German Council on Foreign Relations

October 2022

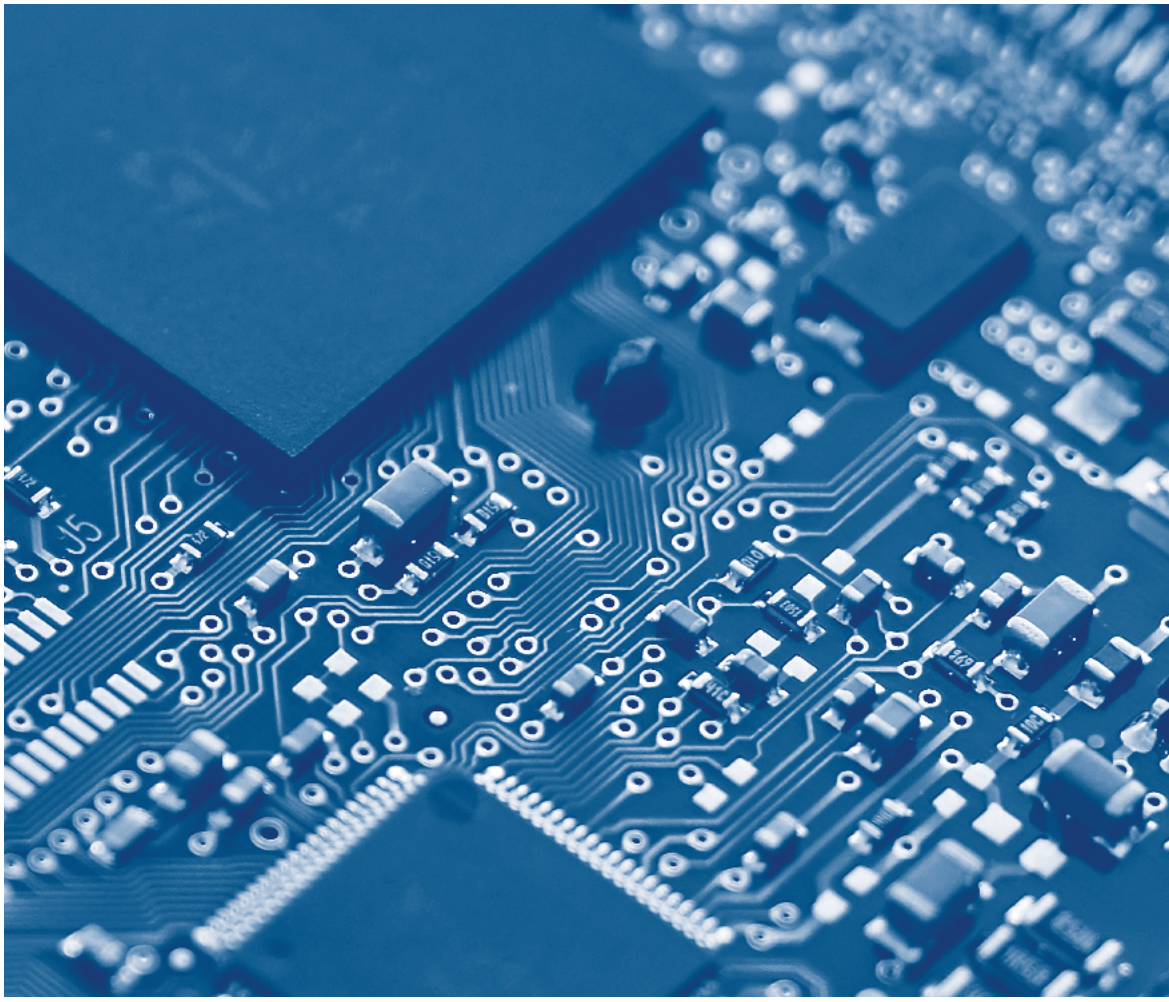
DGAP REPORT

Germany's Economic Security and Technology

Optimizing Export Control, Investment Screening and Market Access Instruments

Tyson Barker
Head, Technology and
Global Affairs Program

Dr. David Hagebölling
Associate Fellow,
Technology and
Global Affairs Program



CHAPTER OVERVIEW

Key Takeaways

1 Technological development and increasingly fraught US-China competition have geopolitical consequences for technology access. The erosion of post-Cold War multilateral dual-use technology export control regimes, such as the Wassenaar Arrangement, and investment and other control frameworks have led to national, EU, and ad hoc measures, such as the restrictions on Russian semiconductor access following the invasion of Ukraine.

2 The German government must integrate technology access and control instruments – export controls, FDI screening, critical infrastructure access, research protection, and outbound investment– in its Digital Strategy and National Security Strategy. The former currently neglects critical technology access and control; the latter must address it comprehensively.

3 German – and EU – dual-use export and FDI screening reforms have been updated and are now in place. Capacity building and alignment with EU and NATO partners now deserves greater attention. Measures could include more robust, institutionalized information-sharing and consultations on dual-use technology export, import, investment, and research controls in a Multilateral Technology Control Committee born out of the G7 or TTC. The committee should also establish the capacity to deny end-user access to German technology through its own Foreign-Direct Product Rules and Entity List.

Introduction

The scope of technologies that can be defined as dual-use – those that have civil and military applications – is widening.[1] Dual-use classifications were once limited mainly to capital-intensive technologies in areas such as nuclear, chemical, precision-guidance, and detection. They are now shifting to a much broader range of information and communications technologies (ICT) whose use and development are diffuse.

As technologies and their building blocks have become more strategically important, they have also become able to disrupt Germany's digitizing society, economy, and even political processes. Technologies manufactured or developed in Germany and the EU can be a target of foreign influence, espionage, and acquisition by actors with ill intent. Similarly, technology manufactured abroad but needed domestically for the functioning of critical infrastructure, such as semiconductors and 5G technology, gives foreign entities similar opportunities for nefarious political and economic manipulation.

Germany's use of technology and market access governance will, therefore, be crucial for safeguarding social cohesion, economic competitiveness, and, ultimately, national security. Governance tools – whether technology access control, intellectual property (IP) protection, mitigation of supply chain dependencies, or foreign direct investment scrutiny – should be central to Germany's digital policy and national security.

Limiting technology access is inherently imperfect. Since Soviet atomic bomb development early in the Cold War, industrial espionage, illicit technology transfer, IP diffusion, and research and development (R&D) efforts have allowed competitors to catch up with technology leaders. Controls on critical technologies are, therefore, effective for only a limited time. How long is dependent on multiple factors - state capacity (China, Iran, Saudi Arabia, Russia and others have different innovation bases to draw from) and technological complexity (capital and skills intensive production processes can create acute, long-term constraints; in contrast, restrictions on some forms of technology like AI and cyber surveillance software are easier to illicitly access or replicate).

1 SPIRI, "Dual-use export controls", (n.d.): https://www.sipri.org/research/armament-and-disarmament/dual-use-and-arms-trade-control/dual-use-export-controls (accessed October 20, 2022).

The State of Play

The proliferation of digital technologies has fueled German and global prosperity through greater ICT connectivity, a narrower digital divide, and a larger capacity for cross-border research. But these advances have also had geopolitical consequences. Access to and control over advanced semiconductors, online platforms, cloud services, data pools, and increasingly cutting-edge artificial intelligence (AI) and quantum technology is now at the core of economic and military power. Moreover, the shift in critical technology innovation from discrete to general-purpose applications, and from the military to the private sector, has fundamentally altered the nature of export, investment, research, and procurement concerns. This has national security and dependency implications.

THE MULTILATERAL APPROACH TO TECHNOLOGY ACCESS AND CONTROL

Against the backdrop of US-China competition, Russian military aggression, and an increasingly vigorous push by states to use technologies on their own ideological terms, global technology governance is strained. Germany participates in numerous multilateral export control regimes, such as the Wassenaar Arrangement, the Nuclear Suppliers Group, the Australia Group, the Missile Technology Control Regime, and the smaller Zangger Committee. Of these, the Wassenaar Arrangement, the voluntary regime that governs export controls for conventional weapons and some dual-use technologies, has had primacy. But it has also demonstrated the limitations of multilateral arrangements that include democratic and increasingly authoritarian regimes.

Current multilateral export coordination regimes are out of sync with today's geopolitical requirements. The Wassenaar Arrangement's 42-country membership provides a normative basis for limited aspects of dual-use technology, but it lacks the teeth of its Cold War predecessor, the Coordinating Committee for Multilateral Export Controls (COCOM).[2] It does not grant veto authority over proposed export licenses. Information-sharing among signatories is voluntary. It does not clearly designate countries that should be denied key technologies, referring instead only to "states of concern" for which there is no definition. Its broad membership, which includes Russia, forgoes cohesion. Lastly, the scope of dual-use technology can be a mismatch to the broadening sphere of software, computing capabilities, and enabling IP, for instance in chip-making, that have domestic repression and surveillance, and military, applications.

GERMAN REFORMS TO TECHNOLOGY CONTROL

Given the limitations of multilateral critical technology governance, most relevant regulation is at the national and EU levels, or through ad hoc arrangements. Germany's export control framework recognizes the shift toward greater licensing volume of dual-use technologies. But in the past, loopholes allowed German technology to be bought and traded by actors that should be evaluated as unfriendly.[3] The case of Munich-based FinFisher is a well-known example of this. The company created one of the world's most sophisticated forms of spyware used by German law enforcement and took advantage of lax controls to sell its product to authoritarian governments in Egypt, Uganda, Ethiopia, Bahrain, and Turkey. They, in turn, used it to crack down on opposition activists.[4] Germany tightened exports after 2015, which led to FinFisher's bankruptcy in 2022.[5] But bureaucratic silos and a lack of systemic foresight remain big hurdles to timely regulation of domestic technology and its use.

2 It is important to look at COCOM as a product of technological development at the time. The cohesion of Western interests around a single threat contributed to its effectiveness, as did preponderant US leadership, consistent application of a core technology list, and a small set of technologies whose production, usage, and transfer were easier to identify and monitor. John H. Henshaw, "The Origins of Cocom: *Lessons for Contemporary Proliferation Control* Regimes", The Henry L. Stimson Center Report No. 7, (May 1993): https://www.stimson.org/wp-content/files/file-attachments/Report7_1.pdf (accessed October 20, 2022).

3 Hans-Martin Tillack and Philipp Grüll, "Deutsche Technik in Kriegsschiffen Chinas" [German technology in Chinese warships], Tagesschau, (November 6, 2021): https://www.tagesschau.de/investigativ/report-muenchen/china-kriegsschiffe-motoren-deutschland-101.html (accessed September 9, 2022).

4 Andre Meister, "German Made State Malware Company FinFisher Raided", Netzpolitik, (October 14, 2020): https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided/ (accessed September 12, 2022).

5 Chaos Computer Club, "Stage win: FinFisher is bankrupt", (March 28, 2022): https://www.ccc.de/en/updates/2022/etappensieg-finfisher-ist-pleite (accessed September 12, 2022).

DIRECT AND INDIRECT APPLICABILITY OF SPECIFIC EXPORT CONTROL REGIMES BY EMERGING TECHNOLOGY AREAS

TECHNOLOGY SECTOR	AI	QC	AS	CS	SC	BT	CT	ET	AT	R
AUSTRALIA GROUP	○	○	○	○	○	●	○	○	○	○
GERMAN AWV	●	●	●	●	●	○	●	○	●	●
CWC	○	○	○	○	○	○	○	○	○	○
MTCR	○	○	●	○	○	○	◐	○	○	○
NUCLEAR SUPPLIERS GROUP	○	○	○	○	○	○	○	○	○	◐
WASSENAAR ARRANGEMENT	◐	◐	◐	◐	◐	◐	●	○	◐	◐
ZANGEN CONVENTION	○	○	○	○	○	○	○	◐	○	○

● DIRECTLY APPLICABLE
◐ PARTIALLY APPLICABLE

AI = Artificial Intelligence | **QC** = Quantum Computing | **AS** = Aviation- and Space Technology | **CS** = Cyber Security | **SC** = Semiconductor Products | **BT** = Biotechnology | **CT** = Communication Technology (incl. 5G) | **ET** = Energy Technology | **AT** = Autonomous technology | **R** = Robotics

Source: Authors' illustration

In other areas as well, Germany continues to have unique assets in international critical-technology supply chains, which should be subject to scrutiny. Three of the top five advanced chip suppliers to ASML, the Dutch ultraviolet lithography systems producer, are German *Mittelstand* companies (Zeiss, machine tools and laser manufacturer Trumpf, and the integrated photonics company Jenoptik). More broadly, Germany is the third-largest technology IP exporter to China, accounting for 10 percent of its external technology IP sourcing. Only the United States (31 percent) and Japan (21 percent) account for more.[6]

Investment screening has also undergone an overhaul in the wake of increasing technological competition between the United States and China. Domestically, Germany has enacted reforms to its Foreign Trade and Payments Act (*Außenwirtschaftsgesetz*, or AWG)[7] and Foreign Trade and Payments Ordinance (*Außenwirtschaftsverordnung*, or AWV)[8] to strengthen and modernize foreign direct investment (FDI) control.[9] This restructuring of foreign investment screening was accelerated by the COVID-19 pandemic, shock of the 2016 takeover of the robotics national champion, Kuka, and intensification of the US-China tech competition.

The new legislation impacts 16 sectors, most relating to critical technologies, such as AI, robotics, chips, aerospace, quantum technology, data infrastructure, and 3D printing, as well as critical infrastructure areas including telecommunications.[10] Updated rules require German investment screening authorities to be notified of acquisitions exceeding 20 percent of voting shares of a company. Allies' FDI review thresholds are lower. Japan's sharpened economic security policy reduced it, in designated industries, from 10 percent to 1 percent.[11]

6 McKinsey Global Institute, "China and the world. Inside the dynamics of a changing relationship", (July 2019): https://www.mckinsey.com/~/media/mckinsey/featured%20insights/china/china%20and%20the%20world%20inside%20the%20dynamics%20of%20a%20changing%20relationship/mgi-china-and-the-world-full-report-june-2019-vf.ashx (accessed September 23, 2022).

7 Bundesministerium für Wirtschaft und Klimaschutz (BMWK), "Außenwirtschaftsgesetz" [Foreign Trade and Payments Act], (July 7, 2020): https://www.bmwk.de/Redaktion/DE/Gesetze/Aussenwirtschaft/AWG.html (accessed September 9, 2022).

8 Ibid.

9 BMWK, "Außenwirtschaftsrecht – Investitionsprüfung" [Foreign Trade and Payments Ordinance - Investment Review], (2022): https://www.bmwk.de/Redaktion/DE/Artikel/Aussenwirtschaft/investitionspruefung.html (accessed September 9, 2022).

10 United Nations Conference on Trade and Development, "World Investment Report 2020. International Production beyond the Pandemic - Chapter III: Recent Policy Developments and Key Issues", United Nations, (2020): https://unctad.org/system/files/official-document/WIR2020_CH3.pdf (accessed September 9, 2022).

11 Didi Kirsten Tatlow and Afra Herr, "Japan's "Economic Security" Measures – A Model for Managing China's Rise", DGAP Policy Brief, German Council on Foreign Relations, (February 7, 2022): https://dgap.org/en/research/publications/japans-economic-security-measures (accessed September 9, 2022).

A diverse group of German agencies and ministries often lacking close cooperation, such as the Federal Office for Economic Affairs and Export Control (BAFA), the Federal Foreign Office (AA), the Federal Ministry for Economic Affairs and Climate Action (BMWK), the Federal Ministry of Defence (BMVg), and the Federal Ministry of the Interior and for Community (BMI), reviews the transactions. The screening caseload has more than tripled since implementation of the reforms in 2020, putting a significant strain on government capacity to review cases effectively. The FDI screening reforms have caused the BMWK, the BMVg, and others to increase bilateral consultations with allied counterparts, including the US Treasury Department.

EU REFORMS TO TECHNOLOGY CONTROL

The EU Commission has been a driving force behind national efforts to update technology access and control policy, and develop more coherent European technology governance. The EU's new export control regime came into force in September 2021, and it significantly upgrades the role of critical-technology export governance. It focuses particularly on cyber surveillance technologies and their "human security dimension,"[12] a catch-all phrase for non-listed goods. The goal is to keep German and other member states' technology off international markets to prevent misuse or replication.[13]

The regime introduces several innovations. First, it increases consultation and reporting between member states and the Commission. Second, it creates greater coordination and visibility among licensing authorities. And third, it expands the EU electronic licensing platform, which gives member states visibility into the actions of their peers. So far, however, the licensing platform has had limited success. Only three member states and one region use it: Italy, Latvia, Romania, and Belgium's Wallonia.

THE GERMAN AND EU REGIMES IN THE CONTEXT OF LIKE-MINDED STATE ACTION

Actions in like-minded states, particularly the United States, have influenced Europe's export control and FDI screening upgrades. The US Congress began in 2018 to overhaul of review processes for critical technology, data, software, and IP to ensure that they could keep up with the rapid development of general-purpose technologies. In twin reforms – the Foreign Investment Risk Review Modernization Act (FIRRMA) and the Export Control Reform Act (ECRA) – Congress vastly expanded the scope, speed, and force of potential export, IP licensing, and FDI restrictions.[14] In light of increased geopolitical competition with China and Russia's war on Ukraine, the Trump and, subsequently, Biden administrations have used these new powers to restrict Chinese and Russian access to semiconductor IP and supplies. The United States has also restricted Chinese access to American markets for drone, smart city, AI, biotech, and mobile network technology.

Most recently, Washington has broadened the intent of its semiconductor technology restrictions on China to go beyond the previous objective of remaining two generations ahead of Beijing.[15] Now, the United States is taking a maximalist position and limiting Chinese access to "force-multiplying" chip technology. This includes restrictions on semiconductor design for chips used in AI and high-performance computing, and prohibiting US nationals from working on the production, sale, and maintenance of chip-making equipment intended for the Chinese market.[16] The effects of this shift in US approach are rippling through global technology value chains and pose challenges to German and European companies that are deeply integrated into these. It also signals US determination to leverage its dominant position in global technology markets to curb China's power and, if necessary, to do so unilaterally.

12 European Parliament, Council of the European Union, "Setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items", L 206/1, (June 11, 2021): https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021R0821 (accessed September 9, 2022).

13 IHK Düsseldorf, "Leitfaden zur Exportkontrolle" [Export control guideline], (October 2021): https://www.ihk.de/duesseldorf/aussenwirtschaft/zoll-und-aussenwirtschaftsrecht/exportkontrolle-2594636 (accessed September 9, 2022).

14 Stormy-Annika Mildner and Claudia Schmucker, "Investment screening: protectionism and industrial policy? Or justified policy tool to protect national security?", Task Force 3 Trade Investment and Growth, (September 2021): https://www.t20italy.org/wp-content/uploads/2021/09/TF3_PB08_LM04 (accessed October 20, 2022).

15 Reva Goujon, "Running Target: Next-Level US Tech Controls on China", Rhodium Group, (September 28, 2022): https://rhg.com/research/running-target/ (accessed October 20, 2022).

16 Max A. Cherney, "The Biden administration issues sweeping new rules on chip-tech exports to China", protocol, (October 7, 2022): https://www.protocol.com/enterprise/chip-export-restrictions-tsmc-intel (accessed October 20, 2022).

This shift in US approach, together with the rapidly deteriorating geopolitical environment, especially Russia's invasion of Ukraine, will further propel cooperation formats between the EU and like-minded states. Through the bloc's coordination with the United States in the EU-US Trade and Technology Council (TTC), Germany swiftly applied export and IP restrictions to high-end semiconductor technology bound for Russia.[17] The effects of this collaboration, arguably the most important related to sanctions on the Kremlin, will degrade Russian military power in aviation, drone technology, and precision guided missiles. It will also lead to a gradual decay of Russia's automobile, civilian aerospace, appliance, and ICT equipment manufacturing.

Still, for Chinese companies with significant ties to the Chinese Communist Party and the People's Liberation Army, noticeable differences in technology access between Germany and the EU, on the one hand and their allies, on the other, remain. Germany, in stark contrast to some of its partners, does not have an instrument for designating end users (a so-called Entity List) that should be denied access to critical technology and IP.[18] Germany's regime – like the rest of Europe – also differs from the United States' in that it is more benign on technology imports – including from authoritarian states. The adoption of untrustworthy technology as critical infrastructure components has become a bigger topic of EU policy debate given Germany's and other member states' reliance on 5G mobile network equipment from Chinese state-adjacent enterprises (Huawei and ZTE), Russian cybersecurity software (Kaspersky Labs), and US hyperscaler cloud services (Amazon Web Services and Microsoft Azure Cloud). Despite this growing European awareness of technology-related risks, the 2020 EU Toolbox for 5G Security demonstrates the difficulties of restricting technology and software imports since that authority remains firmly with member states.

Current Policy Approach

The German government's 2022 Digital Strategy excludes any mention of technology access and control instruments. This is a noticeable blind spot given the centrality of critical-technology access and control in Germany's technological modernization. Still, Germany and Europe over the past five years have rapidly reformed national, multilateral, and normative mechanisms that link critical technology and market access to geopolitical power. These efforts have elevated democracy, human rights, and economic security as considerations for market access instruments such as investment screening, export controls and sanctions, IP licensing, and R&D protection. Germany and the EU have also been moving quickly to diversify and build resilience in supply chains, create reliable friend-shoring partnerships, and develop new instruments to guarantee preferential access to critical technology when shortages impact European security.[19]

Germany and the EU are increasingly leveraging their market power and unique technological assets, together with the EU, US, UK, Japan and other like-minded states. The current government continues to build capacity to enforce technology export and FDI screening reforms. The knock-on effects of severing Russia from access to foundational chip technology demonstrate the potency of technology access as a geopolitical instrument for the EU and NATO, themselves.

Germany – within the EU – is also prioritizing critical-technology supply chain security to inoculate itself against external technological vulnerabilities. Amid pandemic-related supply chain bottlenecks,

17 US Department of Commerce Bureau of Industry and Security, "§ 734.9 Foreign-Direct Product (FDP) Rules", (n.d.): https://www.bis.doc.gov/index.php/licensing/reexports-and-offshore-transactions/direct-public-guidelines#:~:text=Foreign%2Dproduced%20items%20located%20outside,a%20foreign%2Dproduced%20item%20is (accessed September 19, 2022); US-EU Trade and Technology Council, "US-EU Joint Statement of the Trade and Technology Council", (May 16, 2022): https://www.whitehouse.gov/wp-content/uploads/2022/05/TTC-US-text-Final-May-14.pdf (accessed September 19, 2022).

18 This differs notably form the United States' use of entity lists and the Foreign-Direct Product Rule to deny access to designated end users, including through secondary markets. This applies not only to companies but also, following Russia's invasion of Ukraine, to a country.

19 European Commission, "European Chips Act", (2022): https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en (accessed September 19, 2022).

Germany began rolling out government incentives to encourage onshoring, diversification, and supply chain resilience for critical technologies and their components. Ahead of the release of Germany's China Strategy, controversial discussions have taken place on policy changes to limit, or possibly end, government investment and export guarantees for expanding corporate operations in China. The goal is to diversify trade, sourcing, and investment relationships with other East Asian states.[20] Germany has also updated its supply chain due diligence to consider human rights, including the use of forced labor.[21]

The European Commission, for its part, has pushed for greater onshoring and friend-shoring of technology and strategic inputs, including through industrial policy.[22] The European Chips Act, alongside Important Projects of Common European Interest (IPCEI), is the most ambitious attempt to create a regime for critical-technology access and resilience. The act proposes strengthening the security of European semiconductor supply through a mix of targeted state support, strengthened collaboration with partner states, and enhanced means for action in times of crisis. The Commission has called on member states and their industries to map supply chain bottlenecks and vulnerabilities in semiconductors. This is an especially sensitive issue for the German automotive, industrial Internet of Things (IoT), robotics and manufacturing sectors. Lastly, the Commission is targeting state aid to "first-of-a-kind production" to limit subsidizing critical technology for which markets already have established demand. All this is happening as a lively German debate about the efficiency of a heavier state capitalist model for guaranteeing access to critical technology rages. Some argue that the marginal benefit does not justify the cost. But it is the trend in China, East Asian democracies, and, increasingly, the United States, where eliminating dependencies and guaranteeing technology access and development outweigh market considerations.

Beyond EU borders, the Commission is increasing coordination with partners, particularly the United States. Brussels supported in 2021 and 2022 a US request for German government and industry to participate in a mapping and early-warning exercise on the security of semiconductor supply. However, COVID-19 vaccine nationalism in early 2021, particularly that shown by the United States and the United Kingdom, has driven a reevaluation of reliable critical-technology supply, even from allies. The Commission has sparked a debate about monitoring and crisis response, including that related to technology export restrictions. Washington's use of its Defense Production Act to force COVID-19 vaccine producers to prioritize filling American contracts spurred that action.[23]

Regarding cybersecurity due diligence for supply chain sourcing, Berlin has anticipated updates to its critical-technology infrastructure (as reflected in the NIS 2 Directive). It has imposed stricter IT security requirements on critical infrastructure operators and, for the first time, is invoking IT security as a reason for regulating certain companies and designating certain infrastructure as critical.[24] Equipment used in critical infrastructure may now be used only with a guaranteed declaration of the vendors' trustworthiness, and the declaration must meet minimum BMI requirements, although they have yet to be defined.

The German government has thereby taken important steps toward prohibiting the use of critical components that conflict with German, EU, or NATO security interests. This implicitly targets Huawei and ZTE 5G/6G network equipment. But the process of forging technical and political consensus, culminating with the chancellor, is deliberately complex, and the product of hard-to-reconcile differences between different interests and ministry perspectives. Decision-making has also been slow as the Federal Office for Information Security (BSI) is just launching its certification process for trustworthiness.[25] Meanwhile,

20 Andreas Rinke and Sarah Marsh, "Exclusive: German economy ministry reviews measures to curb China business", Reuters, (September 8, 2022): https://www.reuters.com/markets/exclusive-german-economy-ministry-reviews-measures-curb-china-business-2022-09-08/ (accessed September 19, 2022).

21 Federal Ministry of Labour and Social Affairs, "Act on Corporate Due Diligence in Supply Chains.", (August 18, 2021): https://www.bmas.de/EN/Services/Press/recent-publications/2021/act-on-corporate-due-diligence-in-supply-chains.html (accessed September 23, 2022).

22 EU Commission, „Commission presents an updated in-depth review of Europe's strategic dependencies", (February 23, 2022): https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1124 (accessed October 24, 2022).

23 European Commission DG Trade, "Defense Production Act (DPA) during COVID-19", (March 27, 2022): https://trade.ec.europa.eu/access-to-markets/de/barriers/details?isSps=false&barrier_id=15818 (accessed September 12, 2022).

24 Deutscher Bundestag, "Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme" [Draft of a Second Law to Increase Security of IT Systems], Drucksache 19/26106, (January 25, 2021): https://dserver.bundestag.de/btd/19/261/1926106.pdf (accessed September 12, 2022).

25 Stefan Krempl, „Huawei-Klausel: BSI startet Zertifizierungsprogramm für 5G-Komponenten"[Huawei clause: BSI starts certification program for 5G components], heise online, (July 5, 2022): https://www.heise.de/news/Huawei-Klausel-BSI-startet-Zertifizierungsprogramm-fuer-5G-Komponenten-7163182.html (accessed October 20, 2022).

political pressure for rapid 5G rollout is high as Huawei is still on track to provide up to 60 percent of Germany's 5G network infrastructure, primarily in its radio access network (RAN) infrastructure.[26] The assessments of some of Germany's EU and NATO partners has been that the provision of mobile equipment from Huawei poses an unacceptable risk with many banning equipment use in both core and RAN 5G infrastructure. In other areas, the BSI has also pointed to new restrictions. For instance, it issued a public warning about security risks related to Kaspersky IT security software, and the agency recommended that the German private sector stop using it.[27]

Finally, Germany is taking the first furtive steps to match its allies' concern about research protection. The Federal Ministry of Education and Research (BMBF) has discreetly begun to consider means of protecting the integrity and openness of basic research programs at universities and in networks such as the Max Planck, Fraunhofer and Helmholtz institutes. This is an effort consistent with increased Commission attention to Chinese illicit research transfer.[28] Germany's unique quantum, AI, and robotics research capabilities have garnered particular attention for their attractiveness to Chinese researchers at People's Liberation Army-adjacent academic institutions.[29] China is purposeful in sending personnel affiliated with its military-academic-industrial complex to foreign universities and pressuring returning scientists for insights into their work abroad.[30] Cases of research infiltration by proxies of authoritarian militaries has become an EU concern.[31] Paradoxically, while many German universities actively shun cooperation with their own country's military and defense sector, there is little awareness of the risks of academic cooperation with individuals and research institutions embedded in the Chinese military system.

The German research community must balance screening for infiltration risks with a continued commitment to openness to global researchers, including those from China and Russia. In the United States, the crackdown on Chinese researchers has led to reputational and strategic damage to the country's attractiveness as a research and innovation hub.[32] As Germany – and the EU more broadly – reevaluate international participation in research, German academic institutions and BMBF guidance must remain centered on due diligence, respect for human rights, rule of law, proportionality, and an open German research environment.

Recommendations

In line with the rest of Europe, Germany is actively recalibrating critical-technology access and control as a function of a darkening geopolitical landscape and an ever-accelerating speed of technological development. Germany's first National Security Strategy, currently being drafted, should enable a more cohesive and controlled approach to technology governance and critical technology markets while maintaining open access to technological innovation. This will require Germany to balance open markets and other business needs with national and European security and resilience. To do this, Germany should:

Work with allies to create a 21st-century Multilateral Technology Control Committee. The new body would systematize information sharing and coordination on restricted access to strategic technology by authoritarian states like Russia and China. This body could be incubated in the TTC or G7

26 Philipp Alvares de Souza Soares, Moritz Koch and Dietmar Neuerer, „Bundesregierung droht Huawei mit Rauswurf" [Federal government threatens to expel Huawei], Handelsblatt, (July 25, 2022): https://www.handelsblatt.com/technik/cybersecurity/it-sicherheit-bundesregierung-droht-huawei-mit-rauswurf/28541284.html?utm_campaign=hb-update&utm_content=25072022&utm_medium=email&utm_source=nl (accessed October 20, 2022).

27 Bundesamt für Sicherheit in der Informationstechnik, "BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten" [BSI Warns Against Using Kaspersky Virus Protection Products], (March 15, 2022): https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html (accessed September 12, 2022).

28 Ursula von der Leyen, "2022 State of the Union Address", (September 14, 2022): https://ec.europa.eu/commission/presscorner/detail/ov/speech_22_5493 (accessed September 19, 2022).

29 Naomi Conrad, Esther Felden and Sandra Petersmann, "Are European academics helping China's military?", Deutsche Welle, (May 19, 2022): https://www.dw.com/en/are-european-academics-helping-chinas-military/a-61834716 (accessed September 19, 2022).

30 Alex Joske, "The China Defence Universities Tracker", Australian Strategic Policy Institute, (November 25, 2019): https://www.aspi.org.au/report/china-defence-universities-tracker (accessed September 12, 2022).

31 Ursula von der Leyen, "2022 State of the Union Address", (September 14, 2022): https://ec.europa.eu/commission/presscorner/detail/ov/speech_22_5493 (accessed October 20, 2022).

32 Nidhi Subbaraman, "Scientists' fears of racial bias surge amid US crackdown on China ties", Nature, (October 29, 2021): https://www.nature.com/articles/d41586-021-02976-8 (accessed October 20, 2022).

with potential docking mechanisms for other consolidated democracies like Australia and New Zealand. Its remit should include information-sharing dashboards and recommendations for dual-use import and export controls for critical technology, investment screening, trustworthy vendors, and research protection. Concerning imports, particular attention should be paid to AI-powered surveillance technology used in smart cities, digital services, and hardware. The committee could also work to level export, investment, and IP restrictions on cyber players that sell their wares to authoritarian regimes that surveil their citizens and undermine human rights. These players include Israel's NSO, which produced the notorious Pegasus spyware, and North Macedonia's Cytrox, developer of the Predator spyware.[33]

Create Foreign-Direct Product Rule- and "Entity-List" Instruments for Germany. The US Foreign-Direct Product Rule permits restricting technology exports if they were made in the United States or contain American equipment, tools, software, or proprietary IP. Most crucial technological choke points in Europe are elsewhere, but Germany has many key, hidden levers in high-tech value chains. Moreover, such instruments would help Germany to prepare in anticipation of future potential chokepoints in quantum technology and biotech where Germany could have important niche supply chain capabilities.

Start an action-oriented policy debate on research and outbound investment governance. The BMWK has begun to evaluate proper screening mechanisms and to consider ending incentives for investment in production, R&D, or joint ventures in authoritarian states that could lead to illicit technology transfer. With its EU and NATO partners, Germany should examine options for evaluating investment in autocracies without endangering open markets.[34] The BMBF should prepare for EU action in these areas by creating guidelines and making them publicly available.

Expand trustworthiness assessments beyond 5G equipment. Germany's National Security Strategy should permit more development of national instruments that invoke political and security considerations for trustworthy sourcing of technology. These instruments should go beyond the stipulations of the IT Security Law 2.0 and the EU Toolbox for 5G Cybersecurity and apply to areas including smart city, smart grid, and satellite technology. Such integration has been standard in US policy but is now seen in the United Kingdom's 2021 Integrated Review of Foreign Policy, Defence, Security and International Development,[35] and in Japanese economic security policy. Funding should be made available for assessing hidden economic and security externalities of relying on untrusted vendors. These externalities include "rip and replacement" of core technology in 5G/6G and smart city critical infrastructure, and in screening and surveillance technology procured by cities and the *Länder*.[36]

Encourage European participation in emerging Indo-Pacific technology access and control arrangements. Greater strategic convergence between Europe and other democratic actors is key to creating a robust, reliable market for critical technologies. Through the EU, Germany should push for Europe to pursue more geo-economic and technological engagement with the Indo-Pacific. The EU could participate in the burgeoning cooperation among democratic semiconductor production powerhouses, such as the United States, Taiwan, Japan, and South Korea (see the nascent Chip 4 Alliance). In this forum, the EU could help secure free movement of chip design, IP, and production, and co-shape access rules that hinder illicit technology and IP transfer.[37]

33 Ryan Gallagher, "Spyware Vendor FinFisher Claims Insolvency Amid Investigation", Bloomberg, (March 28, 2022): https://www.bloomberg.com/news/articles/2022-03-28/spyware-vendor-finfisher-claims-insolvency-amid-investigation (accessed September 19, 2022).

34 Inu Manak, "Outbound Investment Screening Waits in the Wings", Council on Foreign Relations, (August 15, 2022): https://www.cfr.org/blog/outbound-investment-screening-waits-wings (accessed October 20, 2022).

35 The Cabinet Office, "The Integrated Review 2021", (March 16, 2021): https://www.gov.uk/government/collections/the-integrated-review-2021 (accessed September 12, 2022).

36 Johannes Rieckmann and Tim H. Stuchtey, "The Hidden Cost of Untrusted Vendors in 5G Networks – State of Discussion and Estimations for Germany", Brandenburgisches Institut für Gesellschaft und Sicherheit, (March 2021): https://www.bigs-potsdam.org/publikationen/the-hidden-cost-of-untrusted-vendors-in-5g-networks-state-of-discussion-and-estimations-for-germany (accessed September 19, 2022).

37 Arjun Gargeyas, "The Chip 4 Alliance Might Work on Paper, But Problems Will Persist", The Diplomat, (August 25, 2022): https://thediplomat.com/2022/08/the-chip4-alliance-might-work-on-paper-but-problems-will-persist/ (accessed September 12, 2022).

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 25 42 31 -0
info@dgap.org
www.dgap.org
@dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Editing Andrew Cohen

Layout Luise Rombach

Design Concept WeDo

Author picture(s) © DGAP

Cover Photo © IMAGO/Kosecki