Report

Risky Configuration

China's Footprint in Germany's Technology Stack

Sharinee L. Jagtiani

G | M | F

Table of Contents

Preface

About GMF Technology

The German Marshall Fund of the United States (GMF) Technology Program is dedicated to ensuring that democracies collectively win the strategic technology competition against autocrats. With a transatlantic team based in Washington, DC, Berlin, Brussels, and Paris, GMF Technology offers technical expertise in three strategic areas: advancing democratic values in Artificial Intelligence (AI) innovation and policy, developing research and analysis to inform the emerging EU-US-China technology competition, and enhancing allied coordination and competitiveness in critical and emerging technologies including AI, biotechnology, defense technology and quantum information.

About the Report

This study is part of a research report series by GMF Technology that uses a "technology stack" or "tech stack" framework to assess the technology footprint of the People's Republic of China (PRC) in Europe and Central Asia. The report maps the presence of the PRC and its affiliated entities across countries' technological landscapes. These entities include publicly owned companies, PRC-registered private firms, and other organizations connected to the government and the Communist Party of China (CCP). Building on previous work detailed in two reports by GMF's Alliance for Securing Democracy (ASD) on the future internet and the digital information stack released in 2020 and 2022, this series introduces a five-layered "tech stack" framework: network infrastructure, data infrastructure, device, application, and governance. The reports present findings from desk research and study tours conducted by GMF Technology in the summer of 2024, as well as recommendations for policymakers informed by these findings.

Attributions

This publication was written under the supervision and guidance of Lindsay Gorman, Managing Director, and Astrid Ziebarth, Deputy Managing Director, of GMF Technology at the German Marshall Fund of the United States (GMF). It has been edited and reviewed by Sabine Muscat. The author acknowledges the role of Dylan Welch, China Technology Analyst, Adrienne Goldstein, Senior Program Coordinator, Caitlin Goldenberg, Program Coordinator, Julia Trehu, Program Manager and Fellow, and Livia Hartmann, Summer Trainee at GMF Technology for their research and editorial support. The author extends gratitude to Andrew Small, Mareike Ohlberg, Heli Tiirmaa-Klaar, and Valentin Weber for their feedback and input on this report. Special thanks to all the interviewees for their time and insights. Finally, thanks to the communications teams for their support in refining and enhancing the outreach of the piece. The views expressed in this publication are solely those of the author.

A Note on Methods

This analysis provides an indicative, rather than exhaustive, overview of the PRC's technology footprint in Germany. It is grounded in qualitative research, drawing from government statements, think tank reports and official policy documents and news reports. These sources shed light on policy priorities, geopolitical dynamics, and sectoral developments in Germany's technology landscape. The study also incorporates data collected from a series of unstructured interviews with Berlin-based policy experts in 2024.

The following caveats must be considered: First, desk research relies on the availability and reliability of publicly accessible information. Second, the interviews reflect the views of a specific group of stakeholders and may not capture the full spectrum of opinions or experiences within Germany. Despite these methodological limitations, this research seeks to deliver a comprehensive overview and nuanced analysis of the PRC's presence in Germany's technology landscape for policymakers and other interested readers.

List of Acronyms

AA: Auswärtiges Amt (Federal Foreign Office)
AI: Artificial Intelligence
ANNA: Access, Network of Networks, Automation and Simplification
ASD: Alliance for Securing Democracy
AWG: Außenwirtschaftsgesetz (Foreign Trade and Payments Act)
BEV: Battery electric vehicles
BMBF: Bundesministerium für Bildung und Forschung (Federal Ministry for Education and Research)
BMDS: Bundesministerium für Digitales und Staatsmodernisierung (Federal Ministry for Digitalization and Government Modernization)
BMFTR: Bundesministerium für Forschung, Technologie und Raumfahrt (Federal Ministry for Research, Technology and Space)
BMI: Bundesministerium des Inneren (Federal Ministry of the Interior)
BMWE: Bundesministerium für Wirtschaft und Energie (Federal Ministry for Economic Affairs and Energy)
BMWK: Bundesministerium für Wirtschaft und Klimaschutz (Federal Ministry for Economic Affairs and Climate Action)
BRI: Belt and Road Initiative
BSI: Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
CAICT: China Academy of Information and Communications Technology
CALT: China Academy of Launch Vehicle Technology
CCP: Communist Party of China
CETs: Critical and Emerging Technologies
CFSP: Common Foreign and Security Policy
CTG: China Telecom Global
DGAP: German Council on Foreign Relations
DSR: Digital Silk Road
E2EE: End-to-end Encryption
ECFR: European Council on Foreign Relations
ENISA: European Union Agency for Cybersecurity
GDPR: General Data Protection Regulation
GTAI: Germany Trade and Invest
IISS: International Institute for Strategic Studies
ICT: Information and Communication Technology
IoT: Internet of Things
ITA: International Trade Administration
ITU: International Telecommunication Union
IW: Institut der Deutschen Wirtschaft (German Economic Institute)
LEO: Low Earth Orbit
LLM: Large Language Models
MERICS: Mercator Institute for China Studies
MIC 2025: Made in China 2025
MIIT: Ministry of Industry, Information and Technology of the People's Republic of China
MoU: Memorandum of Understanding
NATO: North Atlantic Treaty Organization
NIS: Network and Information Security Directive
NSC: National Security Council
OECD: Organization for Economic Cooperation and Development
PRC: People's Republic of China
RAN: Radio Access Network
SeaMeWe-6: South East Asia-Middle East-Western Europe 6 Cable
SECM: Shanghai Engineering Center for Microsatellites
SHK: Swedish Accident Investigation Authority
SSST: Shanghai Spacecom Satellite Technology
TTK: TransTeleCom
VDA: Verband der Automobilindustrie (German Association of the Automotive Industry)

Executive Summary

Germany—just like the EU as a whole—has recognized the strategic importance of reducing unilateral dependencies in digital technologies.[1] In the face of geopolitical threats and economic uncertainty, the new German government has vowed to strengthen the country's technological growth and resilience.[2]

Germany confronts a changing global order, in which it faces a growing threat from Russia while traditional security guarantees under the transatlantic alliance have weakened. While the threat from Russia dominates Berlin's immediate strategic concerns, the growing alignment between Moscow and Beijing demands that this challenge cannot be viewed in isolation. As Germany recalibrates its national security posture from a peacetime orientation to one prepared for potential war, it is crucial to address the deepening strategic ties between Russia and the People's Republic of China (PRC) as part of a broader, interconnected threat.

The PRC's growing dominance in the German technology landscape threatens both Germany's national security and its long-term economic resilience. Germany's new government should now make increased efforts to effectively implement its China strategy, especially in the technology sector. Reducing exposure to systemic risks and de-risking the technological ecosystem is an urgent economic need and should be a security priority.

This analysis examines the digital footprint of PRC entities in Germany's technology ecosystem. It applies a "tech stack" framework to assess this footprint and its associated risks across five technology layers: network infrastructure, data infrastructure, device, application, and governance. The report illustrates the PRC's involvement within each layer, situates this engagement within the PRC's broader strategic objectives and identifies key vulnerabilities that could undermine Germany's security and competitiveness if left unaddressed.

Key Findings

- **Persisting 5G risks and emerging 6G threats:** Germany's efforts to secure its 5G infrastructure remain limited. Telecom operators have only been required to remove some, but not all Huawei equipment from their radio access network (RAN). Looking ahead, Huawei, ZTE, and China Mobile are already participating in public discussions hosted by partners in Germany's federally funded 6G-ANNA project, raising concerns about future 6G vulnerabilities.

- **Undersea cable vulnerabilities:** PRC firms—including China Telecom, China Unicom, China Mobile, and Hengtong—are key partners in new undersea cables linking Germany to Asia and Africa, creating strategic vulnerabilities in critical network infrastructure.

- **PRC presence in Germany's data infrastructure:** PRC firms such as Huawei, Alibaba, and Tencent control around 35% of Germany's cloud-computing infrastructure, which poses long-term risks of surveillance, IP theft, and military exploitation. These risks are amplified in critical use cases in Germany—such as the choice of Huawei as the cloud provider for university research in applied sciences in Germany.

- **Risky bets on electric and connected vehicles:** German firms—despite EU tariffs—continue deepening ties with PRC partners in electric and connected vehicles, as seen in the Tencent-Bosch cloud partnership and BMW's AI plans with DeepSeek. This bet on the PRC market undermines Germany's competitiveness and raises data security concerns.

- **Investment screening gaps:** Foreign entities can still acquire up to 25% of German firms in critical sectors like biotechnology and robotics without triggering investment review—sectors where PRC firms are actively seeking footholds through strategic partnerships and acquisitions, posing risks to competitiveness and data security.

- **PRC gains advantage in global standard-setting:** The Sino-German Industrie 4.0 Cooperation has helped China build expertise in global technical standard-setting, granting it long-term strategic leverage to shape global norms in line with its technological and economic goals.

Policy Recommendations

For German Policymakers

The National Security Council (NSC) under the Federal Chancellery should:

- Establish a cross-ministerial coordination mechanism on Critical and Emerging Technologies (CETs), using the 2024 Council for Technological Sovereignty CET list as a foundation (AI, quantum, biotech, semiconductors, ICT, and Industry 4.0)

- Convene a high-level technology advisory panel of independent experts in technology, geopolitics, and economic security to regularly brief the NSC

- Conduct a review of Germany-China technology collaborations using the technology stack framework

The Federal Office for Information Security (BSI) should:

- Drive EU coordination on data security by defining categories of high-risk and sensitive data—such as national security and government data—that must not be processed on untrusted foreign systems

The Federal Ministry for Digitalization and State Modernization (BMDS) should:

- Establish a Strategic Foresight Unit for coordinated response to technology crises

- Strengthen data security through a risk-based toolbox in digitalization

- Guide the secure digital transformation of German SMEs by creating a state-backed platform offering regulatory compliance resources, training, and a curated marketplace of trusted digital tools, data centers, and cloud providers

The Federal Foreign Office (AA) should:

- Update Germany's China Strategy with a robust technology de-risking component

The German Navy should:

- Enhance the security of German and European undersea internet infrastructure by:
    - Incorporating sabotage stress tests into Baltic Sea exercises (e.g. Northern Coasts maneuvers with NATO allies)
    - Sharing lessons learned from its role as Commander of Task Force (CTF) Baltic with European partners involved in the CTF Mediterranean, to enhance the security of undersea network infrastructure.

The Federal Ministry for Research, Technology, and Space (BMFTR) should:

- Strengthen research security for emerging and dual-use technologies
- Support German leadership in European satellite internet by directing seed funding to German startups and research institutions developing satellite internet technologies, reducing dependence on PRC-based investors and building European satellite infrastructure champions

The Federal Ministry for Economic Affairs and Energy (BMWE) should:

- Initiate Bundestag debates on:
    - Phasing out PRC-made surveillance technologies in public spaces
    - Updating public procurement law to prioritize vendor trustworthiness, data protection, and supply chain transparency—not just price
    - Expanding investment screening rules to include CETs

For the European Commission

- Adopt the technology stack framework to broaden its 2023 risk-assessment recommendations to member states
- Publish a third progress report on 5G Cybersecurity Toolbox implementation, with a focus on member state compliance — particularly Germany
- Urge Germany to transpose the EU's NIS 2 Directive into national law
- Reduce EU dependence on PRC cable companies for undersea network infrastructure
- Diversify IoT device imports via Indo-Pacific Free Trade Agreements (FTAs)
- Ensure the Strategic Dialogue on the Future of the European Automotive Industry addresses PRC dependencies, aligning member states and industry leaders on mitigation strategies

For the United States

- Encourage Germany to support the creation of an EU-level entity list mechanism under the Common Security and Foreign Policy (CSFP) framework
- Engage and coordinate directly with the European Union as a whole— in addition to coordinating with individual member states like Germany—to develop a joint response to the PRC's expanding global technology footprint
- Preserve and strengthen transatlantic coordination mechanisms on export controls, investment screening, sanctions, and technology standardization
- Promote bilateral exchange on research security best practices

The Tech Stack Framework: Assessing China's Technology Footprint and Associated Risks in National Technology Ecosystems

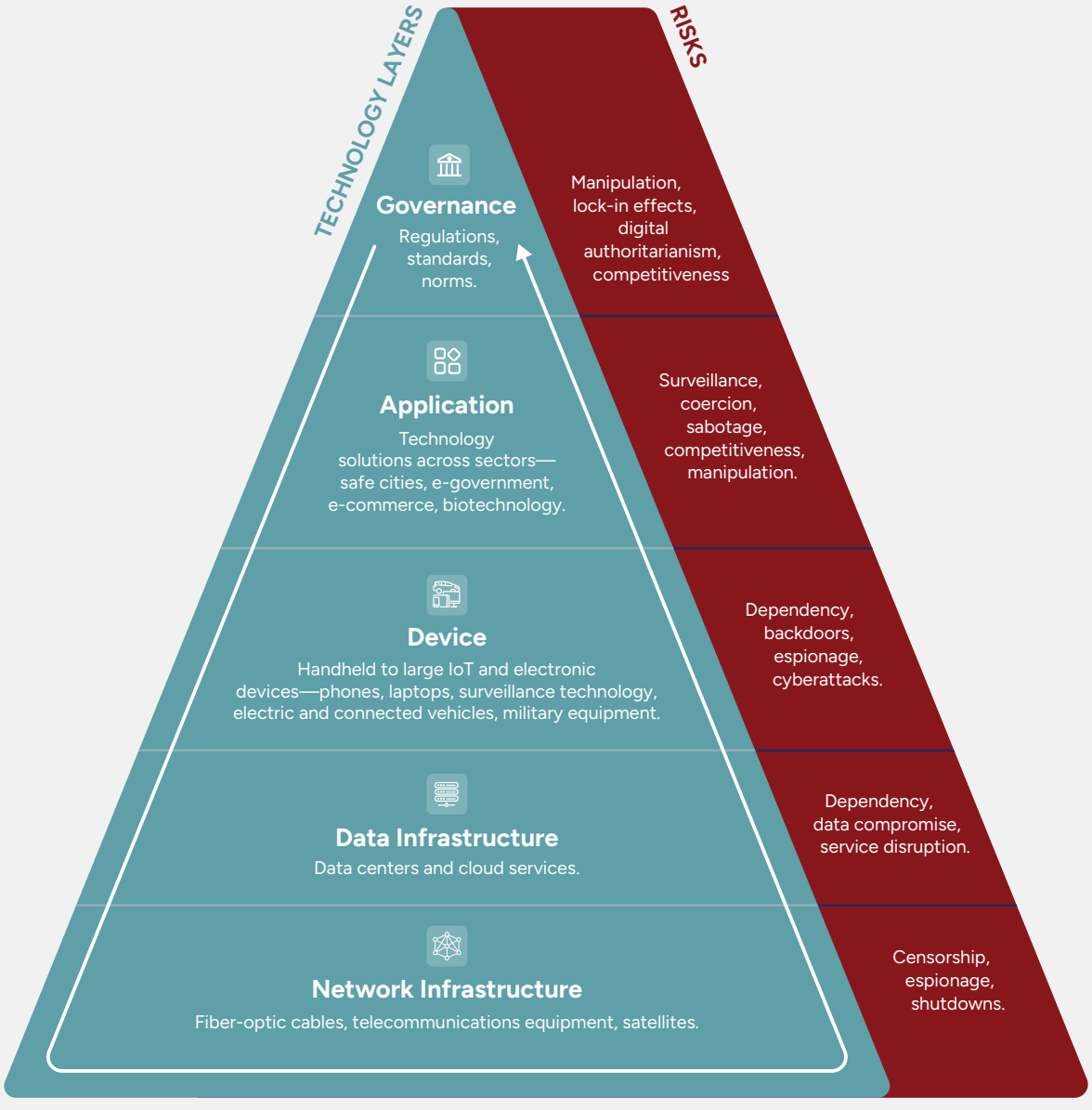


Figure 1: The tech stack framework illustrates how China's digital footprint penetrates a country's technology ecosystem and the associated risks across five layers: network infrastructure data infrastructure, device, application and governance. The framework is detailed on pages 12 and 13.

Familiar to technologists, the term "tech stack" refers to all aspects of information technology (IT) infrastructure required to deploy and manage digital applications and services: hardware and software components, databases, middleware, storage and networking.[3] In the recent past, GMF and others have transferred the concept to the policy discourse, broadening it to include the hardware, governance, and infrastructure that a country's digital systems are built on.[4]

The tech stack framework (Figure 1) is built on two prior studies by GMF's Alliance for Securing Democracy (ASD) program. The first, Lindsay Gorman's 2020 "Future Internet for Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything" presented a "Future Internet technology stack" to analyze China's expanding footprint in global telecommunications, the Internet of Things, applications, and international technical standards—and the threats it poses to the United States and its allies.[5] The second, in 2022, "China and the Digital Information Stack in the Global South" by Bryce Barros, Nathan Kohlenberg, and Etienne Soula adapted this stack framework to the digital information landscape and applied it to five country case studies: Thailand, Myanmar, Uganda, Nigeria, and Jamaica.[6]

In this analysis, the tech-stack framework spans five layers to assess how the PRC and its affiliated entities penetrate and influence Germany's technology landscape: network infrastructure, data infrastructure, device, application, and governance. Each layer is examined in relation to the potential dependency or influence risks therein.

Network Infrastructure Layer: The physical infrastructure that transforms isolated computers into a vast, interconnected network defining the modern internet. It includes but is not limited to optical cables (terrestrial and undersea), telecommunications equipment, satellites, and space-based connectivity infrastructure.

Risks: Actors with malicious or autocratic intent who control network infrastructure can censor, filter, or shut down internet access, and reroute, copy, and exfiltrate data flows for espionage and surveillance purposes.

Data Infrastructure Layer: The physical infrastructure used to store, manage, access, and process data, including cloud technology and data centers. These technologies are foundational to compute-intensive applications like AI, connected devices in the Internet of Things (IoT), and smart and safe cities.

Risks: Actors with malicious or autocratic intent can abuse control over data centers and cloud infrastructure to create dependencies, compromise sensitive data, and disrupt key services.

Device Layer: The physical devices used by individuals or institutions to access the internet such as hand-held consumer devices like mobile phones, tablets, and laptops. This layer also encompasses IoT devices, such as surveillance equipment; larger devices such as electric and connected vehicles; and equipment used in defense and law enforcement.

Risks: Actors with malicious or autocratic intent can abuse their dominance in device manufacturing to create dependencies and gain strategic leverage, while backdoors built into these devices enable data theft, cyberattacks, network infiltration, and espionage.

Application Layer: The application of technological tools, systems, and innovations to tackle sector-specific challenges and enable new capabilities. It comprises hardware, software, data analytics, and digital platforms used to deliver tailored solutions to consumers, sectors, and industries. This layer therefore includes sectors like public security (surveillance systems, safe cities), digital services (e-government), education (e-learning platforms), transport (smart traffic systems), manufacturing (robotics, automation), healthcare (telemedicine, biotechnology), and consumer-facing applications (e.g. e-commerce, e-finance, social media).

Risks: Actors with malicious or autocratic intent can leverage their dominance in digital services to create strategic dependencies and gain commercial advantages. By controlling social platforms, they can surveil users, harvest data, and manipulate public discourse. Additionally, their control over critical applications enables them to disrupt or disable critical infrastructure, including energy grids, transportation networks, and financial systems.

Governance Layer: The legal and normative framework that governs technology use across the entire tech stack. It serves as a "layer of layers", including regulations, norms, and standards.

Risks: Actors with malicious or autocratic intent can circumvent or find loopholes in a country's data protection laws and other relevant technology-related regulations. They do this through knowledge-sharing initiatives and by influencing standard-setting bodies to institutionalize their regulatory models. Their influence on technical standards also poses cybersecurity risks, as they retain deep knowledge of system vulnerabilities, which they can exploit.

Introduction

Germany finds itself at the cusp of a changing global order. The American foreign policy consensus that shaped the country's post-World War II trajectory has significantly eroded.[7] A few weeks into the second Trump administration, US defense secretary Pete Hegseth told European defense ministers that the United States was no longer "primarily focused" on European security.[8] With the potential vacuum left by the weakening American security guarantee in Europe, the threat posed by Russia has become a central concern in Berlin's security calculus.[9] The Russian threat in Europe, however, is also amplified by the People's Republic of China (PRC).

In a statement before the US Subcommittee on Strategic Forces, Commander of the US Strategic Command Anthony J. Cotton highlighted that Beijing has enabled Russia's ability to enhance its defense industrial base and bypass extensive sanctions.[10] This material support is reinforced by an evident display of solidarity at the political level. At the margins of the 14th National People's Congress on March 7, 2025, the PRC's foreign minister Wang Yi held, "China and Russia have decided to forge everlasting good-neighborliness and friendship, conduct comprehensive strategic coordination, and pursue mutual benefit, cooperation and win-win, because this best serves the fundamental interests of the two peoples and conforms to the trend of our times."[11]

Amid strained relations with the United States and the pressing threat from Russia, German policymakers may be tempted to reconsider the assessment of the PRC as a "systemic rival". But as Germany recalibrates its national security posture from a peacetime orientation to one prepared for potential war, it is crucial to address the deepening strategic ties between Russia and the PRC as part of a broader, interconnected threat. This threat analysis is essential as Germany seeks to strengthen its resilience—both on the conventional battlefield and across emerging strategic frontiers. Among these, technology stands out as a critical domain. Leadership in advanced technologies is central to the PRC's geopolitical ambitions, exemplified by the "Made in China 2025" strategy (MIC 2025)—a ten-year plan aimed at upgrading the country's manufacturing capabilities. Building on decades of industrial policy, these efforts have helped transform the PRC into a global powerhouse in electronics, machinery, and high-tech production. The blueprint drew significant inspiration from Germany's "Industrie 4.0" initiative, which marked the country's drive toward the digitalization of manufacturing in the Fourth Industrial Revolution.[12]

It is crucial to understand the PRC's technological footprint in Germany in the context of its broader strategic ambitions. This requires viewing the full scope of the PRC's technological engagement—spanning connectivity, data infrastructure, device, application and governance—as part of the Digital Silk Road (DSR), the digital arm of the Belt and Road Initiative (BRI), but also as part of the PRC's ambition to take on the world's leading tech nations, including Germany.[13] This report offers a comprehensive review of Germany's technological ties with the PRC by assessing a full spectrum of national and economic security risks, from espionage and supply chain dependencies to economic coercion, disruption and sabotage.

In 2023, Germany released its first-ever Strategy on China in response to the PRC's growing assertiveness and efforts to reshape the rules-based international order. On technology, the strategy stressed that the EU should not become dependent on "third countries" that do not "share [its] fundamental values".[14] It emphasized "de-risking" these critical dependencies by factoring geopolitical risks into economic decisions, and by bolstering resilience across its technology landscape.[15] While the strategy acknowledged the challenges posed by the PRC, its discussion of technology-related risks was limited and lacked a clear framework for addressing them.[16]

Relatedly, Berlin's 2024 decision to partially ban components from Huawei and ZTE in its 5G networks—set for a distant 2029 deadline—reflects the gaps between vision and implementation of the China strategy.[17] This disconnect extends beyond 5G, highlighting a broader reluctance to address technological dependencies.

This report contends that the new German government must significantly strengthen the technology dimension of its China strategy and invest greater effort in de-risking its technological engagement with the PRC. To support this goal, this report maps the extent and nature of the PRC's presence and engagement within Germany's technology stack or "tech stack". Building on previous GMF research, the term "tech stack" is used to examine one country's presence in and penetration of another country's technology ecosystem.[18] The "tech-stack framework" spans five layers: network infrastructure, data infrastructure, device, application, and governance.

The analysis provides examples of the PRC's engagement with Germany within these layers and contextualizes them within the PRC's broader strategic goals. Across the layers, the analysis highlights the risks for Germany if these areas are overlooked. It begins with an outline of the tech-stack framework used in the analysis. Next, it details evidence of the PRC's presence across Germany's technology stack. Finally, the report concludes with 25 recommendations for policymakers in Germany, the EU and the United States.

China's presence in Germany's Technology Stack

Network Infrastructure Layer

The German government announced its first-ever Strategy for International Digital Policy in 2024. The strategy notes that it complements Germany's China strategy and seeks to advance "a global, open, free and secure Internet".[19] This vision of the future internet stands in stark contrast to the PRC's authoritarian model, which is built on tight control, censorship, and suppression in pursuit of the Communist Party of China's (CCP) mission to make the world safer for the country.[20] As early as 2018, a White Paper on the PRC's international optical cable connections by the China Academy of Information and Communications Technology (CAICT), a research institute under the PRC's Ministry of Industry, Information and Technology (MIIT), noted Europe as "one of the important destinations for China's international communications services".[21] The analysis below illustrates the PRC's presence in three segments of the German network infrastructure: telecommunications infrastructure, optical cables (submarine and terrestrial) and satellite internet.

Telecommunications:

Public debate over Huawei's role in Germany's 5G infrastructure began in 2018. By that time, major telecom operators in Germany, including Deutsche Telekom, Vodafone, and Telefónica, had already integrated Huawei technology into their 4G and planned 5G networks.[22] In 2019, Germany created a legal framework for excluding Huawei, but the implementation was delayed until 2024, when the government decided to initiate a phased removal of Huawei and ZTE equipment. Under this mandate, mobile operators are required to eliminate Huawei and ZTE components from 5G core networks by the end of 2026 and to replace Huawei's and ZTE's management systems in 5G access and transport segments by 2029.[23]

Some German lawmakers have criticized the extended timeline, arguing that by 2029, much of Huawei's equipment would be obsolete and need replacement regardless.[24] Notably, the mandate still allows operators to retain all Huawei products except the configuration management system—a relatively minor part of the radio access network (RAN)—, which must be replaced by the end of 2029. [25] This also raises concerns that Huawei could exploit those products to conduct espionage or disrupt Germany's communications infrastructure through malicious software.[26] According to the Danish Strand Consult, as of 2024, 59% of Germany's 5G infrastructure is sourced from China. Moreover, Germany has only partially implemented the EU's 5G toolbox, which outlines a coordinated European strategy for securing 5G networks.[27]

This is especially significant given the integration of Huawei technology into some of Germany's critical public infrastructure. [28] The German public rail network Deutsche Bahn as a key example. Deutsche Bahn relies on Huawei technology not only for the passenger Wi-Fi but also for its internal communications infrastructure. Since 2015, PRC-manufactured components have supported systems that facilitate communication between train personnel and control centers.[29]

This integration creates security risks, as it provides the PRC with access points to data that could be exploited for espionage or cyberattack, introducing a critical vulnerability during periods of geopolitical tension. If Germany

were to oppose a policy position taken by the PRC—such as by adopting a more assertive stance in support of Taiwan's sovereignty—PRC-linked actors could exploit their access to disrupt essential services across German cities. This could result in widespread paralysis of public transportation networks, catching authorities and civilians off guard. In more severe scenarios, such disruptions could impede emergency response or military mobility or even involve the embedding and activation of "kill switches" to disable transport systems entirely. These risks highlight the strategic importance of securing digital infrastructure across all sectors, including those traditionally seen as civilian and non-combatant.

Despite the long-drawn 5G debate in Germany, there are indications that Huawei and other PRC vendors are not entirely excluded from Germany's 6G plans. In April 2024, representatives from Huawei and China Mobile Research Institute were included in a "6G Expert Days" workshop organized by German company Rohde & Schwarz.[30] The company is listed as a partner in the then-Federal Ministry for Education and Research (BMBF) (now Federal Ministry for Research, Technology and Space, BMFTR)-funded 6G-ANNA project, which leads national research and deployment efforts on 6G.[31] This reveals that the de-risking framework outlined in its China strategy is yet to permeate Germany's 6G discussions.

Optical Cables

Submarine cables account for over 99% of the world's internet traffic.[32] Germany is not home to major high-capacity, intercontinental submarine cable connections. Instead, through a network of terrestrial cables, it depends on other EU member states to transfer data to other continents.[33] PRC-based equipment providers such as China Mobile, Hengtong Marine, China Telecom and China Unicom are part-owners of Germany's undersea and overland connections to Asia and Africa. The PRC's involvement in German and European network infrastructure has been part of its grand strategic vision for global connectivity provision. The 2018 CAICT White Paper notes that the PRC seeks to "facilitate synergy between the submarine and terrestrial cables, allowing them to work together to build a 'Eurasian information hub' that connects east to west".[34]

Submarine Cables

Germany hosts six main landing points for submarine cables that run across the North and Baltic Seas (see Figure 2). Germany is not a primary landing point for the world's major submarine cables—those characterized by significant length and high data-transmission capacity. Instead, it relies heavily on neighboring European countries for access to the global internet via undersea infrastructure.[35] For instance, transatlantic cables like Grace Hopper and Marea have landing points in Spain while Amitie and Dunant run from France to the United States. These cables have a combined capacity of 1,132 terabits per second (Tbps).[36] To the south and east, in Marseille, France, ten submarine cables, including high-capacity lines like 2Africa and IMEWE, extend to North Africa and the Middle East, continuing onward to South Asia.[37]

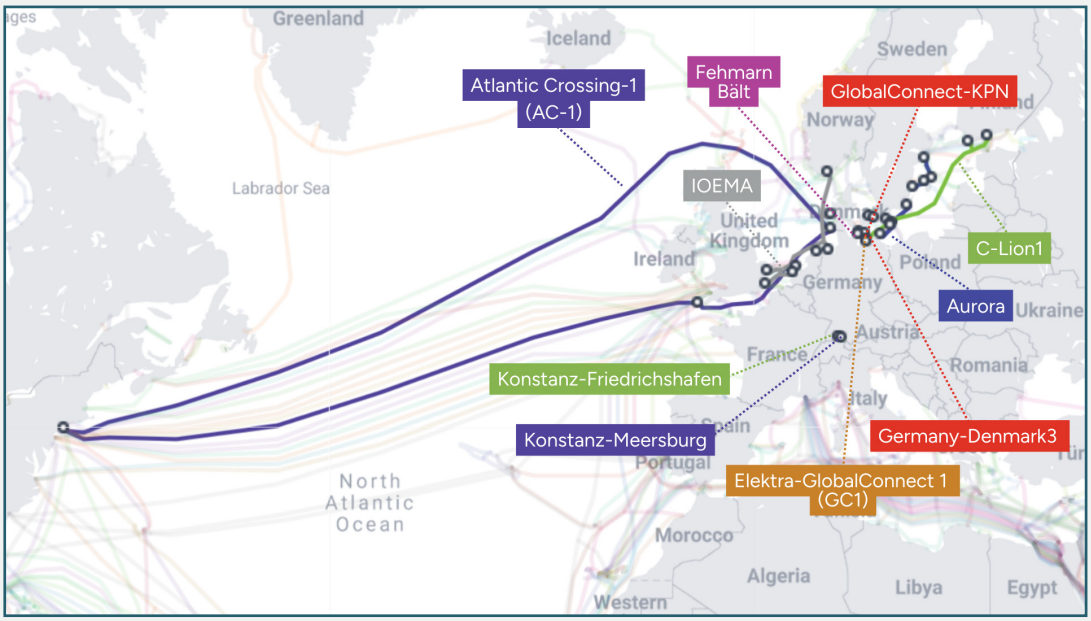


Figure 2: Submarine Cables with Landing Stations in Germany
Source: Adapted from TeleGeography

The security of Germany's internet infrastructure therefore relies heavily on its European neighbors.[38] These high-capacity transmission cables would be primary targets for surveillance, espionage and sabotage.[39] These risks are heightened with the untrustworthy ownership of cables. As noted in a 2023 study commissioned by the European Parliament's Committee on Security and Defence, investors under PRC state control (state-owned companies) and PRC (including Hong Kong) private companies with indirect, yet strong party-state links can have similar risk profiles.[40] PRC-owned cable companies are encouraged and supported by the state to contribute to global undersea cable provision.[41] In the long term, the growing share of global traffic routed through cables owned by PRC-based providers will strengthen the PRC's ability to reshape global internet architecture—by creating strategic chokepoints.[42]

Some PRC-based companies are part-owners of cables connecting Europe to the world. For instance, the 2Africa cable (Figure 3), which was launched in 2020, forms a 180 Tbps loop around Africa and is supported by eight partners, including Meta and China Mobile.[43] Similarly, the PEACE cable (Figure 4), offering the shortest routes from Asia to Europe and Africa since 2022, is led by Hengtong Marine, a subsidiary of China's Hengtong Group. It also includes partners like China Mobile, China Telecom, China Unicom, and European telecom operators such as Orange. [44]

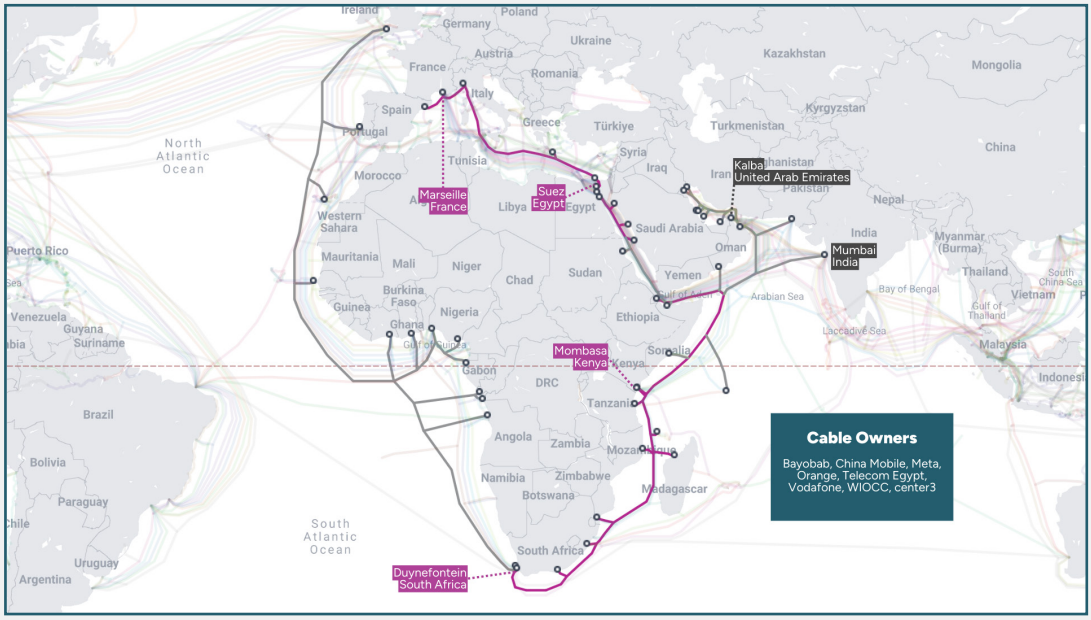


Figure 3: 2Africa submarine cable with selected landing stations highlighted
Source: Adapted from TeleGeography

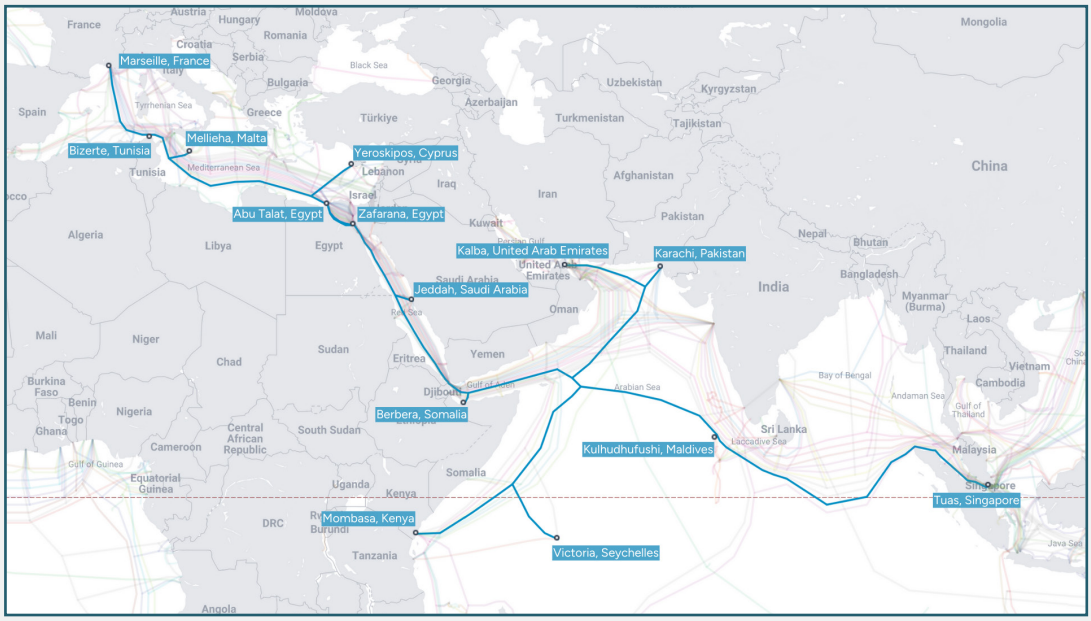


Figure 4: The PEACE submarine cable with landing stations highlighted
Source: Adapted from TeleGeography

According to MERICS' DSR tracker, Hengtong's portfolio has expanded in Europe. The company has acquired stakes in companies like Portugal's Alcobre, Spain's CABLESCOM, and Germany's J-Fibre.[45] After the acquisition, J-Fibre publicly stated that it "shares the same values" as its parent company.[46] This is especially concerning given Hengtong's involvement in constructing underwater surveillance systems in the East and South China Seas, as highlighted in the 2023 study for the European Parliament.[47] The study notes that Hengtong's joint venture with the People's Liberation Army (PLA)'s cyber lab heightens the possibility of espionage through the cables it owns. Accordingly, it notes that cables laid close to EU and NATO member states' naval bases by Hengtong and its subsidiaries present a "high-level security vulnerability".[48]

In 2021, the United States added Hengtong subsidiaries Jiangsu Hengtong Marine Cable Systems and Jiangsu Hengtong Optic-Electric to its Entity List for acquiring and attempting to acquire US-origin items in support of military modernization for the PLA.[49] Submarine cable communication-service provider HMN International was also added to the list on the same grounds. In 2023, through a combination of incentives and pressure, Washington successfully prevented Tianjin-headquartered submarine cable-service provider HMN Tech from securing the supply contract by a multinational consortium to lay the South East Asia–Middle East–Western Europe 6 (SeaMeWe-6) cable.[50]

Beyond surveillance, the risk of physical sabotage of undersea infrastructure is a growing concern. Officials from Taiwan have accused the PRC of employing tactics such as sand dredging to damage undersea communication cables and intimidate residents and tourists.[51] Taiwan characterizes these activities as "grey zone operations"—tactics employed by the PRC to exert pressure without engaging in open conflict. [52] In April 2025, Taiwan charged a ship captain from the PRC with intentionally damaging undersea cables off the island in February that year.[53] Closer to home, a series of recent disruptions in the Baltic Sea has heightened concerns about Europe's own cable vulnerabilities.[54]

From October 2023 to December 2024, there were nine instances of damage to submarine cables linking Estonia, Finland, Germany, Lithuania, Russia, and Sweden.[55] While these incidents raised suspicions in Europe that Russia might be targeting undersea infrastructure as part of a broader campaign of hybrid attacks, an incident in November 2024 draws attention to the PRC. According to the Swedish Accident Investigation Authority (SHK), a PRC-owned carrier Yi Peng 3 severed two subsea cables—one linking Germany and Finland, the other connecting Lithuania and Sweden. SHK stated however, that there was no conclusive evidence to determine whether the incident was accidental or an act of intentional sabotage.[56]

These examples highlight critical vulnerabilities in Germany and Europe's network infrastructure, which need to be addressed with greater urgency. In its preparation for a pre-war scenario, Germany would also need to factor in the risk of a simultaneous attack on high-transmission cables, which could result in an EU-wide blackout.

Terrestrial Cables

Germany is also home to landing points of terrestrial cables developed by companies headquartered in China and Russia, which connect Europe to Asia. Notable examples include the Europe-Russia-Asia (ERA) cable system, a project of China Telecom and Russia's TransTeleCom (TTK); the Transit-Mongolia Pathway (TMP), operated by China Telecom Global (CTG) alongside Mongolian and Russian partners; and the Diverse Route for European and Asian Markets (DREAM) cable, which connects Germany, Austria, Slovakia, Ukraine, Russia, Kazakhstan, and the PRC.[57] DREAM was launched in 2013 and developed by Russia's MegaFon in partnership with

Kazakhtelecom.[58] The data traffic on these routes remains relatively low, and interviews with Berlin-based tech policy experts suggest that these cables currently pose comparatively lower espionage risks than the undersea cables discussed above. And yet, these routes warrant attention given China's vision of integrating land and sea infrastructure across Eurasia and of leveraging expanded communication networks to bolster influence.

Satellite Internet

Satellites carry only about 1% of global internet traffic, but they offer advantages over terrestrial or undersea cables, being less vulnerable to natural disasters, conflict, or sabotage.[59] The PRC has prioritized the development of satellite internet as part of its "new infrastructure concept", a strategic vision laid out by the National Development and Reform Commission in 2020.[60] In 2024, the PRC launched three batches of satellites for the Shanghai-backed Qianfan (SpaceSail) network, aiming—like Elon Musk's Starlink—to deliver global high-speed internet access.[61] One researcher interviewed for this study noted that German firms have sought to compete in the satellite industry, but limited public funding has left an investment gap, which PRC companies have stepped in to fill.

A notable example is Munich-based KLEO Connect, a startup that sought to deploy a network of over 300 Low Earth Orbit (LEO) satellites, mirroring SpaceX's Starlink.[62] To this end, it partnered with the Liechtenstein-based Trion Space, which had secured valuable International Telecommunication Union frequency allocations (hereafter: ITU filings).[63] This included the Ka-band (26–40 GHz) frequency allocations ideal for robust broadband connectivity. Lacking investors, however, KLEO Connect struggled to operationalize its plans until two Shanghai-based firms, Shanghai Engineering Center for Microsatellites (SECM) and Shanghai Spacecom Satellite Technology (SSST) became involved. SECM is a satellite manufacturer and SSST is a military-linked, majority state-owned company in the PRC, and according to former US national security officials Glenn Chafetz and Xavier Ortiz, was specifically established to invest in Western satellite projects.[64]

In 2017, KLEO's founders accepted an initial 10% investment from SSST, which grew to a 53% majority stake by 2018.[65] This led to a governance structure in which co-founder Matthias Spott oversaw technical operations, while Shanghai-based Shawn Shey managed the commercial side. Kleo's European founders later alleged however, that SSST's true objective was not partnership, but control over KLEO's valuable ITU filing.[66] Tensions escalated in 2019 when SSST unilaterally awarded a satellite manufacturing contract to SECM, a move the Europeans saw as an attempt to transfer KLEO's orbital priority to the PLA—an act prohibited by ITU rules.[67] Their suspicions deepened in 2021 when SECM launched test satellites into the same orbital slot and frequency range KLEO had planned to use, reinforcing fears that the joint venture was being exploited to advance the PRC's strategic interests in space. [68]

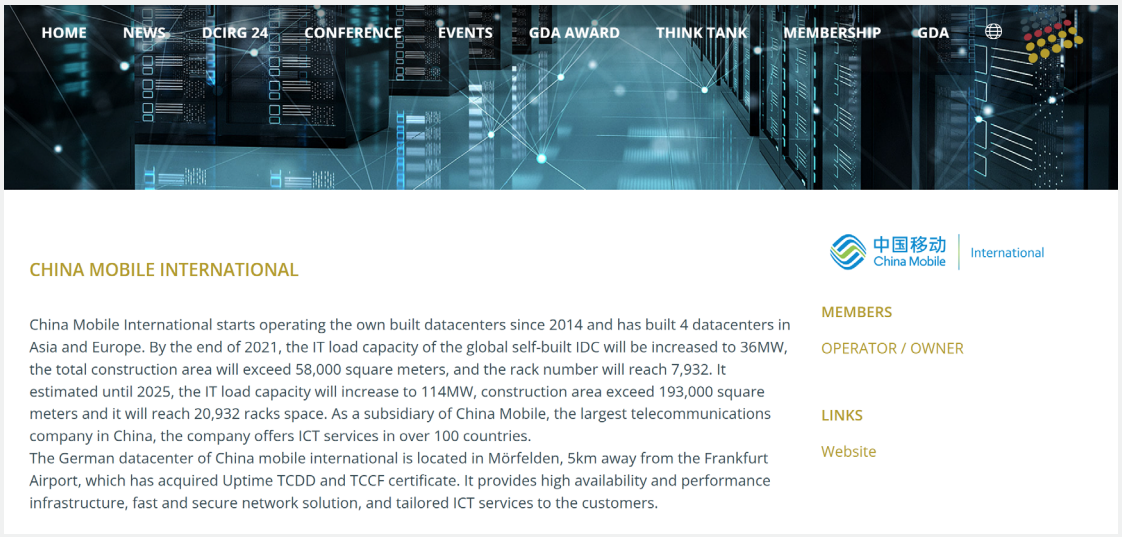
The founders then triggered a provision of the investment agreement allowing them to redeem investors' shares and bring in a new partner, the US telecommunications company Rivada.[69] The PRC investors, however, rejected the redemption offer and launched a series of lawsuits in Liechtenstein, Germany, Luxembourg, and the US to gain control of KLEO's spectrum rights. While litigation was ongoing, SSST moved ahead with plans to build and launch satellites from China using the Liechtenstein ITU filings. [70] In March 2022 however, Liechtenstein's telecoms regulator rejected SSST's claim to the filings and awarded the spectrum rights to Rivada—a decision later upheld by Liechtenstein's courts. [71]

The following year, SSST attempted to increase its stake in KLEO Connect, but the move was blocked by Berlin after an investment review by the then-German Federal Ministry for Economic Affairs and Climate Action (BMWK) – now Federal Ministry for Economic Affairs and Energy (BMWE) – which determined that the acquisition posed a potential threat to public security.[72] According to the CELIS Institute, a Berlin-based non-profit dedicated to studying and debating investment screening policy, the China strategy released that same year had led to a perception change vis-à-vis PRC-based investors. Additionally, the report noted that the volume of shares SSST was attempting to purchase constituted an "acquisition" under the Foreign Trade and Payments Ordinance, allowing the BMWK to examine and prohibit it.[73]

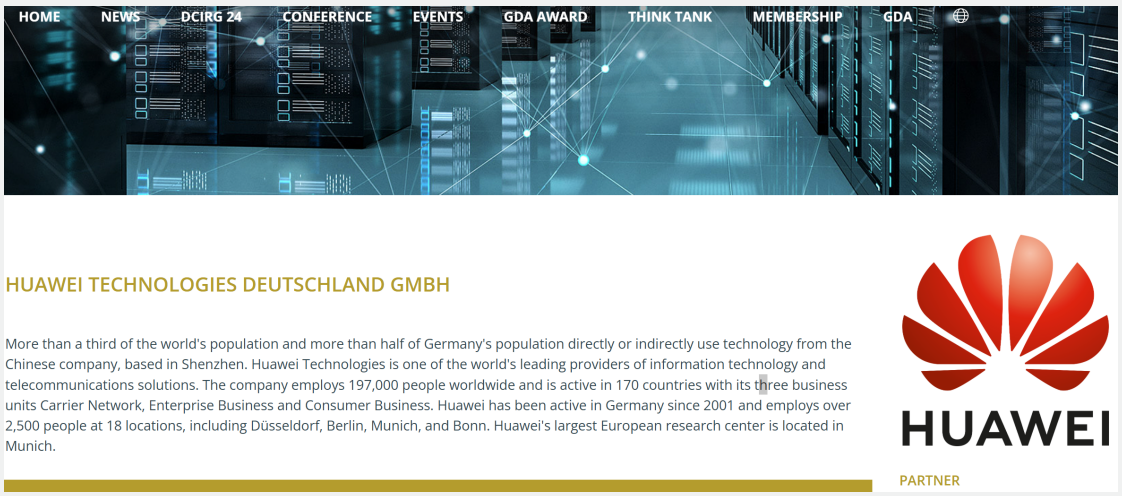
In 2024, Liechtenstein's telecoms regulator, which had licensed transmission frequencies to Rivada, revoked the authorization, citing non-payment of annual fees and the absence of a credible business plan.[74] Meanwhile the PRC continued to pursue its space ambitions. In March 2025, the China Aerospace Science and Technology Corporation announced the successful launch of 18 additional satellites for the Qianfan constellation.[75] This raises important questions about the extent to which SSST's ownership stake in KLEO Connect helped pave the way for advancing China's LEO ambitions. An expert interviewed for this report noted that the KLEO Connect case illustrates a pattern of PRC investors acquiring European firms primarily to gain control over valuable assets such as ITU frequency allocations, often without fully utilizing the technology or growing the company. Whereas Berlin's intervention in 2023 reflects a proactive approach to halt the PRC's acquisitions in network infrastructure, it also highlights a broader concern: the lack of public funding for satellite internet technology.[76] The underemphasis on building critical network infrastructure technology reflects a missed opportunity for Germany to build a home-grown competitor in the satellite market.

Data Infrastructure Layer

The German government has emphasized the expansion and protection of cloud and data infrastructures in its 2024 international digital policy strategy.[77] This strategy identifies a strong data infrastructure as crucial for a sustainable global digital ecosystem while avoiding critical dependencies.[78] Marketplace platform Cloudscene describes Germany's data center industry as "thriving", with Frankfurt leading in data center density nationwide.[79] The Frankfurt/Rhine-Main area also hosts DE-CIX, one of the world's largest Internet Exchanges by data throughput.[80] Proximity to DE-CIX significantly reduces latency in data transmission, making Frankfurt a rapidly growing data center market.[81] Germany's data center market features several players, including Dell, Nokia and Nvidia.[82] There is evidence of the presence of major PRC providers, such as Alibaba, China Mobile, China Telecom, and Tencent.[83] Specifically, China Mobile (International) and Huawei are members and partners, respectively, of the German Datacenter Association (GDA), an advocacy alliance of data center operators and owners in the country (see screenshot below).[84]



China Mobile (International) listed as a member of the German Datacenter Association
Source: GDA



Huawei listed as a partner of the German Datacenter Association
Source: GDA

According to a 2024 study by the Asia-based philanthropic organization, the Hinrich foundation, the PRC's investment in global data infrastructure is part of a border, long-term strategy aimed at gaining asymmetric advantage in cross-border data flows.[85] This involves enforcing stringent data localization laws domestically, developing infrastructure to access foreign data, and competing to set the standards for data architecture and the physical data center outposts globally.[86] The PRC's Global Tone Communications Technology (GTCOM), a subsidiary of the state-owned China Publishing Group, once described data as the "new oil", making data centers, in this analogy, one of its essential refineries.[87] In 2020, the PRC's Politburo Standing Committee designated data centers as part of a list of "new infrastructures", and by 2022 they were prioritized in the National Development and Reform Commission's (NDRC) Implementation Plan for the 14th Five-Year Plan.[88]

In 2022, Alibaba Cloud launched its third data center in Germany, with a special focus on AI and machine-learning applications. In a press release, Alibaba stated that the data center complies with the Cloud Computing Compliance Controls Catalog (C5) laid out by the German Federal Office for Information Security (BSI).[89] While data centers based in Germany or the EU are subject to European data protection laws and security standards, this does not eliminate the risk of data leakage. A cybersecurity expert interviewed for this study, noted that data could potentially be transferred back to a data center's home country on the pretext of a "technical problem", placing it outside EU jurisdiction. This risk is heightened in the case of data centers owned by PRC companies. Under the PRC's National Intelligence Law of 2017, PRC citizens and companies are obliged to turn data over to the state upon request.[90]

In addition to data centers, PRC companies like Alibaba and China Telecom are expanding their services as cloud providers and positioning themselves as gateways for German businesses to access the PRC market. For instance, China Telecom's European division promotes itself as the "Digital Silk Road to China/APAC", while Alibaba's China Gateway 2.0 offers European businesses access to PRC consumers.[91] Several major German companies have used Alibaba Cloud in their services and platforms. For example, Siemens' IoT platform, MindSphere, was hosted on Alibaba Cloud in 2019, allowing PRC-based clients to develop applications securely within the PRC.[92] More recently, in 2023, Alibaba Cloud signed a strategic cooperation agreement with Siemens Xcelerator, an online digital business platform.[93] German multinational SAP has also partnered with Alibaba Cloud in 2018 to expand its customer base in the PRC. [94] This collaboration has continued to deepen, and in May 2025 SAP announced a strategic partnership with the Alibaba Group to accelerate cloud transformation for customers, with an initial focus on the PRC market.[95]

In addition to major German companies, Alibaba Cloud has recently targeted German SMEs, providing AI-driven tools for strategic decision-making and customer engagement. According to Alibaba's own surveys, many German SMEs believe that AI will improve their export activities, yet only 11% have implemented AI tools in their businesses.[96] In response, Alibaba is offering AI-powered tools, including product listings, a chatbot, and automatic data analysis to support strategic decision-making and enhance customer outreach.[97]

As German companies deepen partnerships with PRC-based cloud providers, they must also consider the risk that these arrangements could create technology dependencies on PRC companies, with long-term lock-in effects. Foreign firms operating in the PRC are required to use local platforms and infrastructure, such as Alibaba's services, which can gradually bind them to the PRC's digital ecosystem. Large companies like SAP may have the resources to utilize multiple cloud providers in different markets. But smaller businesses may not have the resources to use more than one cloud provider. This could potentially lock them into PRC-based cloud ecosystems even when operating in markets outside the PRC.

According to a 2025 study by researchers at the Oxford Internet Institute and Aalto University in Finland, which mapped the global footprint of the six leading global hyperscalers—Amazon Web Services (AWS), Microsoft Azure, Google, Alibaba, Huawei, and Tencent—PRC firms provided approximately 35% of Germany's cloud computing infrastructure, with the remainder dominated by US providers (Figure 5). While smaller firms were excluded, the researchers noted that these six hyperscalers accounted for most of the global and national public cloud markets examined.[98] This statistic points to a significant presence of PRC firms in Germany's data infrastructure—especially when considered alongside examples of how this cloud infrastructure is used in Germany.

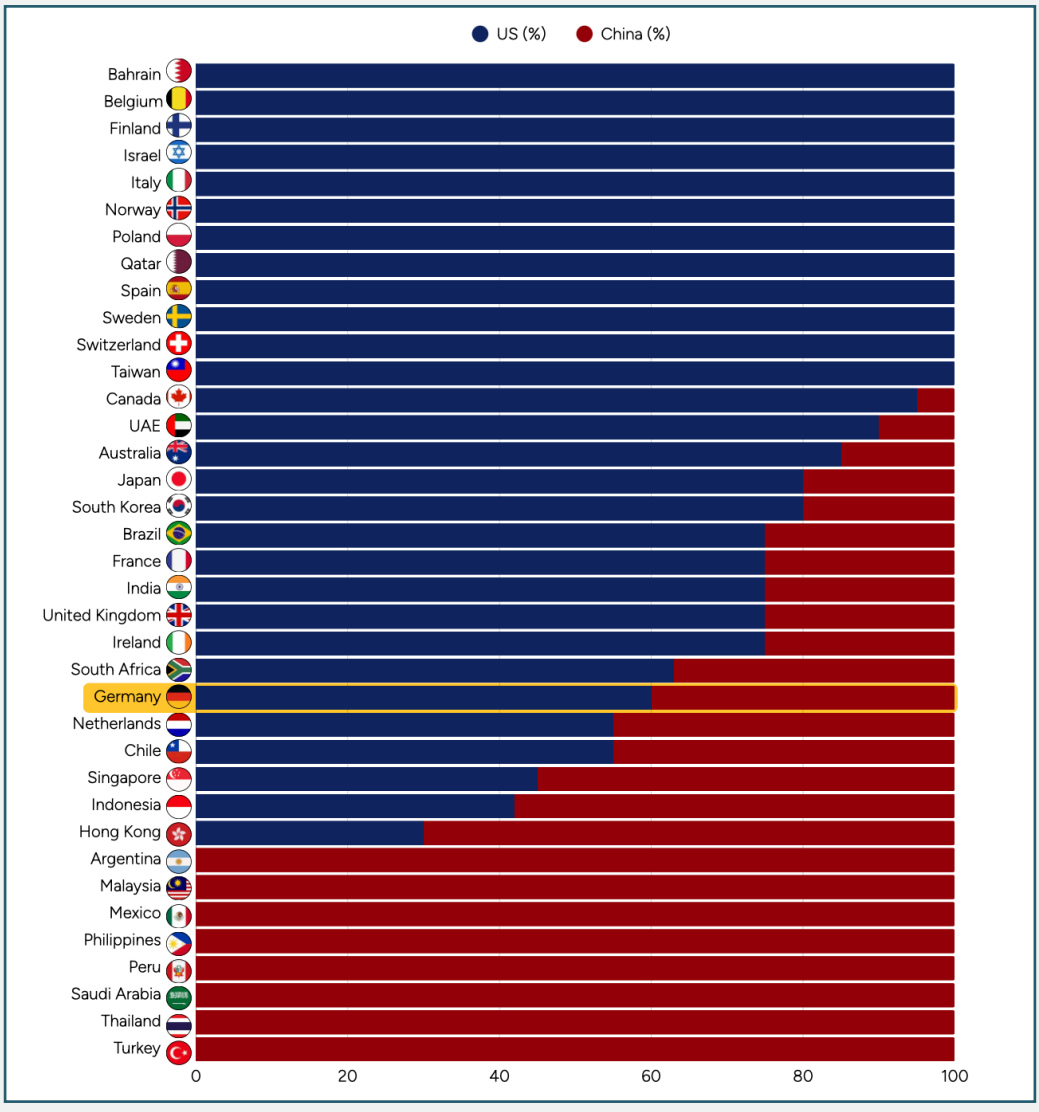


Figure 5: Proportions of US (blue) and PRC (red) cloud availability zones by location.
Source: Lehdonvirta et. al., Review of International Political Economy, 2025

In July 2024, the German non-profit investigative outlet Correctiv reported that the state of North Rhine-Westphalia selected Huawei as the hardware and cloud provider for the DataStorage.nrw project, a large-scale data-storage initiative for the state's universities with applied sciences programs.[99] The project was led by RWTH Aachen University, one of Germany's leading technical universities ranking within the top five in the country in mechanical engineering, mining engineering, materials science, and chemical engineering according to QS World University Rankings in 2024.[100] Correctiv also reported that the University is recognized for its research on dual-use technology.[101] The report drew on an earlier investigation, according to which the university had previously conducted research projects in cooperation with military institutions or military-related institutions from the PRC.[102]

The national security risks posed by espionage through academic research—particularly in the applied sciences and dual-use technologies—should not be underestimated. This concern is especially urgent as Germany shifts toward a pre-war posture, with the potential of finding itself in opposition to the PRC in future geopolitical conflicts. In such a scenario, research security becomes an essential pillar of national security, particularly when scientific advances have both civilian and military applications. Safeguarding these areas is critical to preventing technological advantage from being transferred, exploited, or weaponized by strategic competitors.

Device Layer

While data infrastructure enables companies and individuals to store data on the back end, devices and equipment serve as the front-end collectors and users of this data. The analysis below highlights three sectors, in which growing dependence on the PRC can pose risks to national security and economic competitiveness: electric and connected vehicles, security technology and electronic devices.

Electric and Connected Vehicles

The automotive industry is a cornerstone of Germany's economy. As of 2024, the Federal Statistical Office of Germany reported that motor vehicles accounted for 16.8% of its total exports, making them the country's main export.[103] German automotive companies have long profited from the PRC market and significantly influenced Berlin's policy towards the PRC.[104] In recent years, however, they have faced growing challenges and declining market share in the PRC. In 2023, Volkswagen's PRC sales were down by 9.5% on the previous year, Mercedes-Benz's by 7% and BMW's by 13.4%. Their combined share of the PRC market had shrunk to 18.7%, from a peak of 26.2% in 2019.[105] The longstanding influence of German automakers in Berlin's China policy explains Germany's opposition to EU-led tariffs on PRC-manufactured electric vehicles (EVs). These tariffs followed an EU investigation, that concluded that the PRC's battery electric vehicle (BEV) value chain —BEVs being a subset of EVs— benefits from unfair subsidies, posing a threat of economic injury to EU producers of BEVs.[106] Ahead of EU member states' vote on the tariffs on October 4, 2024, former German Chancellor Olaf Scholz argued that shutting out foreign competition would be counterproductive and that negotiations with the PRC on EVs should continue.[107] While the EU voted in favor of the tariffs, Germany joined Hungary, Malta, Slovenia, and Slovakia in opposing them.[108]

These developments highlight why Germany has been hesitant to follow an approach similar to the United States' "connected vehicles rule", which prohibits the import and sale of certain connected vehicles and key components that are manufactured in, or incorporate hardware, software, or technology sourced from Russia or

China.[109] The German Association of the Automotive Industry (VDA) has gone as far as to criticize proposals for "blanket bans", arguing that Germany's proactive approach to cybersecurity, with rigorous testing and regular security checks, renders such measures unnecessary.[110]

German automakers have struggled to reconcile short-term profitability with long-term competitiveness. As the most auto-dependent of the major EU economies, Germany stands to lose the most if the PRC's industrial policies succeed in transforming it from a net importer of EU automobiles into a serious competitor in the mid-and high-end segments of the European market.[111] As of April 2024, Germany's Federal Statistical Office reported that 40.9% of EVs sold in the country were manufactured in the PRC.This figure includes EVs from PRC-headquartered brands but also those produced in China by internationally headquartered automakers. At the same time, EVs from PRC-headquartered companies are steadily expanding their footprint in Germany (see Figure 6). As of 2023, the PRC's automobile brands made up just 3% of all new car sales in Germany, but their share of BEVs had already reached 8% (see Figure 7).[112] BYD, which recently surpassed Tesla as the world's largest EV seller, is actively working to strengthen its presence in Germany. The company has announced plans to acquire its distributor in Germany, Hedin Electric Mobility (Hedin eMobility), to secure direct control over its sales operations in Germany.[113]

While PRC-manufactured EVs pose competitiveness risks to the German automotive industry, there are also significant national security risks associated with a new generation of cars. Equipped with advanced sensors, these connected vehicles collect extensive data on road conditions and in-cabin activity, potentially capturing sensitive information about individuals' locations, habits, and consumption patterns.[114] Lindsay Gorman's 2020 GMF report on the future internet highlights the "less benign effects" of connected vehicles, where personal data can be misused for malicious purposes with limited control by the individuals to whom the data pertains.[115] In theory,

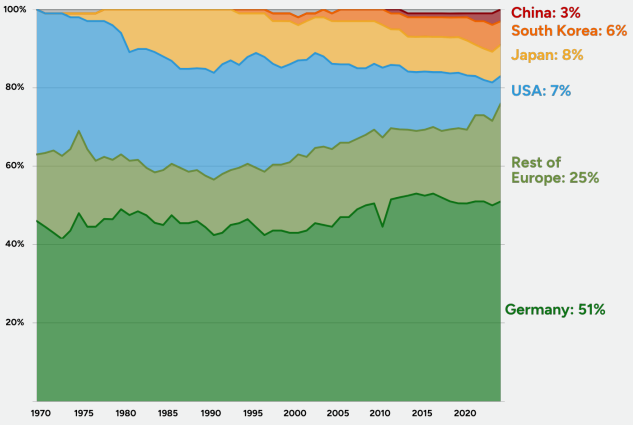


Figure 6: New passenger car registrations in Germany by location of brand ownership
Source: Peter Mock et al., International Council on Clean Transportation, 2024

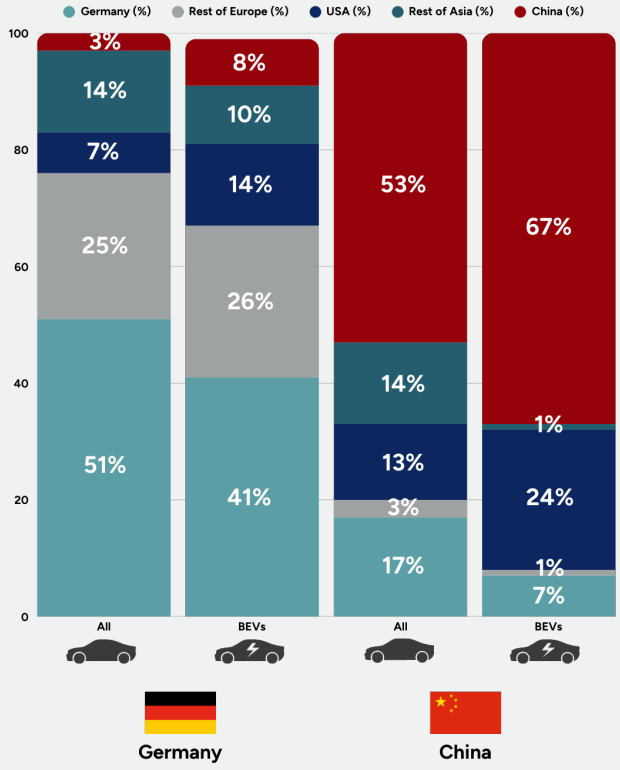


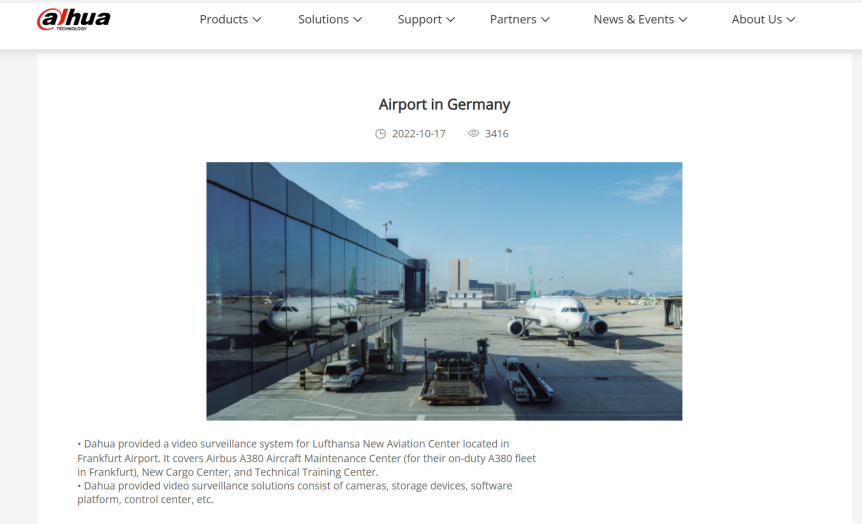
Figure 7: New passenger car registrations in Germany by location of brand ownership, in 2023
Source: Peter Mock et al., International Council on Clean Transportation, 2024

data generated by connected vehicles on German roads could be vulnerable to exploitation for purposes such as espionage or surveillance. This risk is heightened in a pre-war situation, where knowledge of government officials' travel and movement becomes particularly valuable. Despite these risks, German automakers have continued their engagement with PRC entities rather than diversifying away.[116] In 2019, Mercedes-Benz and Geely launched a joint venture to supply, sell, and service future smart vehicles in Europe.[117] More recently, in 2024, Tencent and Bosch's PRC-based units in November 2024 signed Memorandums of Understanding (MoUs) with the aim of exploring opportunities in cloud computing and mapping for autonomous driving, integrating large language models (LLMs) into smart cockpits, and helping PRC-based carmakers venture overseas.[118] In 2024, Volkswagen announced a partnership with Xpeng to jointly develop smart e-cars, and in 2025, BMW revealed plans to integrate AI from PRC startup DeepSeek into its new models in the PRC.[119]

During former Chancellor Scholz's state visit to the PRC in April 2024, both countries renewed their MOU on autonomous vehicles. The government readout stated that the MOU would also "serve to allow concrete progress to be made on the topic of reciprocal data transfer, while respecting national and EU data legislation".[120] A commitment to abiding by European data protection laws, however, does not eliminate the risk of data processing by PRC companies, which are obliged by the PRC to turn over data to the state when requested. This concern is highlighted by recent complaints filed by data protection activist and lawyer Max Schrems' organization Noyb (None of Your Business) against six major PRC companies—TikTok, AliExpress, SHEIN, Temu, WeChat, and Xiaomi—before data protection authorities in Italy, Greece, Belgium, the Netherlands, and Austria, citing alleged violations of Chapter V of the GDPR. According to Noyb, these companies fail to provide adequate safeguards to effectively protect personal data subject to the GDPR from unauthorized access by the PRC government.[121]

Security Technology

According to several market analysis platforms, Hikvision Digital Technology and Dahua Technology are key players in Germany's security technology market.[122] News reports highlight that PRC-manufactured surveillance cameras are installed at key infrastructure sites, such as Frankfurt and Nuremberg rail stations, and the Lufthansa New Aviation Center at Frankfurt Airport (see screeshot below).[123]



Dahua's video surveillance system at Lufthansa's New Aviation Center in Frankfurt Airport is featured as a success story on Dahua's official website
Source: Dahua

Hikvision's website features three "success stories" in Germany. One is the installation of body-temperature screening terminals for the German conference organizer Hotelreservierungs- und Tagungsmanagement in 2020, enabling them to host events during the COVID-19 pandemic.[124] Another one is the installation of an indoor parking guidance system for e-commerce company Otto's headquarters in Hamburg.[125] This system detects available parking spaces using cameras (DS-TCP345D) installed throughout the structure. It relies on AI technology for surveillance of the car park and for streamlining operation.[126] Hikvision's local branch, HikvisionDACH, cultivates its market presence in Germany through outreach and free seminars.[127] Dahua's website also features a 2019 German project on its website, noting its provision of video surveillance technology to German security company "Ihre Sicherheit" in Bielefeld.[128] More recently, in March 2025, Dahua organized "TechDay Events" in Munich, featuring its partners, which include the BSKI Federal Association for the Protection of Critical Infrastructures (BSKI), the German Association for Security Technology (BHE) and the Bavarian Association for Security in the Economy (BSVW).[129]

In October 2019, the US Commerce Department placed Hikvision and Dahua on its Entity List over Beijing's treatment of Uighur Muslims and other predominantly Muslim ethnic minorities.[130] In addition to these human-rights concerns, dependence on PRC-manufactured security devices comes with key security risks. Backdoors can be built into these devices, enabling data theft, cyberattacks, network infiltration, and espionage. In a 2023 report, the Internet Protocol Video Market, a leading authority on physical security technology, exposed vulnerabilities in Hikvision technology, which allowed cybercriminals to take over a user's account simply by listening to network traffic.[131] The report concluded that "Hikvision is helping itself to deceive regulators around the world about its cybersecurity issues by hiding them".[132] Policy experts interviewed for this study highlighted that German government contracts for security technology in public spaces often prioritize the lowest-cost suppliers, which inadvertently favors PRC-manufactured security devices. While cost efficiency drives procurement decisions, it comes at the cost of national security and cybersecurity. As in the case of connected vehicles, these risks are heightened in a pre-war context, where knowledge of strategic locations, civilian traffic, and the movement of government officials becomes strategically valuable for military opponents.

Electronic Devices

Germany's consumer electronics market is among Europe's largest, particularly for IoT devices.[133] According to a 2023 study by economists at Kiel University, Germany's reliance on PRC-manufactured products, particularly on smartphones and laptops, is significant, with import shares of 68% and 80% respectively.[134] The study classifies Germany's dependence on PRC-manufactured laptops as "extreme", though it is only slightly above the global average (see Figure 8).[135] A 2024 Bundesbank study also notes this dependency, pointing to reliance not only on electronic end-products like smartphones but also on intermediate products such as batteries and rare earths.[136] Germany —and the EU more broadly— have recently experienced the consequences of such dependencies when the PRC's Ministry of Commerce

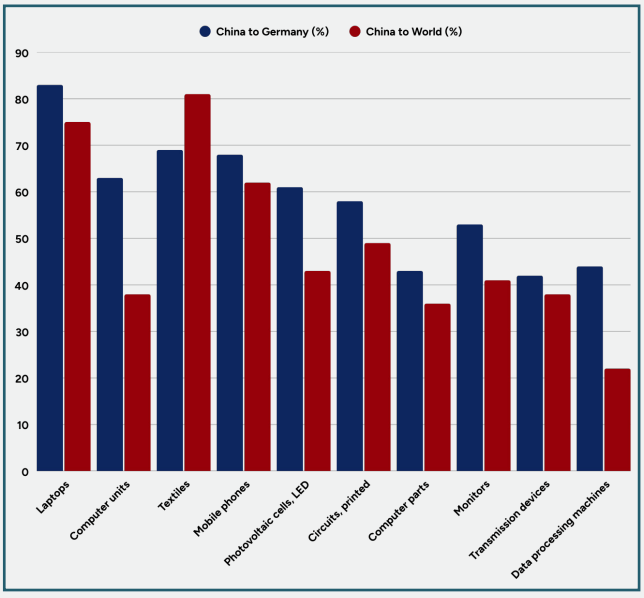


Figure 8: German import dependence on China in selected areas
Source: Adapted from Sandkamp et. al., Kiel Institute for the World Economy, 2023

imposed export restrictions on seven rare earth elements (REEs) and magnets used in the defense, energy, and automotive sectors in response to increased US tariffs on PRC products in April 2025.[137] In a report for the Financial Times, Frank Eckard, CEO of German magnet manufacturer Magnosphere, noted that PRC authorities were requiring companies to disclose confidential information about their products and operations as a condition for export approval. "It's a matter of [China] getting information officially", he remarked, "rather than trying to steal it."[138]

The PRC could similarly exploit these dependencies in the device layer by restricting access to products such as laptops and smartphones, especially if Germany's foreign policy diverges from Beijing's interests, such as on the question of Taiwan. It is important for Germany to diversify its laptop and smartphone imports sooner rather than later, especially since—as the 2023 Kiel study notes— if this supply-chain risk is triggered by a crisis, such as a PRC-Taiwan conflict, many countries will simultaneously seek new suppliers.

More generally, China's footprint in Europe's consumer electronics sector may also be expanding. In July 2025, PRC-based e-commerce giant JD.com launched a takeover bid for German electronics retailer Ceconomy, in what the Financial Times described as potentially one of the largest acquisitions by the PRC in Europe in recent years.[139] JD.com CEO Sandy Xu stated the company's ambition to "build Europe's leading next-generation consumer electronics platform" by combining JD's digital capabilities with Ceconomy's physical retail presence and brand recognition.[140] Xu's vision stands in contrast to Germany and Europe's broader goals of fostering homegrown innovation and competitiveness.

Application Layer

PRC-manufactured technology is present in the German market through physical devices and across a range of technological applications in industries and sectors including robotics, biotechnology, e-finance and e-commerce. The examples below illustrate how PRC entities engage in the application layer of Germany's technology stack, often through strategic partnerships and acquisitions of German firms. In 2018, just three years after the announcement of Made in China 2025, a Bertelsmann Foundation study found that 64% of the German companies sold to the PRC between 2014 and 2017 belonged to the sectors prioritized by the PRC's industrial strategy.[141] Of the ten priority sectors, three were specifically relevant to the application layer: new information technology, high-end numerically controlled machine tools and robots, bio-medicine and high-end medical equipment.[142] In 2025, the PRC has reached many of its targets, and German companies are facing growing competition from their PRC counterparts.[143] A recent survey by the German Economic Institute (IW) found that 60% of German companies focusing on innovation (that is, those conducting research and development) perceive competition with the PRC as a "major" or "rather major" challenge (see Figure 9).[144]

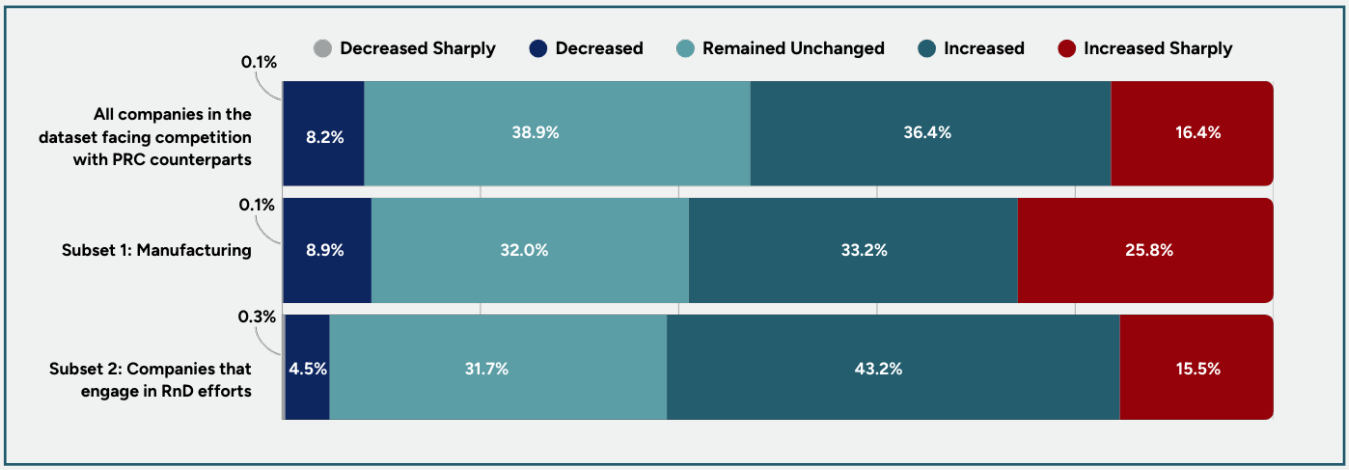


Figure 9: German business responses to competitive pressure from PRC companies
Source: Adapted and translated by GMF Technology from Matthes and Schmitz, Kiel Institute for the World Economy, 2024

Biotechnology

According to OECD indicators, Germany ranks among the top ten countries in terms of the number of active biotechnology firms.[145] Berlin's 2023 National Pharma Strategy, together with the 2024 National Strategy for Gene and Cell Therapies, highlights the government's commitment to positioning the country as a leading hub for pharmaceutical and healthcare innovation.[146] A 2025 study by the European School of Management and Technology and the Bertelsmann Foundation found, however, that Germany is not fully capitalizing on its biotechnology research strengths, leaving substantial economic potential untapped.[147]

As seen in the KLEO connect case discussed above (pages 21-22), German biotech firms often depend on partnerships with PRC counterparts to secure financing. Likewise, as seen in the automotive industry, these collaborations are also crucial for market access in China. For instance, in 2016, Shanghai-headquartered WuXi AppTec acquired Crelux, a German provider of structure-based drug discovery services.[148] Four years later, in 2020, the German subsidiary of another PRC-based biotech company, WuXi Biologics, bought a biologics substance facility at a Wuppertal site belonging to the German multinational Bayer. Bayer's press release noted that WuXi intended to use the facility to manufacture COVID-19 vaccine components and other biologics, with plans for additional investments in process equipment at the site.[149] The company had also invested in a drug product facility in Leverkusen.[150] In May 2025, WuXi Biologics divested from its Leverkusen branch, transferring the German plant to the Tokyo-based CDMO Terumo.[151] According to Ernst & Young's 2024 assessment of Germany's biotechnology industry, PRC companies such as DualityBio and MeiLink Therapeutics are partnering with BioNTech for clinical trials.[152]

A briefing by the Hong Kong-based management consulting firm Dezan Shira & Associates describes PRC financing of Western biotech firms as a "sophisticated" extension of the BRI.[153] In this model, PRC investors gain access to cutting-edge biotech, while Western firms secure capital from the PRC and access to the PRC market.[154] Similar to the 2020 WuXi Biologics-Bayer agreement, in May 2021, BioNTech also forged a partnership with the PRC's Fosun Pharma during the COVID-19 pandemic. Under this partnership, the companies conducted joint clinical trials of BioNTech's COVID-19 vaccine in the PRC. BioNTech contributed its proprietary mRNA technology, while Fosun provided access to the PRC market.[155] BioNTech has also secured partnerships on cancer treatments with PRC firms such as AcroImmune Group, Duality Biologics, Doer Biologics and Biotheus.[156]

While these partnerships may be motivated by a shared goal of addressing major health challenges, the German government and industry leaders must remain vigilant to the long-term risks they pose—particularly through potential intellectual property theft—, which could undermine the competitiveness of Germany's biotech sector, a key national asset.

In addition to competitiveness risks, the data security risks of these partnerships should not be underestimated. In June 2024, MGI Tech—a genomic sequencing firm and spin-off of BGI Group—opened its European headquarters in Berlin, featuring advanced capabilities in DNA sequencing, cell omics, and spatial omics. [157] This development is particularly concerning given that, in 2023, several BGI-affiliated entities were added to the US Entity List on the grounds that their genetic data activities could support surveillance and military applications by the PRC government.[158] Furthermore, WuXi AppTec, WuXi Biologics, and BGI are on the list of entities included in the Biosecure Act, passed by the US House of Representatives in September 2024, which seeks to limit business dealings with certain PRC biotech firms on security grounds.[159] The fact that PRC ambitions include indigenization capabilities in strategic fields such as biotechnology, should lead German players to consider the long-term risks of these partnerships and dependencies.

Robotics

Germany remains the fifth-largest robotics market globally and the leader within Europe, according to its economic development agency, Germany Trade & Invest (GTAI).[160] As of 2024, however, the PRC has overtaken Germany in industrial robot adoption, reaching a robot density of 470 units per 10,000 employees—compared to Germany's 415.[161] Germany's long-standing advantage in the sector is being challenged—not only by the PRC's rapid adoption of robotics, but also by the acquisition of German robotics firms by PRC companies.

A well-known example is the 2016 acquisition of leading German industrial robotics manufacturer KUKA by the PRC-headquartered appliance giant Midea, in a deal valued at approximately €4.66 billion.[162] The transaction sparked strategic concern in Berlin over foreign access to critical technologies and led the German government to tighten its foreign investment screening rules. The revised regulations lowered the threshold for reviewing and potentially blocking non-European acquisitions of German companies that operate in "sensitive security areas" from 25% foreign ownership to 10%.[163] These "sensitive areas" include the development and manufacturing of weapons and other critical military technologies, specialized engines and gearboxes for armored vehicles, and IT-security products used for processing classified government information. Similar rules apply to companies operating high-grade earth remote sensing systems.

For all other sectors, however, the regulations stipulate that the standard investment screening threshold of 25% remains in effect.[164] This means that foreign entities can still acquire up to a 25% stake in German firms operating in critical and emerging technology sectors—such as robotics—without triggering a special investment review. A notable example occurred in 2019, when Shenzhen-based Nanjing Estun Automation Technology Co. acquired Carl Cloos Schweißtechnik GmbH, a manufacturer of welding technology for both manual and automated applications, for €196 million—despite heightened scrutiny following the KUKA acquisition.[165] Founded in 1919, Cloos was established more than seven decades before Estun.[166] The acquisition of a long-established German technology firm by a relatively young foreign company reflects a development with implications for future competitiveness in German robotics—one that policymakers need to scrutinize more closely.

E-Commerce and E-Finance

According to the most recent assessment by the US International Trade Administration (ITA), Germany has one of the largest e-commerce markets in Europe.[167] From 2017 to 2022, business to consumer (B2C) e-commerce grew by 69%—from €58.5 billion to €99.1 billion – with the COVID-19 pandemic contributing significantly to this surge.[168] PRC-developed e-commerce platforms have also benefited from this trend. Temu achieved nearly $750 million in sales within its first year after launching in 2022, when it surged to the top spot in downloads, making it the 13th-largest marketplace in Germany.[169] In addition to Temu, Nanjing-founded e-commerce fast-fashion platform Shein more than doubled its order frequency from 10% in 2023 to 22% in the first quarter of 2024 in the country.[170]

Although e-commerce platforms may seem benign, a report by the US-China Economic and Security Review Commission argues that PRC-developed e-commerce platforms like Shein and Temu outpace competitors through controversial—and often illegal—business practices.[171] The report notes that Shein, for instance, has failed to disclose its use of cotton sourced from Xinjiang, a violation of the Uyghur Forced Labor Prevention Act in the United States.[172] Recognizing the risks posed by certain e-commerce platforms that violate EU standards for product safety, environmental protection, health, intellectual property, and consumer protection, the German government called for stricter legal enforcement of regulations in this sector at both the national and EU levels in September 2024.[173] While the government's risk assessment rightly emphasizes consumer protection and market fairness, it fails to mention—at least publicly—the data protection and national security risks these platforms may present.

The US-China Economic Security Review Commission report highlights that while Shein's business model relies heavily on collecting and analyzing user data, it has struggled to safeguard that data.[174] In 2022, the state of New York fined Shein's parent company for mishandling credit card and personal information after a 2018 cyberattack had compromised the data of 39 million users, including 800,000 in New York. [175] Temu's business practices raise similar concerns. Operated by PDD Holdings—the company behind the PRC-developed platform Pinduoduo—Temu has benefited from a data-driven, low-cost model.[176] In April 2023, CNN reported that multiple cybersecurity teams had discovered sophisticated malware embedded in the Pinduoduo Android app.[177] This malware was capable of bypassing user permissions, accessing private messages, modifying settings, viewing data from other apps, and even preventing uninstallation.[178]

These data protection concerns are amplified by the PRC's 2017 National Intelligence Law, which, as mentioned above, compels companies to grant state authorities access to data upon request. This concern also extends to PRC-developed e-finance and payments applications, such as Alipay and WeChat Pay. These e-finance services have become embedded in global payment ecosystems, including platforms like Stripe, facilitating their growing presence in markets such as Germany.[179]

WeChat Pay, operated by tech giant Tencent and integrated into the widely used instant messaging app WeChat, is particularly noteworthy. Unlike many Western counterparts that rely on end-to-end encryption (E2EE), Tencent uses the secure sockets layer (SSL) to secure data transmission, and stores and decrypts user data (including chat data) on its servers. While SSL ensures data is secured during transit, unlike E2EE, it does not prevent service providers from potentially accessing data once it reaches their servers.[180] This applies to all users globally, whether they use the PRC or international version of the app. Alipay, WeChat Pay's PRC-based competitor, has also expanded across Europe. In Germany, it served as the official payment partner and sponsor of UEFA Euro

2024, increasing its visibility.[181] With reference to e-finance applications, Elisabeth Braw, senior fellow at the Scowcroft Center for Strategy and Security at the Atlantic Council, has pointed out that "a government official's daily life can be tracked using his or her Alipay transactions".[182] As discussed in the previous section, location data can prove strategically valuable to military opponents during periods of heightened geopolitical tension.

Governance Layer

Germany's technology governance emphasizes data protection, cybersecurity, and ethical AI development, supported by strong regulatory oversight. It is shaped by EU-wide regulations such as the GDPR and the AI Act. In promoting an open internet, Germany and the EU are, in principle diametrically opposed to China's authoritarian approach, which is built on data localization, censorship and surveillance of its citizens. And yet, German and EU technology governance has blind spots when it comes to protecting its citizens and businesses from the risks of data transfers to China. For instance, the EU has only recently opened formal proceedings against TikTok.[183] As discussed in the device and application layers, Germany has also been slow to address the security and data protection risks posed by technology manufactured or developed in the PRC.[184] Cybersecurity poses a similarly pressing challenge. A 2024 survey by Germany's IT sector trade association Bitkom, found that 80% of German businesses had experienced data theft, industrial espionage, or sabotage within the past year. Of these incidents, 45% were attributed to the PRC and 39% to Russia.[185] These mounting threats highlight the urgency for Germany to transpose the EU's revised Cybersecurity Directive (NIS2) into national law—a deadline it missed in October 2024. NIS2 establishes a harmonized legal framework to bolster cybersecurity across 18 critical sectors and requires member states to adopt national strategies, while ensuring coordinated, cross-border response and enforcement efforts.[186]

Within the governance layer, PRC's influence is exerted subtly—through partnership agreements and structured dialogue formats. The area of technical standards has emerged as a significant domain of cooperation between Germany and the PRC. Through the Sino-German Industrie 4.0 Cooperation framework (Figure 10), both countries have developed a format for collaborative standard-setting.[187] Technical standards determine how technologies are designed and how they interoperate, shaping market dynamics and embedding strategic values into digital infrastructure. Those who lead in setting global standards hold substantial economic and political power.[188] Recognizing this, the PRC has moved rapidly to close the gap with Western countries—and views Germany as a pivotal partner in advancing its standardization goals.[189]

The groundwork for the Sino-German Industrie 4.0 Cooperation partnership was laid during President Xi Jinping's 2014 state visit to Germany when both sides established a joint action plan on standardization, industry collaboration and research and science partnerships (Figure 11).[190] In 2015, both countries signed an MoU to promote mutual understanding and facilitate dialogue among government, industry, and experts at all levels.[191] This enabled experts from both countries—across industry and academia—to

Figure 10: The Three Pillars of Sino-German Industrie 4.0 Cooperation
Source: German Federal Ministry for Economic Affairs and Energy and Federal Ministry of Education, Research, and Technology

collaborate on joint policy recommendations that would guide political and industrial dialogues.[192] Key areas of focus included the application of AI in manufacturing, and the establishment of standards to integrate humans, machines, and products within global ecosystems.[193]

While Germany sees its partnership with the PRC as reinforcing its global standards influence and securing market access, key asymmetries underpin the relationship. In a 2022 study, Humboldt University scholars Daniel Fuchs and Sara Eaton highlighted the PRC-based representatives in the Sino-German partnership on technical standardization includes experts who are mostly from the Standardization Administration of China and Ministry of Industry and Information Technology (MIIT)-affiliated research institutes.[194] The PRC's state-coordinated approach contrasts with Germany's decentralized approach to standard-setting, which primarily includes standardization experts from companies with business interests in the PRC, alongside representatives from business associations, universities, and German standards bodies, the German Institute for Standardization (DIN) and German Commission for Electrical, Electronic & Information Technologies (DKE).[195] The study found that German actors often prioritized access to the PRC market—even while acknowledging the risks of transferring technology and know-how to the PRC.[196] This raises questions about whether Germany's approach to standard-setting fails to account for the PRC's state-coordinated model and strategic interests—a concern also expressed by Lindsay Gorman in her 2020 report on the future internet.[197]

Gorman's report further highlighted the national and economic security risks associated with the PRC's global ambitions in technical standard-setting.[198] She argues that through its state-coordinated approach, the PRC can leverage its DSR initiative to build de facto technical standards on the ground, and increase international support for them.[199] As a result, this strategy enhances PRC companies' influence in international organizations, and it offers financial gains through securing patents, which generate considerable royalties.[200] With this in mind, German policymakers must consider that the PRC's rise as a standard-setting power could come at the expense of Germany's historical influence in this domain. This strategic calculation must also account for cybersecurity risks, as actors who shape technical standards also have access to deeper knowledge of a standard's technology, including potential vulnerabilities.[201] Such control could pose a serious threat in the event of a geopolitical conflict—particularly if Germany finds itself in strategic opposition to the PRC.

Conclusion and Key Findings:

Germany's new government under Chancellor Friedrich Merz—in office since May 7, 2025—will play a critical role in redefining Germany's international position amid a shifting global order and waning US security guarantees. Central to this is a clear-eyed assessment of Germany's relationship with the PRC. The government should build on the momentum of the 2023 China Strategy and strengthen it with a focus on technology and strategic resilience. This report argues that the de-risking calculus of Berlin's China strategy should be firmly embedded in all five layers of Germany's technology stack. In particular, German policymakers should pay attention to the network infrastructure layer, as it is foundational and serves as the basis for the rest of country's technology stack. Overall, the analysis highlights the critical need to broaden trustworthiness assessments to encompass the entire technology stack. The key findings and policy recommendations are listed below.

Key Findings:

1. **PRC vendors remain embedded in Germany's telecom infrastructure, raising long-term security concerns for both 5G and 6G networks.** Germany has not fully eliminated PRC vendors from its 5G networks. Telecom operators may retain all Huawei equipment except for the configuration management system—a minor part of the radio access network (RAN)—,which must be replaced by 2029. This raises concerns that PRC vendors could still exploit their remaining presence in Germany's 5G infrastructure for espionage or disruption through malicious software. Looking ahead, untrusted vendors may continue to be part of Germany's telecom future. Huawei, ZTE, and China Mobile are participating in public discussions hosted by partners of the federally funded 6G-ANNA project, highlighting potential risks in the upcoming 6G rollout.

2. **Amid high strategic vulnerability, PRC-based companies are partners in new high-capacity undersea cables linking Germany and Europe to Asia and Africa.** Germany's network security is intertwined with that of its European neighbors. PRC-based companies like China Telcom, China Unicom, China Mobile, and Hengtong—many of whom are blacklisted by Washington—are partners in new high-capacity undersea cables connecting Germany and Europe to Asia and Africa, such as the PEACE or 2Africa cables. These high-capacity transmission cables could be primary targets for surveillance, espionage and sabotage in case of a conflict.

3. **PRC firms such as Huawei, Alibaba and Tencent provide approximately 35% of Germany's cloud computing infrastructure.** This significant presence raises concerns about data security risks and dependencies that can be weaponized. These risks are amplified in critical use cases—such as data storage for university research in applied sciences—where sensitive intellectual property could be vulnerable to theft or exploitation for military purposes by the PRC.

4. **Despite planned EU tariffs on electric vehicle imports in 2024, Germany and China continue to deepen cooperation on electric and connected driving.** Recent deals—such as the Tencent-Bosch partnership on cloud computing and smart driving, and BMW's AI integration plans with DeepSeek—highlight German firms' continued "risky bet" on the PRC market. This strategy not only jeopardizes the future competitiveness of one of Germany's key export sectors but also raises significant data security concerns in the connected vehicle ecosystem.

5. **Despite Germany's 2018 revisions to foreign investment screening rules, foreign entities can still acquire up to a 25% stake in German firms in critical and emerging technology sectors without triggering a special investment review.** Notably, the list of "sensitive areas" requiring such reviews excludes sectors like biotechnology and robotics—key targets for PRC firms pursuing strategic partnerships and acquisitions in Germany. This poses long-term risks to German competitiveness and data security in these sectors.

6. **Through its Sino-German Industrie 4.0 Cooperation, Germany has boosted China's expertise and influence in global technical standard-setting.** This framework, established through cooperation between the two countries on technical standardization for Industrie 4.0, has facilitated partnerships between businesses, industry, and academia over several years. It offers standard-setters from the PRC opportunities to learn the intricacies of global technical standard-setting from Germany—a global leader in this area. This collaboration provides China with long-term strategic leverage, creating a pathway for aligning global norms with its technological and economic priorities.

Policy Recommendations:

To German Policymakers:

The National Security Council under the Federal Chancellery should:

1. **Establish a structured coordination mechanism on Critical and Emerging Technologies (CETs)**

   The NSC should create a cross-ministerial framework linking information on security, foreign affairs, economic, and research ministries to ensure a national approach to CETs. The mechanism should align policies on tech regulation, supply chain security, digitalization, and dual-use technologies. The CET list from the 2024 study by the Council for Technological Sovereignty—covering AI, quantum, biotech, semiconductors, ICT, and Industry 4.0—provides a solid foundation for prioritization.

2. **Establish a high-level technology advisory panel to brief the NSC**

   The NSC should form a standing panel of independent technology, geopolitical, and economic security experts to provide regular, forward-looking briefings to the NSC. This panel should offer

insights into emerging risks, global tech trends, and supply-chain vulnerabilities in the list of CETs mentioned above.

3. **Conduct a review of the Sino-German Industrie 4.0 Cooperation partnership using the tech-stack framework**

   Working in coordination with the Federal Foreign Office (AA) on an updated China strategy, the NSC should lead a comprehensive review of the Sino-German Industrie 4.0 Cooperation partnership through the lens of the tech stack. This review should assess the dialogue's impact on Germany's national security, competitiveness, and industrial resilience. The findings should guide the articulation of a clear, forward-looking vision that defines strategic objectives and sets national and geopolitical priorities.

The Federal Office for Information Security (BSI) should:

4. **Lead EU efforts on data security and promote trusted national providers**

   The BSI should drive EU coordination on data security by defining categories of high-risk and sensitive data—such as national security and government data—that must not be processed on untrusted foreign systems. Germany should promote the development and adoption of trusted national and European cloud and data infrastructure providers to reduce strategic dependencies.

The Federal Ministry for Digitalization and Government Modernization (BMDS) should:

5. **Establish a strategic foresight unit for crises triggered by a coordinated cyber-physical attack across Germany's technology stack**

   The BMDS should create a strategic foresight unit tasked with enhancing national resilience and decision-making capabilities in scenarios involving large-scale, coordinated cyber and technological attacks targeting multiple layers of Germany's technology stack. The unit should develop, maintain, and simulate scenarios involving cascading failures across the technology stack—spanning both physical infrastructure sabotage and cyberattacks. These findings should be shared with the NSC.

6. **Strengthen data security through risk-based toolbox for digitalization**

   The BMDS should launch a formal consultation with the BSI and the Federal Ministry of the Interior (BMI) to assess and manage data security risks and treat them as a national security issue.

   - This effort should include identifying high-risk and sensitive data—such as government, national security, medical data—that must not be stored or processed within data infrastructure hosted on untrusted platforms, particularly those owned or operated by PRC-linked firms. Based on this classification, the ministry should set clear restrictions on permissible data usage across such platforms.

- To ensure consistent implementation, a standardized risk assessment toolbox should be developed to guide German companies, research institutions and individuals in securing their digital infrastructure. Initially, this toolbox can be introduced as a voluntary measure, with the option to transition into a mandatory requirement if uptake is insufficient or emerging risks demand stricter compliance.

- This complements the Data Protection Impact Assessment (DPIA) requirement under the GDPR, which applies when a project's data processing is likely to pose a high risk to individuals' rights and freedoms. Since the responsibility for the DPIA lies with the individual or company processing data, the toolbox serves as an initial step to clarify any potential ambiguity regarding what constitutes personal or sensitive data.

7. **Guide the secure digital transformation for German SMEs**

   The BMDS should support SMEs in their digitalization efforts by creating new online platforms or updating existing ones such as the "Digital Jetzt" platform. These resources should offer information on funding and grants, regulatory compliance guidance, risk assessment toolkits, tailored training programs, and a curated marketplace of trusted digital tools, data centers, and cloud service providers.

The Federal Foreign Office (AA) should:

8. **Update Germany's China strategy with a robust technology de-risking component**

   Germany's China strategy must be updated to include a solid technology focus that addresses systemic dependencies and emerging risks across the entire technology stack as illustrated in this analysis. It should outline specific de-risking measures including supplier diversification, investment screening, export controls on dual-use technologies, and stricter procurement standards for public security infrastructure. It should also include clear guidelines for technological cooperation with the PRC, based on transparency, reciprocity, and national security safeguards. The technology stack could also be integrated into Germany's updated China strategy as a framework for its de-risking objectives—helping to map critical dependencies, assess systemic vulnerabilities, and steer investment toward secure and resilient technological infrastructure.

The German Navy should:

9. **Strengthen security of German and European undersea internet infrastructure**

   - Building on its reaffirmed commitment to underwater security in the 2035+ Maritime Strategy, the German Navy should incorporate sabotage stress tests into Baltic Sea exercises—such as the Northern Coast (NoCo) manoeuvre with NATO allies—to strengthen preparedness against accidents or attacks on undersea cables.

   - Given the German Navy's recent assumption of the role of Commander Task Force (CTF) Baltic—a national headquarters with multinational participation established by NATO—

Germany should share insights and lessons learned from this effort with European partners for the CTF Mediterranean. The focus should be on securing ports that host key landing stations for high-capacity transmission cables, such as Marseille (France) and Carcavelos (Portugal).

The Federal Ministry for Research, Technology, and Space (BMFTR) should:

10. Enhance research security in emerging and dual-use technologies

The BMFTR should establish a platform dedicated to research security that issues guidelines and help the scientific community conduct risk assessments on current and future international research collaborations in emerging—especially dual-use—technologies and applied sciences.

11. Support German leadership in European satellite internet through DLR

In coordination with the German Aerospace Center (DLR), the BMFTR should direct seed funding to German startups and research institutions developing satellite internet technologies—reducing dependence on PRC-based investors and building European satellite competitors. This early support would position these companies to secure scale-up funding through programs such as the European Space Agency's Scale Up initiative.

The Federal Ministry for Economic Affairs and Energy (BMWE) should:

12. Enhance public security by phasing out PRC-made surveillance technologies

The BMWE should initiate a debate in the Bundestag with the goal of banning and replacing PRC-manufactured security technologies in public spaces across Germany, pursuant to the Foreign Trade and Payments Act (Außenwirtschaftsgesetz, AWG), on the grounds that such technologies pose a sufficiently serious threat to national security.

13. Reform public procurement standards for security technologies

The BMWE should initiate a debate in the Bundestag on updating public procurement law to prioritize vendor trustworthiness, data protection, and supply chain transparency—not just price—when awarding government contracts for security-related technologies.

14. Strengthen investment screening to safeguard CETs

The BMWE should initiate a debate in the Bundestag on expanding Germany's investment-screening rules, which are currently applied to sensitive security sectors such as defense manufacturers, IT security products for classified government use, and high-grade earth remote sensing systems. Updated rules should include core products and technologies fundamental to CETs listed in the first recommendation in light of their strategic importance to national security and economic competitiveness.

EU Policymakers should:

15. **Extend the 2023 technology-related risk-assessment recommendations to member states**

    Under its Vice President for Tech Sovereignty, Security, and Democracy Henna Virkkunen, the European Commission should use the tech-stack framework to broaden the 2023 risk-assessment recommendations to member states. These recommendations call on the Commission and member states to initiate collective risk assessments for advanced semiconductors, AI, quantum technologies, and biotechnologies. The tech-stack approach can inform de-risking priorities by accounting for the layering of technologies and the resulting dependencies.

16. **Publish a third progress report on the implementation of the 5G Cybersecurity Toolbox and reinforce member state compliance**

    Given that the last progress report was released in 2023, a new assessment is now warranted. The Commission should evaluate the current state of implementation across member states—with particular attention to Germany's progress—and actively encourage full compliance to ensure the security of its network infrastructure.

17. **Urge Germany to transpose the EU's NIS 2 Directive into national law**

    Given the change of government in 2025, Germany has delayed transposing the EU's NIS 2 Directive, which is critical for enhancing coordination among member states on cybersecurity. The directive establishes robust protocols for risk management, incident reporting and response, governance, and data protection. Given the increasing scale and sophistication of cyberattacks targeting Germany—particularly from Russia and the PRC—it is essential that the EU Agency for Cybersecurity (ENISA) presses Germany to adopt the directive into national law without further delay. Doing so will strengthen national cybersecurity resilience and facilitate more effective cross-border collaboration and enforcement within the EU.

18. **Reduce EU dependence on PRC cable companies for undersea network infrastructure**

    The European Commission should extend the risk-focused approach of the 5G toolbox to include the broader network infrastructure layer. Companies like HMN Tech should be phased out and eventually prohibited from owning or operating cable infrastructure in the EU.

19. **Maintain de-risking from PRC dependence as a priority in Europea's electric and connected vehicles sector**

    The Commission's Strategic Dialogue on the Future of the European Automotive Industry, launched in 2025 and informed by the insights of working groups led by Commissioners Šefčovič, Hoekstra, Séjourné, Virkkunen, Mînzatu, and Tzitzikostas, should address the risks of overreliance on the PRC. The dialogue should aim to align member states and industry leaders on strategies to mitigate these dependencies.

20. Diversify IoT device imports via Indo-Pacific Free Trade Agreements (FTAs)

The EU Commission's Directorate-General for Trade (DG TRADE) should leverage existing and forthcoming FTAs to diversify imports of smartphones, laptops, and related components away from China, prioritizing Indo-Pacific partners such as South Korea, Japan, Vietnam, and India.

The United States should:

21. Encourage Germany to support the creation of an EU-level entity-list mechanism under the Common Security and Foreign Policy framework

The State Department, through relevant bureaus like the Bureau of European and Eurasian Affairs should coordinate with experts from Department of Commerce's Bureau of Industry and Security (BIS) to encourage the Council of the European Union to develop a trade restriction tool analogous to the US Entity List, aimed at enhancing transatlantic coordination in addressing challenges posed by PRC technology. Such a mechanism would strengthen the EU's ability to respond to security and economic risks linked to sensitive tech transfers.

22. Engage and coordinate with the EU as a whole—in addition to coordinating with individual member states like Germany—to develop a joint response to the PRC's expanding global technology footprint.

The State Department, through relevant bureaus like the Bureau of European and Eurasian Affairs and the Bureau of Cyberspace and Digital Policy, and the Department of Commerce should coordinate with the EU as a whole—in addition to coordinating with individual member states like Germany to develop a joint response to the PRC's expanding global technology footprint especially since the EU has taken clear steps to address the risks posed by PRC technology—such as imposing tariffs on electric vehicles and launching investigations into PRC subsidies for wind turbines, irregularities in public procurement of medical devices, and the practices of fast-fashion companies. These actions demonstrate that in addition to member states, the EU is well positioned to lead a cohesive and strategic response to the challenges presented by PRC technological influence.

23. Preserve and strengthen transatlantic coordination mechanisms on export controls, investment screening, and sanctions

The State Department and the National Security Council should draw from relevant expertise from bodies such as BIS and the Federal Communications Commission (FCC) to maintain close coordination with Germany and the EU to counter the technological threats posed by the PRC, including on export restrictions and coercive sanctions. Particular attention should be given to data-related technologies, including surveillance systems, cloud infrastructure, and IoT devices.

24. Preserve and strengthen transatlantic coordination mechanisms on technology standardization

The State Department and Department of Commerce should work with Berlin and Brussels to counter the PRC's growing influence in global technology standard-setting. Sustaining mechanisms like the TTC Working Group on Technology Standards is essential to promote democratic values and prevent the adoption of global standards that legitimize and favor authoritarian technology governance.

25. Promote bilateral exchange on research security best practices

To strengthen the integrity and resilience of research ecosystems, the State Department should coordinate with the National Science Foundation to establish a structured dialogue with German counterparts focused on research security. This initiative should facilitate the exchange of best practices, risk mitigation strategies, and policy frameworks to address shared challenges such as foreign interference, intellectual property theft, and the protection of sensitive technologies.

Endnotes

[1] Federal Ministry of Research, Technology and Space, "Technological Sovereignty", https://www.bmftr.bund.de/EN/Research/EmergingTechnologies/TechnologicalSovereignty/technologicalsovereignty_node.html

[2] Coalition agreement between CDU, CSU, and SPD, "Responsibility for Germany", April 9, 2025. https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf

[3] Paul Kirvan, Margie Semilof and James Montgomery, "What is a software stack?", TechTarget, September 2024. https://www.techtarget.com/searchapparchitecture/definition/software-stack

[4] See, for example, the concept of "Eurostack" as a European industrial policy initiative bringing together tech, governance and funding for Europe-focused investment with the goal to build and adopt a suite of digital infrastructures from connectivity to cloud computing, AI and digital platforms. Eurostack, "Why, What, How", https://euro-stack.eu/; See also the concept of "IndiaStack" established in India referring to open APIs on which digital services can be built. IndiaStack, "India Stack is", https://indiastack.org/

[5] Lindsay Gorman, "A Future Internet for Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything", The German Marshall Fund of the US, October 27, 2020. https://securingdemocracy.gmfus.org/future-internet/

[6] Bryce Barros, Nathan Kohlenberg and Etienne Soula, "China and the Digital Information Stack in the Global South - Alliance For Securing Democracy", The German Marshall Fund of the US, June 15, 2022. China and the Digital Information Stack in the Global South – Alliance For Securing Democracy

[7] Tobias Bunde, "America First, Germany Alone? Germany's Role in a Changing Global Order", German Marshall Fund of the United States, February 2025. https://www.gmfus.org/sites/default/files/2025-02/Germanys%20Role%20in%20a%20Changing%20Global%20Order_digital_0.pdf; See: Hugo Meijer and Stephen G. Brooks, "Illusions of Autonomy: Why Europe Cannot Provide for Its Security If the United States Pulls Back", International Security, 2021. https://direct.mit.edu/isec/article/45/4/7/100571/Illusions-of-Autonomy-Why-Europe-Cannot-Provide

[8] Dan Sabbagh, "US no longer 'primarily focused' on Europe's security, says Pete Hegseth", The Guardian, February 12, 2025. https://www.theguardian.com/us-news/2025/feb/12/us-no-longer-primarily-focused-on-europes-security-says-pete-hegseth

[9] Timothy Jones, "Germany neither at peace nor war with Russia: defense chief", Deutsche Welle, April 8, 2025. https://www.dw.com/en/germany-neither-at-peace-nor-war-with-russia-defense-chief/a-72172870

[10] Anthony J. Cotton, "Statement of General Anthony J, Cotton before the subcommittee on strategic forces, senate armed services committee", United States Strategic Command, March 26, 2025. testimony_of_general_anthony_jcotton2.pdf

[11] Ministry of Foreign Affairs, The People's Republic of China, "Member of the Political Bureau of the CPC Central Committee and Foreign Minister Wang Yi Meets the Press", March 7, 2025. https://www.mfa.gov.cn/eng/wjbzhd/202503/t20250307_11571025.html

[12] Scott Kennedy, "Made in China 2025", Centre for Strategic and International Studies, June 1, 2015. https://www.csis.org/analysis/made-china-2025; Jeroen Groenewegen-Lau, "Whole-of-nation innovation: Does China's socialist system give it an edge in science and technology?", MERICS, March 5, 2024. https://merics.org/en/report/whole-nation-innovation-does-chinas-socialist-system-give-it-edge-science-and-technology

[13] David Gordon and Meia Nouwens, "The Digital Silk Road: Introduction", The International Institute for Strategic Studies, December 6, 2022. Introduction | The Digital Silk Road: China's Technological Rise and the Geopolitics of Cyberspace

[14] Federal Foreign Office, „Strategy on China of the Government of the Federal Republic of Germany", Auswärtiges Amt, July 2023. https://www.auswaertiges-amt.de/resource/blob/2608580/49d50fecc479304c3da2e2079c55e106/china-strategie-en-data.pdf

[15] Federal Foreign Office, "Strategy on China of the Government of the Federal Republic of Germany"

[16] Bernhard Bartsch and Claudia Wessling, "Germany's new China strategy: Ambitious language, ambiguous course", Merics, July 27, 2023. https://merics.org/en/report/germanys-new-china-strategy-ambitious-language-ambiguous-course

[17] Financial Times, "Germany orders ban on Chinese companies from its 5G network", July 11, 2024. https://www.ft.com/content/aacd77a2-048a-489e-98f8-b9f436e448b6

[18] Lindsay Gorman, "A Future Internet for Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything"; Bryce Barros, Nathan Kohlenberg and Etienne Soula, "China and the Digital Information Stack in the Global South – Alliance For Securing Democracy"

[19] Federal Ministry for Digital and Transport (BMDV), "Strategy for International Digital Policy of the Federal Government", February 7, 2024. https://bmdv.bund.de/SharedDocs/EN/Documents/Press/pm004-internationale-digitalpolitik-en.pdf?__blob=publicationFile

[20] Lindsay Gorman, "A Future Internet for Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything"

[21] China Academy of Information Communications and Technology (CAICT), "White Paper on China International Optical Cable Connection", 2018. http://www.caict.ac.cn/english/research/whitepapers/202003/P020200327550620516330.pdf

[22] 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, 24, 2023. https://scholarsmine.mst.edu/cgi/viewcontent.cgi?article=1211&context=his_polsci_facwork

[23] Federal Ministry of the Interior and Community, "Greater security and technological sovereignty for the German 5G mobile network: The Federal Government concludes contracts with telecommunications companies", July 11, 2024. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2024/07/5g-en.html

[24] Hans von der Burchard, Mathieu Pollet and Jürgen Klöckner, "Germany goes soft on China, dragging out Huawei ban until 2029," July 10, 2025. https://www.politico.eu/article/germany-china-huawei-ban-2029-5g-networks-government-greens-lawmaker-4g-strand/; Tagesschau, "Federal government bans Huawei components in 5G mobile networks," 11 July, 2024. https://www.tagesschau.de/inland/huawei-5g-verboten-100.html; Reinhard Bütikofer, "Germany's Embarrassing Dance Around China's Huawei," The Center for European Policy Analysis, July 7, 2024. https://cepa.org/article/germanys-embarrassing-dance-around-chinas-huawei/

[25] Iain Morris, "The kill Huawei mission is being jeopardized by Germany", October 25, 2024; https://www.lightreading.com/5g/the-kill-huawei-mission-is-being-jeopardized-by-germany; Iain Morris, "Deutsche Telekom boss caught between a Trump and a Huawei", April 17, 2025. https://www.lightreading.com/5g/deutsche-telekom-boss-caught-between-a-trump-and-a-huawei

[26] Ibid.

[27] Strand Consult, "The Market for 5G RAN in 2024: Share of Chinese and non-Chinese Vendors in Europe", January 10, 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/

[28] Hans von der Burchard, Mathieu Pollet and Jürgen Klöckner, "Germany goes soft on China, dragging out Huawei ban until 2029", July 10, 2025. https://www.politico.eu/article/germany-china-huawei-ban-2029-5g-networks-government-greens-lawmaker-4g-strand/; Tagesschau, "Federal government bans Huawei components in 5G mobile networks", July 11, 2024. https://www.tagesschau.de/inland/huawei-5g-verboten-100.html; Reinhard Bütikofer, "Germany's Embarrassing Dance Around China's Huawei", The Center for European Policy Analysis, July 7, 2024. https://cepa.org/article/germanys-embarrassing-dance-around-chinas-huawei/

[29] Tagesschau, "Ban on Huawei technology could cost DB 400 million euros", August 8, 2024. https://www.tagesschau.de/wirtschaft/unternehmen/5g-technik-china-huawei-400-millionen-euro-kosten-fuer-deutsche-bahn-db-100.html

[30] Rhode & Schwarz, "6G Expert Days: 2024", n.d., 59201-6G-Expert-Days-2024-Agenda-240327-web.pdf

[31] BMBF, "6G-ANNA: Holistic Approached for 6th Generation Mobile Networks", n.d. https://6g-anna.de/en/

[32] Alan Mauldin, "Do Submarine Cables Account For Over 99% of Intercontinental Data Traffic?", TeleGeography, May 4, 2023. https://blog.telegeography.com/2023-mythbusting-part-3

[33] Daniel Voelsen, "Untersee-Datenkabel. Kritische Knotenpunkte im Netz globaler Kommunikation", in Maritime kritische Infrastrukturen (e.d). Stiftung Wissenschaft und Politik Deutsches Institut für Internationale Politik und Sicherheit, February 6, 2024. https://www.swp-berlin.org/10.18449/2024S03/

[34] China Academy of Information Communications and Technology (CAICT), "White Paper on China International Optical Cable Connection"

[35] Jannik Hartman, "Protecting the EU's Submarine Cable Infrastructure", DGAP. July 10, 2023. https://dgap.org/en/research/publications/protecting-eus-submarine-cable-infrastructure

[36] See for e.g.: Bikash Koley, "Announcing Google's Grace Hopper subsea cable system", The Google Cloud Blog, July 28, 2020, https://cloud.google.com/blog/products/infrastructure/announcing-googles-grace-hopper-subsea-cable-system; Le Marin, "Le câble sous-marin Amitié entre la France et les États-Unis mis en service", October 19, 2023. https://lemarin.ouest-france.fr/shipping/le-cable-sous-marin-amitie-entre-la-france-et-les-etats-unis-mis-en-service-efb36d8b-d8e4-4d91-86b3-2e1a14cc45aa; TeleGeography, "Anjana", n,d. https://www.submarinecablemap.com/submarine-cable/anjana; Dan Swinhoe, "Meta Plans 480tbps US-Spain Anjana Submarine Cable", Submarine Telecoms Forum, May 3, 2023. https://subtelforum.com/metas-480tbps-us-spain-anjana-submarine-cable/

[37] Submarine Cable Networks. "IMEWE Cable System Upgrades with Cienas 200G Per Wave", November 15, 2019. https://www.submarinenetworks.com/en/systems/asia-europe-africa/imewe

[38] Daniel Voelsen, "Untersee-Datenkabel. Kritische Knotenpunkte im Netz globaler Kommunikation"

[39] Ibid.

[40] Frank Jüris, "Security implications of China-owned critical infrastructure in the European Union", European Parliament: Policy Department for External Relations Directorate General for External Policies of the Union, June 2023. https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf

[41] China Academy of Information Communications and Technology (CAICT), "White Paper on China International Optical Cable Connection"

[42] Justin Shermin, "Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Security", Atlantic Council, September, 2021. Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf

[43] 2 Africa "Partners: China Mobile International Limited", n.d., https://www.2africacable.net/partners

[44] Peace Cable, "Peace Cable System," n.d., http://www.peacecable.net/

[45] Jacob Gunter and Rebecca Arcesati, "The Digital Silk Road: A growing priority for Beijing as its tech champions expand overseas", March 27, 2024. https://merics.org/en/tracker/digital-silk-road-growing-priority-beijing-its-tech-champions-expand-overseas

[46] J-fiber, "Products," n.d. https://www.j-fiber.com/en/products/; Optico, "Hengtong Optic-Electric Has Successfully Acquired J-fiber GmbH", March 15, 2023. https://www.fiberopticom.com/news/hengtong-optic-electric-has-successfully-acqui-67470477.html

[47] Frank Jüris, "Security implications of China-owned critical infrastructure in the European Union"

[48] Ibid.

[49] US Department of Commerce, "Addition of Certain Entities to the Entity List and Revision of an Entry on the Entity List", 17 December, 2021. https://www.federalregister.gov/documents/2021/12/17/2021-27406/addition-of-certain-entities-to-the-entity-list-and-revision-of-an-entry-on-the-entity-list

[50] Joe Brock, "U.S. and China wage war beneath the waves - over internet cables", Reuters, March 24, 2023. https://www.reuters.com/investigates/special-report/us-china-tech-cables/; The multinational consortium included Bangladesh Submarine Cable Company Limited (BSCCL), Bharti Airtel Ltd. (India), Dhivehi Raajjeyge Gulhun Public Limited Company (Dhiraagu Maldives), China Unicom (China), Djibouti Telecom, Mobily (Saudi Arabia), Orange (France), Singtel (Singapore), Sri Lanka Telecom, Telecom Egypt, Telekom Malaysia, Telin (Indonesia), Trans World Associates (Pakistan), and Batelco. See: Submarine Cable Networks, "SEA-ME-WE 6", https://www.submarinenetworks.com/en/systems/asia-europe-africa/smw6

[51] Yimou Lee, Ann Wang and Marco Haernandez "China's latest weapon against Taiwan: the sand dredger", Reuters, February 5, 2021. https://www.reuters.com/graphics/TAIWAN-CHINA/SECURITY/jbyvrnzerve/; Yang Yuan-ting and Jonathan China "Officials urge action over Chinese dredging activity", Taipei Times, June 2, 2023. https://news.ltn.com.tw/news/focus/breakingnews/4320831

[52] Yimou Lee and Ben Blanchard, "In a first, Taiwan charges Chinese ship captain with damaging undersea cables", Reuters. April 11, 2025. https://www.reuters.com/world/asia-pacific/first-taiwan-charges-chinese-ship-captain-with-damaging-undersea-cables-2025-04-11/

[53] Ibid.

[54] The Washington Post, "Accidents, not Russian sabotage, behind undersea cable damage, officials say", January 19, 2025. https://www.washingtonpost.com/world/2025/01/19/russia-baltic-undersea-cables-accidents-sabotage/?nid=top_pb_signin&arcId=DJLIEYR6HZCLHCQSMUBAFALTVA&account_location=ONSITE_HEADER_ARTICLE

[55] Alexander Lott, " Christmas Day Cable Cuts in the Baltic Sea", EJIL: Talk, December 31, 2024. https://www.ejiltalk.org/christmas-day-cable-cuts-in-the-baltic-sea/; The Washington Post, "Accidents, not Russian sabotage, behind undersea cable damage, officials say", January 19, 2025. https://www.washingtonpost.com/world/2025/01/19/russia-baltic-undersea-cables-accidents-sabotage/?nid=top_pb_signin&arcId=DJLIEYR6HZCLHCQSMUBAFALTVA&account_location=ONSITE_HEADER_ARTICLE

[56] Ibid.

[57] Submarine cable networks " Europe-Russia-Asia (ERA)", n.d. https://www.submarinenetworks.com/en/systems/eurasia-terrestrial/era; China Telecom, "Euro-Asia Network Solution," n.d. https://www.chinatelecomeurope.com/wp-content/uploads/ChinaTelecom_Euro-Asia-network-solution.pdf; Submarine cable networks, "DREAM", n.d. https://www.submarinenetworks.com/en/systems/eurasia-terrestrial/dream

[58] Submarine cable networks, "DREAM", n.d. https://www.submarinenetworks.com/en/systems/eurasia-terrestrial/dream; FinTech Futures, "Russian telco links Europe to Asia with high-speed fibre", October 23, 2013. https://www.fintechfutures.com/2013/10/russian-telco-links-europe-to-asia-with-high-speed-fibre/

[59] Medium, "Satellite internet technology: A double-edged sword", December 23, 2023. https://medium.com/@researchoutreach/satellite-internet-technology-a-double-edged-sword-f2cccb63e421

[60] The State Council, People's Republic of China, "China's new mega-constellation marks milestone in satellite internet", August 9, 2024. https://english.www.gov.cn/news/202408/09/content_WS66b55ad9c6d0868f4e8e9cf8.html

[61] The Economist, "Why China is building a Starlink system of its own", December 6, 2024. https://www.economist.com/science-and-technology/2024/12/06/why-china-is-building-a-starlink-system-of-its-own

[62] Kleo, "Constellation," n.d. https://kleo-connect.com/constellation

[63] Dieter Sürig, "Row over huge space project from Liechtenstein", Tagesanzeiger, May 16. 2022. https://www.tagesanzeiger.ch/zoff-um-riesiges-weltraumprojekt-aus-liechtenstein-486754623688

[64] Glenn Chafetz and Xavier Ortiz, "China, Lawfare, and the Contest for Control of Low Earth Orbit", The Diplomat, August 10, 2023. https://thediplomat.com/2023/08/china-lawfare-and-the-contest-for-control-of-low-earth-orbit/

[65] Jeff Foust, "Space industry sees growing effects of coronavirus outbreak", SpaceNews, March 9, 2020. https://spacenews.com/space-industry-sees-growing-effects-of-coronavirus-outbreak/; Eleanor Olcott, "The corporate feud over satellites that pitted the west against China," Financial Times, June 22, 2022. https://www.ft.com/content/f1f342ab-d931-44ca-bf0d-f7762db76982

[66] Glenn Chafetz and Xavier Ortiz, "China, Lawfare, and the Contest for Control of Low Earth Orbit"

[67] Ibid.

[68] Ibid.

[69] Ibid.

[70] Ibid.

[71] Ibid.

[72] Jens Kastner, "Germany to tighten Chinese investment screening", Nikkei Asia, September 29, 2023. https://asia.nikkei.com/Politics/International-relations/Germany-to-tighten-Chinese-investment-screening

[73] Janosch Wiesenthal, "Lessons learned from the „Kleo Connect" Case", CELIS Institute, December 15, 2023. https://www.celis.institute/celis-blog/lessons-learned-from-the-kleo-connect-case/

[74] Chris Forrester, "Rivada suffers Liechtenstein blow," Advanced Television, November 15, 2024 https://www.advanced-television.com/2024/11/15/rivada-suffers-liechtenstein-blow/

[75] Jason Rainbow, "Rivada brushes off regulatory setback for proposed broadband constellation," SpaceNews, December 13, 2034. https://spacenews.com/rivada-brushes-off-regulatory-setback-for-proposed-broadband-constellation/; Xinhua, "China launches 18 satellites from Hainan commercial spacecraft launch site", The State Council Information Office, PRC, March 12, 2025. http://english.scio.gov.cn/m/chinavoices/2025-03/12/content_117761686.html

[76] Janosch Wiesenthal, "Lessons learned from the „Kleo Connect" Case", CELIS Institute, December 15, 2023. https://www.celis.institute/celis-blog/lessons-learned-from-the-kleo-connect-case/

[77] Federal Ministry of Digital and Transport, "Strategy for International Digital Policy of the Federal Government"

[78] Ibid.

[79] Cloudscene, "Germany: Data Center Market Overview", n.d. https://cloudscene.com/market/data-centers-in-germany/all

[80] DECIX, "Europe's largest Internet Exchange DE-CIX Frankfurt sets new traffic record: 15 Terabits per second", September 20, 2023. https://www.de-cix.net/en/about-de-cix/media/press-releases/europes-largest-internet-exchange-de-cix-frankfurt-sets-new-traffic-record-15-terabits-per-second

[81] DECIX, "Europe's largest Internet Exchange hits 18 Tbps data throughput", November 21, 2024. https://www.de-cix.net/en/about-de-cix/media/press-releases/new-record-at-de-cix-frankfurt-europes-largest-internet-exchange-hits-18-terabits-per-second-data-throughput

[82] Ambrose McNevin, "Dell opens German data center", March 7, 2012. Data Centre Dynamics, https://www.datacenterdynamics.com/en/news/dell-opens-german-data-center/; Georgia Butler, "Nokia to bolster Hetzner's data center infrastructure", Data Centre Dynamics, March 17, 2025. https://www.datacenterdynamics.com/en/news/nokia-to-bolster-hetzners-data-center-infrastructure/; Georgia Butler, "Ionos deploys Nvidia DGX H200 system in Germany data centers", Data Centre Dynamics, July 26, 2025. https://www.datacenterdynamics.com/en/news/ionos-deploys-nvidia-dgx-h200-system-in-germany-data-centers/

[83] Alibaba Cloud, "Alibaba Cloud Launches Third Datacentre in Germany", May 17, 2022. https://www.alibabacloud.com/en/press-room/alibaba-cloud-launches-third-datacentre-in-germany?_p_lc=1; German Datacentre Association, "China Mobile International", n.d. https://www.germandatacenters.com/partner/china-mobile-international/; China Telcom Americas, "Global Data Center Map," n.d. https://www.ctamericas.com/global-data-center-map/; Simon Sharwood, "Tencent Cloud adds second data centre in Germany, Thailand, and Japan, plus a third in Hong Kong", The Register, June 3, 2021. https://www.theregister.com/2021/06/03/tencent_cloud_expansion/

[84] German Datacenter Association, "Member and Partner", n.d. https://www.germandatacenters.com/en/gda/member-partner/

[85] Emily de la Bruyere and Nathan Picarsic, "China's quest for asymmetric dominance in data centers", Hinrich Foundation, June 2024. https://research.hinrichfoundation.com/hubfs/White%20Paper%20PDFs/China%E2%80%99s%20quest%20for%20asymmetric%20dominance%20in%20data%20centers%20(Emily%20de%20la%20Bruyere%20and%20Nathan%20Picarsic)/China%E2%80%99s%20quest%20for%20asymmetric%20dominance%20in%20data%20centers%20-%20Emily%20de%20la%20Bruyere%20and%20Nathan%20Picarsic%20-%20Hinrich%20Foundation%20-%20June%202024.pdf?__hstc=251652889.d41904b4171f0f106b0725423c1a88dc.1738447719698.1738447719698.1738447719698.1&__hssc=251652889.2.1738447719698&__hsfp=1351883797

[86] Ibid.

[87] GTCOM, "GTCOM releases alternative data to explore the unique value of global financial quantification", January 1, 2019. https://www.gtcom.com.cn/?c=news&a=view&id=1353

[88] Xinhua News Agency, "The Standing Committee of the Political Bureau of the CPC Central Committee held a meeting to study the current key work of preventing and controlling the new crown pneumonia epidemic and stabilizing economic and social operations Xi Jinping presided over the meeting", March 4, 2023. https://www.gov.cn/xinwen/2020-03/04/content_5486931.htm; The People's Government of Fujian Province, "Outline of the 14th Five-Year Plan (2021-2025) for National Economic and Social Development and Vision 2035 of the People's Republic of China", August 9, 2019. https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm

[89] Alibaba Cloud, "Alibaba Cloud Launches Third Datacentre in Germany", May 17, 2022. https://www.alibabacloud.com/en/press-room/alibaba-cloud-launches-third-datacentre-in-germany?_p_lc=1&spm=a3c0i.8288105.9593763490.15.4a336a37mt9ZZf

[90] U.S. Department of Homeland Security, "Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China", 22 December, 2020. https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf

[91] China Telcom Europe, "Your digital silk road to China and APAC", n.d. https://www.chinatelecomeurope.com/; Alibaba Cloud, "China Gateway: Secure Your Business Success in China - Alibaba Cloud", https://www.alibabacloud.com/en/china-gateway?_p_lc=1&spm=a3c0i.234829.9135018350.19.12d42d782pmOff

[92] Siemens, "Siemens and Alibaba Cloud partner to power industrial Internet of Things in China | Press | Company", July 9, 2018. https://press.siemens.com/global/en/pressrelease/siemens-and-alibaba-cloud-partner-power-industrial-internet-things-china

[93] CACLP, "Siemens and Alibaba Cloud signed strategic cooperation", July 6, 2023. https://en.caclp.com/industry-news/2292.html

[94] Alibaba Cloud, "Alibaba and SAP Deepen Global Partnership to Accelerate Intelligent Enterprises in China", September 19, 2018. https://www.alibabacloud.com/en/press-room/alibaba-and-sap-deepen-global-partnership-to-accelerate?_p_lc=1

[95] SAP, "SAP and Alibaba Group Partner to Accelerate Cloud Transformation", May 27, 2025. SAP and Alibaba Group Partner to Accelerate Cloud Transformation | SAP News Center

[96] Ecommerce News, "Alibaba lowers membership costs for German SMEs", June 28, 2024. https://ecommercenews.eu/alibaba-lowers-membership-costs-for-german-smes/

[97] Ibid.

[98] Vili Lehdonvirta, Boxi Wú and Zoe Hawkins, "Weaponized interdependence in a bipolar world: how economic forces and security interests shape the global reach of US and Chinese cloud datacenters", Review of International Political Economy, February 26, 2025. https://www.tandfonline.com/doi/epdf/10.1080/09692290.2025.2489077?needAccess=true

[99] Anette Dowideit, "How NRW secures its research projects - with technology from Huawei", Correctiv.org, July 22, 2024. https://correctiv.org/aktuelles/bildung/2024/07/22/wie-nrw-seine-forschungsprojekte-absichert-mit-technik-von-huawei/

[100] RWTH Aachen University, "Our Rankings in a Nutshell", August 2024. https://www.rwth-aachen.de/global/show_document.asp?id=aaaaaaaaabdiqax

[101] Anette Dowideit, "How NRW secures its research projects - with technology from Huawei"

[102] Till Eckert, "The bling-bling professors from Aachen", Correctiv, June 18, 2024. https://correctiv.org/aktuelles/china-science-investigation/2024/06/18/die-bling-bling-professoren-aus-aachen/

[103] Federal Statistical Office of Germany, "The main German export product: motor vehicles," n.d. https://www.destatis.de/EN/Themes/Economy/Foreign-Trade/trading-goods.html

[104] Gregor Sebastian, "The bumpy road ahead in China for Germany's carmakers"

[105] Theo Leggett, "Germany's once-mighty car industry is in crisis. What will it take to fix it?", BBC. February 12, 2025. https://www.bbc.com/news/articles/cz6pzwj6qq7o

[106] European Commission, "EU imposes duties on unfairly subsidized electric vehicles from China while discussions on price undertakings continue", October 29, 2024. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5589

[107] Reuters, "Germany's Scholz calls for more talks with China on electric vehicles", October 2, 2024. https://www.reuters.com/business/autos-transportation/germanys-scholz-talks-with-china-electric-vehicles-must-continue-2024-10-02/?utm_source=chatgpt.com

[108] Reuters, "German government voted against EU tariffs on EVs from China, source says", October 4, 2024. https://www.reuters.com/business/autos-transportation/german-government-voted-against-eu-tariffs-evs-china-source-says-2024-10-04/

[109] Federal Register: Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles

[110] The German Association of the Automotive Industry, "A blanket ban would be of little use", October 28, 2024. https://www.vda.de/en/news/articles/2024/a-blanket-ban-would-be-of-little-use

[111] Sander Tordoir and Brad Setser, "How German industry can survive the second China shock", Centre for European Reform, January 2025. https://www.cer.eu/publications/archive/policy-brief/2025/how-german-industry-can-survive-second-china-shock

[112] Peter Mock, Zifei Yang, Uwe Tietge, Ilma Fadhil and May Al-Ali, "Fair play? The German car market amid increasing competition from China-based manufacturers", International Council on Clean Transportation, April 29, 2023. https://theicct.org/german-car-market-amid-increasing-competition-from-china-based-manufacturers-apr24/#:~:text=While%20brands%20based%20in%20China,BEVs%20in%20their%20home%20market.

[113] Hendin Mobility Group, "Hedin Mobility Group and BYD complete the sale and purchase of German distribution network", October 31, 2024. https://hedinmobilitygroup.com/news-and-media/news/762dbbf4-afe7-46cb-a3d2-ea6b7f0a977a

[114] Janka Oertel, "Security recall: The risk of Chinese electric vehicles in Europe", European Council on Foreign Relations, January 25, 2024. https://ecfr.eu/article/security-recall-the-risk-of-chinese-electric-vehicles-in-europe/

[115] Ibid.

[116] Alexander Brown and Andreas Mischer, "German carmakers are placing a risky bet on China", MERICS, December 10, 2024. https://merics.org/de/kommentar/german-carmakers-are-placing-risky-bet-china

[117] Mercedes-Benz Group, "Smart Joint Venture", July 27, 2020. https://group.mercedes-benz.com/company/news/smart-europe.html

[118] Iris Deng, "Tencent renews partnership with Bosch for deeper smart car collaboration", South China Morning Post, November 4, 2024. https://www.scmp.com/tech/big-tech/article/3285134/tencent-renews-partnership-bosch-deeper-smart-car-collaboration

[119] Volkswagon Grounp, "Ready for next EV push: Volkswagen enters into agreement with XPENG for fast joint development of two smart e-cars," February 29, 2024. https://www.volkswagen-group.com/en/articles/ready-for-next-ev-push-volkswagen-enters-into-agreement-with-xpeng-for-fast-joint-development-of-two-smart-e-cars-18246; Reuters, "BMW to integrate DeepSeek AI in its new vehicles in China later this year", April 23, 2025. https://www.reuters.com/business/autos-transportation/bmw-integrate-deepseek-ai-its-new-vehicles-china-later-this-year-2025-04-23/;

[120] The Federal Minister for Digital and Transport (BMWK) "Germany and China sign Memorandum of Understanding on dialogue and cooperation in the field of automated and connected driving", April 16, 2024. https://www.bmwk.de/Redaktion/EN/Pressemitteilungen/2024/04/20240416-germany-and-china-sign-memorandum-of-understanding-on-dialogue-and-cooperation-in-the-field-of-automated-and-connected-driving.html

[121] noyb complaints regarding data transfers to China

[122] Global Newswire, "Germany Video Surveillance Industry to Grow at a CAGR 6.6%", June 6. 2023. https://www.globenewswire.com/news-release/2023/06/06/2682506/0/en/Germany-Video-Surveillance-Industry-to-Grow-at-a-CAGR-6-6-from-2022-to-2027.html; Mordor Intelligence, "Germany Surveillance Analog Camera Market Share", n.d. https://www.mordorintelligence.com/industry-reports/germany-surveillance-analog-camera-market/market-share; 6W Research, "Germany Video Surveillance System Market (2019-2025)", September 2022. https://www.6wresearch.com/industry-report/germany-video-surveillance-system-market-2019-2025

[123] Valentin Weber, "For more cybersecurity, Germany must remove high-risk Chinese technologies"; Hikvision, "Hikvision secures Frankfurt light rail", March 19, 2020. https://www.ventasdeseguridad.com/en/more-in-depth/end-user/21203-hikvision-secures-frankfurt-light-rail.html; Security Worldmarket.com "Hikvision heavy duty domes prove their worth in demanding; environment," July 12, 2011. https://www.securityworldmarket.com/int/Newsarchive/hikvision-heavy-duty-domes-prove-their-worth-in-demanding-environment; Dahua Security, "Success Stories: Airport in Germany", October 17, 2022. https://www.dahuasecurity.com/newsEvents/successStories/5051/1497

[124] Hikvision, "Success stories: Bringing events into a safer 'new normal'", December 16, 2020. https://www.hikvision.com/europe/newsroom/success-stories/hospitality/bringing-events-into-a-safer--new-normal-/

[125] Hikvision, "Success stories: Streamlined parking in Germany", May 16, 2019. https://www.hikvision.com/hu/newsroom/success-stories/safe-city/streamlined-parking-in-germany/

[126] Ibid.

[127] Hikvision, "DACH Webinare," n.d., https://www.hikvision.com/de/support/academy/DACH_webinars/

[128] Dahua, "Dahua Technology Developed Mobile „Video Guards" with Complete Solution for Security Service Company in Germany", July 26, 2019. https://www.dahuasecurity.com/ceen/newsEvents/successStories/137/847

[129] Dahua Germany, "Event: Dahua KRITIS TechDay, Munich (DE)", n.d. https://dahuasecurity.de/event/dh-techday-20032025/

[130] US Department of Commerce, "Addition of certain entities to the entity list", September 10, 2019. https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list

[131] Sean Patten, "Critical Vulnerabilities In Hikvision Hik-Connect, Hikvision Hides From Public", IPVM, May 22, 2023. https://ipvm.com/reports/hik-ipvm-hc

[132] Ibid.

[133] Statista, "Consumer IoT market size in Europe from 2020 to 2022, with a forecast up to 2030, by country", February 21, 2025. https://www.statista.com/statistics/1409187/europe-consumer-iot-market-value-by-country/

[134] Alexander Sandkamp, Vincent Stamer, Falk Wendorff und Steffen Gans, "Empty shelves made in China: When China blocks trading", Kiel Institute, February 2023. https://www.ifw-kiel.de/fileadmin/Dateiverwaltung/IfW-Publications/fis-import/ea898761-22d6-4745-a2a9-daaafdeb1e6a-KPB_164.pdf

[135] Ibid.

[136] Deutsche Bundesbank, "Economic risks from Germany's ties with China", January 24, 2024. https://www.bundesbank.de/en/tasks/topics/economic-risks-from-germany-s-ties-with-china-922490

[137] Gracelin Baskaran and Meredith Schwartz, "The Consequences of China's New Rare Earths Export Restrictions", CSIS, April 14, 2025. https://www.csis.org/analysis/consequences-chinas-new-rare-earths-export-restrictions

[138] Ryan McMorrow, Joe Leahy and Kana Inagaki, "China demands sensitive information for rare earths exports, companies warn", Financial Times, June 12, 2025. https://www.ft.com/content/0fce7177-a713-4c06-ba22-0ae429efe73f

[139] Ibid.

[140] Ibid.

[141] Cora Jungbluth, "Kauft China systematisch Schlüsseltechnologien auf?", Bertelsmann Stiftung, May 22, 2018. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/MT_Made_in_China_2025.pdf

[142] The State Council of the People's Republic of China, "Made in China 2025' plan issued"; Cynthia Wrage and Jakob Kullik, "After Kuka – Germany's Lessons Learned from Chinese Takeovers", China Observers in Central and Eastern Europe (CHOICE), July 21, 2022. https://chinaobservers.eu/after-kuka-germanys-lessons-learned-from-chinese-takeovers/

[143] Camille Boullenois, Malcolm Black and Daniel H. Rosen, "Was Made in China 2025 Successful?"

[144] Jürgen Matthes and Edgar Schmitz, "Competitive pressure from China for German companies", German Economic Institute (IW), June 11, 2024. https://www.iwkoeln.de/fileadmin/user_upload/Studien/Report/PDF/2024/IW-Report_2024-Umfrage-China-Konkurrenz.pdf

[145] Jules Adam, "The top-performing countries in biotechnology (according to the OECD)", Labiotech, January 3, 2025. https://www.labiotech.eu/best-biotech/top-biotech-countries/

[146] Adem Koyuncu and Maximilian Aretz, "Germany prepares new National Strategy for Gene and Cell Therapies", Covington, June 18, 2024. https://www.insideeulifesciences.com/2024/06/18/germany-prepares-new-national-strategy-for-gene-and-cell-therapies/

[147] Francis de Véricourt and Melike Demir, "Assessing Deep-Tech Innovation Hubs in Germany: The Case of Biotechnology", ESMT Berlin and Bertellsman Foundation, January 2025, 394_2025-bst-studie-assessing-deep-tech-innovation-hubs-in-germany-esmt-id2507.pdf

[148] WuXi AppTech, "WuXi AppTec Acquires Crelux", April 15, 2016. https://www.wuxiapptec.com/news/wuxi-news/1873;

[149] Bayer, "Bayer sells a facility at its Wuppertal site to WuXi Biologics", December 21, 2020, https://www.bayer.com/media/en-us/bayer-sells-a-facility-at-its-wuppertal-site-to-wuxi-biologics/

[150] WuXi Biologics, "WuXi Biologics to Increase Manufacturing Capacity in Germany", June 1, 2023. https://www.wuxibiologics.com/wuxi-biologics-to-increase-manufacturing-capacity-in-germany/

[151] Terumo Global, "Terumo and WuXi Biologics Enter into Agreement on a Drug Product Plant in Leverkusen, Germany", May 14. 2025. https://www.terumo.com/newsrelease/detail/20250514/6576

[152] Ernst and Young, "German Biotechnology Report 2024: How can AI be the key to unlocking new opportunities in the German biotech sector?", 2024. https://www.ey.com/content/dam/ey-unified-site/ey-com/de-de/noindex/ey-german-biotechnology-report-2024-how-can-ai-be-the-key.pdf?mkt_tok=NTIwLVJYUC0wMDMAAAGZ-44p-xxhJcLPSdP7RawKiHCiCCgg9Dq_uMHIjEWD91qeZJijoiOBLVoRAKNKsE-1mbAhx1YvJDxPS-y8gGtNK8n5X6VwcKFiPA5PX9ZNziUR2jAqIUY

[153] Chris Devonshire-Ellis, "How Chinese Financing Is Helping US and German Biotechnology", China Briefing from Dezan Shira and Associates, December 16, 2021. https://www.china-briefing.com/news/how-chinese-financing-is-helping-us-germany-biotechnology/

[154] Ibid.

[155] BioNTech, "BioNTech and Fosun Pharma form COVID-19 vaccine strategic alliance in China", March 16, 2020. https://investors.biontech.de/news-releases/news-release-details/biontech-and-fosun-pharma-form-covid-19-vaccine-strategic

[156] BioNTech, "BioNTech and Fosun Pharma form COVID-19 vaccine strategic alliance in China"; Dou Shicong, "Germany's BioNTech Acquires Rights to New Chinese Cancer Drug", Yicai Global, October 12, 2023. https://www.yicaiglobal.com/news/germanys-biontech-joins-hands-with-chinas-medilink-in-developing-new-anti-cancer-drug?utm_source=substack&utm_medium=email

[157] Biospectrum, "China-based biotech firm MGI unveils new European headquarters in Berlin", June 5. 2024. https://www.biospectrumasia.com/news/26/24380/china-based-biotech-firm-mgi-unveils-new-european-headquarters-in-berlin.html

[158] US Department of Commerce, "Additions and Revisions of Entities to the Entity List", Federal Register, https://www.federalregister.gov/documents/2023/03/06/2023-04558/additions-and-revisions-of-entities-to-the-entity-list Alexandra Alper and David Shepardson, "US adds units of China's BGI, Inspur to trade blacklist", Reuters, March 16, 2023. https://www.federalregister.gov/documents/2023/03/06/2023-04558/additions-and-revisions-of-entities-to-the-entity-listlist

[159] Karen Freifeld, "US bill to restrict business with China's WuXi AppTec, BGI passes House", Reuters, September 10, 2024. https://www.reuters.com/markets/us/us-bill-restrict-business-with-chinas-wuxi-apptec-bgi-passes-house-2024-09-09/

[160] GTAI, "Germany Records Record Rise in Installed Robotics", September 25, 2024. https://www.gtai.de/en/meta/press/germany-records-record-rise-in-installed-robotics-1823456

[161] Wiely Industry news, "China overtakes Germany in the use of robots in industry", November 11, 2024. https://www.wileyindustrynews.com/en/news/china-overtakes-germany-use-robots-industry

[162] Cynthia Wrage and Jakob Kullik, "After Kuka – Germany's Lessons Learned from Chinese Takeovers", China Observers in Central and Eastern Europe (CHOICE), July 21, 2022. https://chinaobservers.eu/after-kuka-germanys-lessons-learned-from-chinese-takeovers/

[163] Ibid.

[164] Federal Ministry for Economic Affairs and Climate Action, "Investment Screening", n.d., https://www.bmwk.de/Redaktion/EN/Artikel/Foreign-Trade/investment-screening.html

[165] Eugene Demaitre, "Estun Automation acquires Carl Cloos Welding Technology", The Robot Report, August 30, 2019. https://www.therobotreport.com/estun-automation-acquires-carl-cloos-welding-technology/

[166] Estun, "About us", https://en.estun.com/?about_57/

[167] International Trade Administration, "Germany Country Commercial Guide 2023", 2023. https://trade.gov/sites/default/files/2024-02/Germany_CCG_2023.pdf

[168] GTAI, "E-commerce in Germany", n.d. https://www.gtai.de/en/invest/industries/digital-economy/e-commerce-65482

[169] Sinoletics Radar, "How Temu became Germany's No. 1 App", Table Briefings, February 14, 2024. https://table.media/en/china/sinolytics-radar/temu-has-risen-to-become-germanys-number-one-app/

[170] IFH Köln, "Awareness and use of Temu, Shein and Co. increased immensely", May 22, 2024. https://www.ifhkoeln.de/bekanntheit-und-nutzung-von-temu-shein-und-co-immens-gestiegen/

[171] U.S.-China Economic and Security Review Commission, "Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes", April 14, 2023. https://www.uscc.gov/sites/default/files/2023-04/Issue_Brief-Shein_Temu_and_Chinese_E-Commerce.pdf

[172] Ibid.

[173] Federal Ministry for Economic Affairs and Climate Action, "Germany, Austria, Denmark, the Netherlands and France are calling for stronger legal enforcement in the field of E-Commerce", 26 September, 2024. https://www.bmwk.de/Redaktion/EN/Pressemitteilungen/2024/09/20240926-eu-member-states-calling-for-stronger-legal-enforcement-in-the-field-of-e-commerce.html

[174] U.S.-China Economic and Security Review Commission, "Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes"

[175] Ibid.

[176] Ibid.

[177] Nectar Gan, Yong Xiong and Juliana Liu, "Pinduoduo: One of China's most popular apps has the ability to spy on its users, say experts", CNN Business, April 3, 2023. https://edition.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html

[178] Ibid.

[179]181 Stripe, "Payments in Germany: An in-depth guide," April 5, 2024. https://stripe.com/en-de/resources/more/payments-in-germany-an-in-depth-guide

[180] Sinolytics Radar, "The Risks of WeChat", November 1, 2023. https://table.media/en/china/sinolytics-radar/the-risks-of-wechat/; Stackfield, "In which cases do I activate end-to-end encryption?", n.d. https://www.stackfield.com/help/functionality-of-the-encryption-2086

[181] Fintech Finance News, "Alipay+ Partner E-Wallets Transactions in Germany Rose by 67% One Week into UEFA EURO 2024", June 24, 2024. https://ffnews.com/newsarticle/paytech/alipay-partner-e-wallets-transactions-in-germany-rose-by-67-one-week-into-uefa-euro-2024/

[182] Elizibeth Braw, "Who's Seeing Your Data and Why?", American Enterprise Institute, August 17, 2022. https://www.aei.org/op-eds/whos-seeing-your-data-and-why/

[183] The European Commission, "Commission opens formal proceedings against TikTok on election risks under the Digital Services Act", November 24, 2024. https://ec.europa.eu/commission/presscorner/detail/ru/ip_24_6487

[184] Rebecca Arcesati, The data quagmire for German carmakers in China", May 6, 2024. https://merics.org/en/comment/data-quagmire-german-carmakers-china

[185] Deutsche Welle, "Chinese cyberattacks hit nearly half of German firms, study", August 8, 2024. https://www.dw.com/en/chinese-cyberattacks-hit-nearly-half-of-german-firms-study/a-70070417

[186] The European Commission, "NIS2 Directive: new rules on cybersecurity of network and information system", January 15, 2025. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive#:~:text=The%20NIS2%20Directive%20establishes%20a,cross%2Dborder%20reaction%20and%20enforcement.

[187] Federal Ministry for Economic Affairs and Climate Action, "Sino-German Industrie 4.0 Cooperation", n.d. https://www.plattform-i40.de/IP/Redaktion/EN/Dossiers/china.html

[188] Matt Sheehan and Jacob Feldgoise, "What Washington Gets Wrong About China and Technical Standards", Carnegie Endowment for International Peace, February 27, 2023, https://carnegieendowment.org/research/2023/02/what-washington-gets-wrong-about-china-and-technical-standards?lang=en; Lindsay Gorman, "The U.S. Needs to Get in the Standards Game—With Like-Minded Democracies", Lawfare, https://www.lawfaremedia.org/article/us-needs-get-standards-game%E2%80%94-minded-democracies

[189] Daniel Fuchs and Sarah Eaton, "Diffusion of Practice: The Curious Case of the Sino-German Technical Standardisation Partnership", New Political Economy: Vol 27, No 6, July 28, 2021. https://www.tandfonline.com/doi/abs/10.1080/13563467.2021.1961221

[190] Ibid.

[191] Federal Ministry for Economic Affairs and Energy, "Sino-German Industrie 4.0 Cooperation"

[192] Ibid.

[193] Ibid.

[194] Daniel Fuchs and Sarah Eaton, "Diffusion of Practice: The Curious Case of the Sino-German Technical Standardisation Partnership", New Political Economy: Vol 27, No 6, July 28, 2021. https://www.tandfonline.com/doi/abs/10.1080/13563467.2021.1961221

[195] Ibid.

[196] Ibid.

[197] Lindsay Gorman, "A Future Internet for Democracies: Contesting China's Push for Dominance in 5G, 6G, and the Internet of Everything"

[198] Ibid.

[199] Ibid.

[200] Tim Rühlig, "China's Digital Power: Assessing the Implications for the EU", German Council of Foreign Relations (DGAP), January 27, 2022. https://dgap.org/en/research/publications/chinas-digital-power-assessing-implications-eu

[201] Ibid.

Report

G | M | F