net costs). Even so, the lack of clear consensus on the cost of ripping and replacing creates ambiguity that undermines collective action.

Economic considerations are clearly, therefore, a significant reason why the EU's previous voluntary approach to high-risk ICT vendors has resulted in limited progress. Where member states have faced different economic incentives and perceptions of risk, implementation has diverged. The EU-level binding framework proposed in the amendments to the CSA will, on paper, help to circumvent those divergences and reduce the exposure of individual member states to potential Chinese economic coercion by shifting some politically difficult decisions from the national to the European level.

However, a common EU framework driven through the Commission will only succeed if it is seen as legitimate and implementable. Member states are likely to resist any mechanism that appears to override national security considerations or impose large economic costs without adequate consultation. The EU will therefore need to combine stronger central powers with clear criteria, evidence-based assessments, due process, transition periods and mechanisms for review. A common EU approach is also likely to be more politically and economically viable if it gets ahead of future procurement decisions, rather than primarily focusing on replacement of existing equipment.

Concerns about economic costs also highlight the need for a credible industrial strategy in Europe capable of developing viable alternatives. The telecoms supply chain remains unusual in having multiple European alternatives to Chinese vendors (Nokia and Ericsson). However, this is likely to be much more challenging in other technology supply chains, such as renewable energy, where Chinese suppliers are monopolising market share.

Visibility Gap and the Importance of State Capacity

The experience with high-risk ICT vendors in Germany, Spain and the UK also highlights challenges with understanding and assessing supply chain risk in CNI. Assessing exposure to potential high-risk vendors requires an understanding of which systems are critical, what dependencies exist at first-, second- and third-tier supplier levels, and a detailed understanding of the component parts of hardware and software.

While standardisation of risk assessments through tools like the EU's ICT Supply Chain Security Framework will help with practical implementation of guidance on high-risk

vendors,¹⁶¹ equally important is the need to develop state capacity. The creation of the UK's National Security Unit for Procurement highlights the value of developing institutions dedicated to assessing potential high-risk vendors, advising contracting authorities and monitoring implementation. While some of this work can be carried out at the supranational level for EU member states through the European Union Agency for Cybersecurity, this is not a replacement for national capabilities.

The Role of US Technology Companies in Debates on High-Risk Vendors

A theme that emerges from the Germany and Spain case studies is the growing scepticism in some European countries towards US ICT vendors. This perspective recognises that the heavy concentration of US cloud hyperscalers creates a different kind of strategic risk to that posed by Chinese vendors. The EU has largely treated the debates on achieving more strategic autonomy from the US and designating and excluding Chinese vendors as separate issues, whereas at the national level, some countries have connected the two. While characterised by different actual risks, having parallel debates about Chinese and US vendors risks sending mixed messages to procurement authorities and CNI operators about which vendors are 'high risk' in terms of the likelihood of foreign control undermining European security interests.

Cross-European policy should therefore avoid making a false equivalence between the US and China and instead focus on ensuring that it creates a framework capable of distinguishing between the differing geopolitical and security risks posed by Chinese and US ICT vendors.

The Impact of Designations and Exclusions of High-Risk Vendors on Europe's Cyber Security

A recurring theme in interviews was frustration among cyber security practitioners that current definitions of high-risk ICT vendors focus too much on country of origin at the expense of other types of risk. While concerns about foreign control, ownership and influence of ICT vendors are important, designating and excluding these vendors does not meaningfully mitigate the risk posed by poorly engineered hardware and software, organisational cyber risk management challenges and legacy IT debt. In short, China does not need to exploit the accesses potentially provided by Chinese ICT

161. European Commission, 'Toolbox to Improve ICT Supply Chain Security', 13 February 2026, <<https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security>>, accessed 5 August 2026.

vendors to conduct successful cyber operations. A recent example is that of Salt Typhoon, a Chinese cyber campaign that penetrated huge swathes of Western telecommunications by compromising legacy routers manufactured by US vendors and unpatched edge network devices.¹⁶² One interviewee summed up the current status quo: ‘huge swathes of the public sector are underpinned by vendors that I would class as high risk one way or another.’¹⁶³

At present, this perspective is widespread in practitioner communities but is not reflected in debates or policy about high-risk vendors. Treating the risks posed by Chinese ICT vendors and the bolstering of European cyber security as the same problem – particularly by tacking policy on high-risk vendors onto broader cyber security legislation like the CSA – also risks muddying the waters. This means that messaging about high-risk designations and exclusions needs to emphasise that they are not a substitute for broader cyber security and resilience policies.

Addressing Gaps in the UK’s Approach to High-Risk ICT Vendors

While this chapter has primarily focused on implications for a cross-European approach to high-risk ICT vendors, it is necessary to consider the UK’s position outside EU legislation.

For UK policy, the main conclusion is that there remains a significant gap in its approach to high-risk vendors outside telecoms and the public sector. The mechanisms it has developed do not yet amount to a coherent cross-sector framework. The risk is that the UK develops a two-tier model: high levels of scrutiny in central government and telecoms, but weaker visibility and intervention powers in other CNI sectors.

The UK should not adopt the EU model wholesale but should build a national approach that is aligned with and guided by the CSA’s proposed amendments. Greater coherence between the UK and EU approaches would also reduce the risk that high-risk suppliers excluded from one European market retain significant access through another.

162. Unpatched edge network devices are hardware and software devices at the ‘edges’ of networks – such as routers, firewalls and VPN gateways – which no longer receive vendor security updates or lack critical security patches. This makes them prime targets for malicious actors. See Cybersecurity and Infrastructure Security Agency, ‘CISA and Partners Release Joint Advisory on Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage Systems’, 27 August 2025, <<https://www.cisa.gov/news-events/alerts/2025/08/27/cisa-and-partners-release-joint-advisory-countering-chinese-state-sponsored-actors-compromise>>, accessed 16 July 2026.

163. Authors’ interview with UK public sector cyber security consultant, online, 15 August 2025.

The starting point should be the Cyber Security and Resilience Bill,¹⁶⁴ which is currently making its way through Parliament, or its secondary legislation. This should provide a statutory process for assessing high-risk vendors across CNI, using criteria similar to those developed under the national security grounds of the Procurement Act 2023. At the time of writing, the UK has proposed an amendment to the Bill that would enable the government to intervene where the use of a supplier's goods or services creates a national security risk, including by restricting further procurement or requiring existing technology to be removed, disabled or modified.

If the proposed amendment is included in the Bill, the priority should be to use the Bill's secondary legislation, guidance and implementation arrangements to establish a consistent cross-government process for assessing vendor risk. This should draw on the three criteria already used under the national security provisions of the Procurement Act 2023,¹⁶⁵ and should provide a common basis for assessments across CNI sectors. The government should also consider whether it would be more suitable to publicly designate specific vendors (as it already does under the Telecoms Act) given that this would align more closely with the EU's proposed approach in the Cybersecurity Act.

The NCSC and the DCMS should also adapt the Cyber Assessment Framework to develop dedicated guidance for assessing risks related to foreign control or influence. The government could also explore the development of broader, non-statutory guidance for organisations not covered by the Cyber Security and Resilience Bill. Australia, for example, has recently released a similar form of guidance.¹⁶⁶

164. HM Government, 'Cyber Security and Resilience (Network and Information Systems) Bill', <<https://bills.parliament.uk/bills/4035>>, accessed 8 September 2026.

165. Cabinet Office, 'Guidance: Exclusions Annex 2'.

166. Department of Home Affairs, 'Foreign Ownership, Control or Influence: Risk Assessment Guidance', 2025, <<https://www.homeaffairs.gov.au/nat-security/files/foci-risk-assessment-guidance-with-appendices.pdf>>, accessed 16 July 2026.

Conclusion

The debate about high-risk ICT vendors in Europe is ultimately about how open democracies manage strategic risk in an era of geopolitical competition without sacrificing the economic openness and rule-of-law principles that define them.

Germany, Spain and the UK have each found different answers to that question, shaped by their histories, economic interests and institutional capacities. However, none has yet found a fully satisfactory solution. The CSA's proposed amendments represent the most ambitious attempt yet to forge a common European answer, but as this paper has shown, the gap between legislative ambition and consistent implementation has been the defining failure of European policy in this area. Closing that gap will require not only stronger laws but also deeper institutional capacity, greater economic courage and a willingness to treat technology procurement as an instrument of strategic policy rather than a compliance exercise.

The decisions European governments make now about which vendors they trust – and which they do not – will shape the security and resilience of their CNI for the future.

About the Authors

Jamie MacColl is a Senior Research Fellow in RUSI's Cyber and Tech research team. He leads the UK Cyber Effects Network, RUSI's partnership with the National Cyber Force. His current research focuses on ransomware and other financially motivated cybercrimes, and the UK National Cyber Strategy. He is also currently a Senior Research Associate at Virtual Routes, a European think tank, and a member of the Technical Committee for the Cyber Monitoring Centre. Jamie holds an MPhil in International Relations and Politics from the University of Cambridge and BA in War Studies from King's College London.

Pia Hüsch is a Research Fellow in RUSI's Cyber and Tech research team. Her research focuses on the impact, societal risks and lawfulness of cyber operations and the geopolitical and national security implications of disruptive technologies, such as AI. She currently conducts research on the governance and regulation of cyber security issues, offensive cyber operations, and the geopolitical and national security implications of disruptive technologies, including AI. Pia has an LLM in International Law Security (with distinction) from the University of Glasgow and an LLB in European Law from Maastricht University.

Natasha Buckley is an Associate Fellow with RUSI's Cyber and Tech team. She is a Lecturer in Cyber Security at Cranfield University and a recognised researcher in emerging technologies, national security and research security policy. Her interdisciplinary expertise, spanning computer science, human geography and international relations, informs her strategic approach to her research area.

Sophie Williams-Dunning is a Research Analyst in RUSI's Cyber and Tech team. Her research interests include the evolution of hostile state threats in cyberspace and through cyber means, information operations, as well as UK cyber strategy and resilience. Sophie has an MA in Intelligence and International Security from the War Studies Department at King's College London, where she studied foreign policy with a focus on Russia, national cyber strategies, intelligence and open source investigation. Sophie also has a first-class BA in History and French from the University of Cambridge.

Annex 1

Table 2: Chinese ICT Vendors' Share of 5G RAN in Germany, Spain and the UK

	2022	2024	2028 (est.)
Germany	59%	59%	59%
Spain	38%	32%	24%
UK	41%	20%	0%

Source: Strand Consult, 'The Market for 5G RAN in 2024: Share of Chinese and Non-Chinese Vendors in Europe', 10 January 2025, <<https://strandconsult.dk/get-your-free-copy-of-strand-consults-new-study-the-market-for-5g-ran-in-2024-share-of-chinese-and-non-chinese-vendors-in-europe/>>, accessed 2 September 2026.

Annex 2

Table 3: Huawei Annual Revenue by Country (in € million)

	2018	2019	2020	2021	2022	2023	2024
Germany	2216	2143	1885.2	1390.1	1566.4	1434.9	1296.9
Spain	1321	1173.5	976.4	719.66	1135.12	801.24	646.88
UK	1393.39	1479.45	913.3	568.67	416.5	265.35	226.12

Source: Annual company filings from Huawei Deutschland GMB, Huawei España and Huawei Technologies (UK) Ltd.

Note: Huawei Technologies (UK) Ltd statements have been converted to euros.

Annex 3

Table 4: Comparison of Different Policy Measures Used by Germany, Spain and the UK to Manage Risks Associated With High-Risk ICT Vendors

	Germany	Spain	UK
Cyber Security and Resilience	Measure	Measure	Measure
	IT Security Act 2.0 (IT-Sicherheitsgesetz 2.0), 2021 <i>Legislation and regulatory powers</i>	Royal Decree-Law 12/2018 (Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información) and Royal Decree 43/2021 (Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018) (NIS framework) <i>Legislation and regulatory powers</i>	NIS Regulations 2018 <i>Regulation</i>
	Effect	Effect	Effect
	Amended the then-BSI Act and introduced section 9b. Operators planning the first use of a critical component had to notify the Federal Ministry of the Interior and submit a manufacturer guarantee declaration. The ministry could prohibit its use where public order or security was likely to be impaired, taking account of manufacturer trustworthiness and possible foreign state influence. This created an explicit non-technical vendor-trust control, but it was component- and case-specific rather than a public vendor ban. The Act has been superseded by the NIS-2 Implementation Act (see below).	Transposes the first NIS Directive and sets security, governance and incident-notification obligations for covered entities. The implementing regulation points to risk management, supplier controls and relevant security standards. It does not establish a general high-risk-vendor definition nor a power to designate technology suppliers across sectors.	Impose security and incident-reporting duties on operators of essential services . The regulations do not include any specific powers for screening, designating and removing high-risk ICT vendors from supply chains.

Cyber Security and Resilience (cont...)	Germany	Spain	UK
	Measure	Measure	Measure
	NIS-2 Implementation Act, 2025 <i>Legislation and regulatory powers</i>	Draft Law on Cybersecurity Coordination and Governance (Ley de Coordinación y Gobernanza de la Ciberseguridad) (NIS2 transposition) <i>Draft legislation</i>	Cyber Security and Resilience Bill <i>Draft legislation</i>
	Effect	Effect	Effect
	Replaced the BSI Act with a new version and built on the mechanisms introduced under the IT Security Act 2.0. Section 30 requires proportionate cyber-risk management, expressly including supply-chain security and security in the acquisition, development and maintenance of network and information systems. Section 41 allows the Federal Ministry of the Interior to prohibit a defined critical component, or order its removal. The assessment can consider foreign-state control, coercive third-country laws, hostile activity and manufacturer trustworthiness.	Would broaden the regulated population, strengthen risk-management and supply-chain duties, and create a more integrated national governance structure, including a National Cybersecurity Centre. It should not be treated as law until enacted. The public draft does not replace the separate, sector-specific 5G high-risk-vendor designation mechanism.	Will update the NIS regulations and give the government additional powers. It will give the Secretary of State for DSIT the power to issue binding 'directions' to regulated entities in response to urgent national security threats. At the time of writing, the government has proposed an amendment that would allow it to force CNI operators to stop using the products and services of high-risk ICT vendors.
	Measure	Measure	Measure
	BSI product-warning power (current section 13 Federal Office for Information Security Act, BSIG); (predecessor section 7)	Catalogue of Information and Communication Technology Security Products (CPSTIC) <i>Technical and product assurance</i>	Cyber Assessment Framework <i>Assessment and regulatory-assurance framework</i>
	Effect	Effect	Effect
	The BSI may publish warnings about security risks in information-technology products and recommend protective action or replacement. Its March 2022 Kaspersky warning is Germany's clearest public non-telecom example. A warning can strongly affect procurement and continued use, but it is not the same as a legally binding vendor prohibition.	Lists products and services evaluated for use under ENS or approved for classified-information environments. Its procurement effect depends on the ENS system category and the product's security role. It is not a universal allowlist for every public sector technology purchase, and inclusion is based on technical assurance rather than an across-the-board test of country of origin or foreign state influence.	Designed to help operators of essential services assess their cyber risk and meet legal and regulatory requirements. Tells organisations they must take account of 'all risks', but does not specifically mention supply chain risks associated with vendors linked to national security or country of origin risks.

	Germany	Spain	UK
Telecoms	Measure	Measure	Measure
	Public law contracts on critical 5G components, July 2024	Royal Decree-Law 7/2022 on requirements to guarantee the security of fifth-generation electronic communications networks and services <i>Legislation</i>	Telecommunications Security Act (TSA) 2021 <i>Legislation and regulatory powers</i>
	Effect	Effect	Effect
	Agreement between the German government and telecoms operators to remove Huawei and ZTE 'critical components' from 5G networks by the end of 2026 and replace those vendors' critical management systems in access and transport networks by the end of 2029. The measure is targeted at defined critical functions. It does not amount to an immediate blanket ban on all Huawei or ZTE equipment elsewhere in German networks.	Allows the Council of Ministers to designate a supplier as high, medium or low risk after considering technical assurance and exposure to external interference, including government links, ownership and governance, third-country laws, cyber defence cooperation and data-protection standards. Formal designation activates restrictions and replacement duties. No public Council of Ministers designation was identified by the open source cut-off date, so the strongest statutory prohibitions have not been publicly triggered.	Imposes security obligations (for example, to reduce supply-chain risks) and gives government powers to manage 'high risk vendors' – including the ability to control or require removal of their equipment from UK networks. Under the Act, the relevant secretary of state can issue Designation Notices for vendors whose presence in UK networks poses national security risks, and Designated Vendor Directions to telecoms providers. The latter place controls on the use (or require removal) of the designated vendor's goods and services.
	Measure	Measure	Measure
	Telecommunications Act, section 165: certification of critical components <i>Legislation</i>	National 5G Security Framework (ENS5G), Royal Decree 443/2024 <i>Regulatory powers</i>	UK Telecoms Lab <i>Testing and assurance</i>
	Effect	Effect	Effect
	Amendment to the 2021 Telecommunications Act means that critical components may be used only after certification by a recognised body. For public 5G networks, BSI rules require certification before a critical component is first used from 1 January 2026. The mechanism raises the technical-assurance threshold for components in sensitive network functions, but certification does not replace the separate trust and national security assessment available under the BSIG.	Operationalises 5G risk analysis, security controls, supply-chain dependence and diversification measures, protected geographic areas, a 5G security operations centre and the procedure for vendor risk classification and replacement. It sharpens Spain's 5G regime but does not itself publish a list of designated vendors; the legal consequences depend on a designation under Royal Decree-Law 7/2022.	Undertakes testing of and research on the security and resilience of telecoms technology.
			Measure
			Telecommunications Security Code of Practice <i>Assessment framework</i>
			Effect
			Outlines what 'good' telecoms security looks like and how to comply with the TSA regulations. It includes detailed technical measures and annexes on assessing network equipment security, supply-chain risk and vendor assurance, and is the main reference document Ofcom uses in assessing providers' security posture.

	Germany	Spain	UK
Government procurement	Measure	Measure	Measure
	BSiG sections 43–47 <i>Legislation</i>	Public Sector Contracts Law 9/2017 (Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014) <i>Legislation</i>	Procurement Act 2023 <i>Legislation and regulation</i>
	Effect	Effect	Effect
	Federal bodies must apply BSI IT-Grundschutz and federal minimum standards. BSI technical guidelines and reference architectures can shape acquisitions, and relevant security requirements must be flowed into service contracts. Departmental information security officers may prohibit specific IT products within their departmental remit. These are strong federal controls but do not create one central public sector high-risk-vendor register for federal, state and municipal purchasing.	Requires competition, equal treatment and proportionate technical specifications while allowing contracting authorities to include justified security and performance requirements. It contains no central, UK-style national security debarment list for technology suppliers. In practice, security and strategic autonomy concerns can still affect individual awards: in August 2025 the central government cancelled a Telefónica fibre contract that would have used Huawei equipment, without creating a general vendor designation.	Governs public procurement from February 2025 onwards. It introduced a new regime of mandatory and discretionary exclusion grounds, including a specific ground for national security, a new central debarment list, and expanded powers to terminate contracts and exclude suppliers that pose serious risks. In practice, gives government a legal route to bar or remove high-risk ICT vendors from individual procurements or from whole categories of sensitive contracts.
	Measure		Measure
	Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen, GWB) and Procurement Ordinance (Vergabeverordnung, V) <i>Legislation and regulatory powers</i>		National Security Unit for Procurement <i>Assessment unit</i>
	Effect		Effect
	Provides the general competitive and non-discriminatory procurement framework. Authorities may set proportionate security specifications, and section 107 GWB recognises national security exclusions where essential security interests cannot be protected by less intrusive means. The framework has no UK-style central national security debarment list for technology vendors; application remains decentralised and contract-specific.		Dedicated unit in the Cabinet Office that supports assessments of vendors on national security grounds, as per the Procurement Act. Receives referrals but can also self-refer.

	Germany	Spain	UK
Economic Security	Measure Foreign Trade and Payments Act and Ordinance (Außenwirtschaftsgesetz, AWG / Außenwirtschaftsverordnung, AWV): investment screening <i>Legislation</i>	Measure Article 7 bis of Law 19/2003 (Ley 19/2003, de 4 de julio, sobre régimen jurídico de los movimientos de capitales y de las transacciones económicas con el exterior y sobre determinadas medidas de prevención del blanqueo de capitales), and Royal Decree 571/2023 (Real Decreto 571/2023, de 4 de julio, sobre inversiones exteriores) on screening of foreign investment <i>Legislation</i>	Measure National Security and Investment Act 2021 <i>Legislation and regulation</i>
	Effect The Federal Ministry for Economic Affairs can review acquisitions that may affect public order or security, including lower-threshold holdings in specified sensitive sectors, and can impose conditions or prohibit a transaction. The mechanism addresses ownership and control of German businesses rather than ordinary purchases of equipment or services, so it complements rather than substitutes procurement and product-use controls.	Effect Requires prior authorisation for covered investments – generally acquisitions of at least 10% or control – where the target operates in protected sectors or the investor presents specified risks, including foreign-state control. Transactions may be conditioned or blocked. The regime addresses ownership and control of Spanish businesses, not routine acquisition of technology products or services.	Effect An investment-screening regime. The government can scrutinise and intervene in acquisitions of entities or assets in 17 sensitive sectors – including communications, data infrastructure, computing hardware and ‘critical suppliers to government’ – where acquisitions could pose national security risks. It can limit the ability of ICT vendors associated with national security law or country of origin risks to acquire technology or UK subsidiaries.

Source: The authors.

195 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 195 years.

