A German Digital Grand Strategy: Integrating Digital Technology, Economic Competitiveness, and National Security in Times of Geopolitical Change

Barker, Tyson (Ed.); Hagebölling, David (Ed.)

Veröffentlichungsversion / Published Version
Sammelwerk / collection

German Council on Foreign Relations

No. 7
November 2022

DGAP REPORT

A German Digital Grand Strategy

Integrating Digital Technology, Economic Competitiveness, and National Security in Times of Geopolitical Change

Tyson Barker
Head, Technology and
Global Affairs Program

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

BIOGRAPHY OF THE AUTHORS

Tyson Barker joined the German Council on Foreign Relations (DGAP) in October 2020 as head of its Technology and Global Affairs Program. He previously worked at Aspen Germany where, as deputy executive director and fellow, he was responsible for the institute's digital and transatlantic programs. Prior to that, Barker served in numerous positions including as senior advisor in the Bureau for European and Eurasian Affairs at the US State Department and director for transatlantic relations at the Bertelsmann Foundation. He has written for numerous publications on both sides of the Atlantic including Foreign Affairs, Foreign Policy, Politico, The Atlantic, The National Interest, and Der Spiegel.

Dr. David Hagebölling is an associate fellow in DGAP's Technology and Global Affairs Program. Hagebölling is also a senior scientist at the Hasso Plattner Institute's (HPI) Internet Technologies and Systems Research Group. He was a research fellow at DGAP from May 2021 to June 2022. Previously, he was a guest researcher at the WZB Social Science Research Center Berlin and at the Technical University of Munich. Hagebölling also gained professional experience at the Federal Foreign Office, the Federal Ministry of Economic Affairs and Energy, and the German Investment Corporation. He conducts research and advises primarily on questions relating to German and European digital foreign policy, internet and cyber governance, and international technology cooperation.

ACKNOWLEDGEMENTS

This report is the product of a year's worth of research, discussion, deliberation. and debate with a cross-section of experts from policy, the private sector, think tanks, academia and IT across Germany and Europe. We would like to thank the individuals and institutions that made this report possible. First and foremost, we would like to express our particular gratitude to the 38 working group members who convened numerous times and provided individual guidance as we developed the characterization and recommendations found in this report. We would also like to thank the 15 impulse speakers who framed the questions we addressed in our work.

Our deep gratitude also goes to the in-house support we received from our DGAP colleagues. Their unique contributions proved invaluable to this report. We appreciate the leadership and guidance of Guntram Wolff and Roderick Parkes in each step of this process. We would like to acknowledge the Technology and Global Affairs team of Anke Schlieker, Anthon Klerck, Valentin Weber, Katja Muñoz and Tim Rühlig as well as former team members Brittany Demogenes, Isabeau Höhn, Martin Kümmel, Julian Heiss, Afra Herr, Louisa Biffar, Christoph Mayer, Diego von Lieres, Jonas Winkel and especially Richard Skalt for their support, research, and revisions.

We are also grateful to Andrew Cohen who edited this draft, the DGAP communications team, Wiebke Ewering, Lara Bührer, Luise Rombach and Jana Idris for producing this report, and the DGAP events teams, particularly Yulia Loeva, for their assistance in organizing the workshops and rollout event.

Finally, we express our deep appreciation to the Open Society Initiative for Europe for their support, which has allowed to realize this ambitious project. We would also like to thank the Hasso Plattner Institute and its director, Christoph Meinel, for their academic support and partnership throughout this process, without which this report would not have been possible.

EXECUTIVE SUMMARY

Germany is facing an unprecedented era of techno-geopolitical competition. Even amid Russia's war on Ukraine, rising energy prices, inflation, climate change, and pressure for economic recovery and fiscal consolidation, a burst of development in general-purpose technology is bumping up with increasingly fraught US-China technology competition.

Germany cannot ignore the implications of this. To safeguard its economic and technological competitive advantages, it must knit together its domestic and international capacities and policy objectives in digital technology. The country must do this by anchoring its doctrine of digital sovereignty in six interrelated building blocks based on the principle of "freedom to choose": supporting an environment for indigenous innovation; promoting open competition of ideas and technologies; establishing clear rules that bring a democratic, human-centric order; restoring informational self-determination to European and global users; limiting carbon emissions and guaranteeing technological sustainability; and implementing penalties with teeth for rule breakers. A "third-way" approach to its digital technology posture – equidistant between the United States and China – is not an option for Germany. Germany and the EU should work with other like-minded states – first and foremost with the United States – to harness their collective weight of market size, access, and innovation industrial bases to tie together the rules, values, and reciprocity that act as mutually reinforcing instruments in a democratic technology governance order. At the same time, Berlin must incorporate stabilizers into its innovation industrial base that protect it, and Europe, from vulnerabilities caused by increasingly tense technological competition between the world's two great technology powers.

Germany's success in the ongoing effort to forge a digital grand strategy depends on its ability to foster a "networked mentality" that can establish consensus within the federal government; among national, state, and local policymakers; and between the public and private sectors. While Germany's August 2022 Digital Strategy represents a good first step toward concrete, measurable objectives for its digital modernization, Germany's focus remains too domestic, unable to simultaneously address short-term trends ("the sprint") while developing strategic foresight to plan for mid-term trends ("the marathon") and their national and international impact. The iterative (*Schritt-für-Schritt*) approach that has defined German digital policy has allowed four strategic gaps – in data, adoption, investment and commercialization, and cyber – to emerge. The document also remains too narrowly focused on the four B's: *Bund-Land* (German federalism); *Bürokratie* (public administration IT consolidation and digitization); *Breitband* (broadband and other connectivity infrastructure); and *Bildung* (digital education). All are necessary but insufficient.

This report takes a systematic approach to outline the state of play in digital policy and Berlin's current policy approach, and it provides recommendations for strengthening German efforts to build a confident, high-performing European digital economy embedded in an open, democratic, and rules-based digital order. This report puts forward 48 recommendations in seven policy areas that layer on top of each other to build to a cohesive whole, a sort of "technology policy stack." Together, the recommendations form the basis of an integrated approach to international digital policy that reflects the seven layers of the technology policy stack. The recommendations in the following sections include:

Chapter 1

Digital Sovereignty as Germany's Leitmotif in a Global Context

Push a clearly articulated "rules-centric" doctrine of digital sovereignty rooted in freedom to choose, open markets, and human rights. As Europe operationalizes strategic technology projects and rules on cloud computing, semiconductors, 5G/6G mobile networks, and quantum computing, the German government must shed a counterproductive ambiguity around the notion of digital sovereignty.

Ensure ministry staff and digital policy units, especially at the expanded Federal Ministry for Digital and Transport (BMDV), think geopolitically. The ministry should establish interagency meetings to assess the geopolitical impact and determine the geostrategic implications of digital and technology regulation and policies. This requires boosting the role of the Federal Foreign Office (AA) and Federal Ministry of Defence (BMVg) in technology policymaking.

Draft a Comprehensive Technology and Foreign Policy Action Plan that links the Digital Strategy with the pending National Security Strategy. As a follow-on to the Digital Strategy, the BMDV, the AA, and the Federal Ministry for Economic Affairs and Climate Action (BMWK) should draft an action plan that links domestic and European issues regarding industrial policy for and regulation of the technology sector with foreign policy issues relevant to techno-authoritarianism, setting international standards, internet governance, and technology alliances.

Establish the position of technology ambassador-at-large with three senior deputies that can operationalize German digital technology and foreign policy. The AA should establish an ambassadorship-at-large, with state secretary rank, specifically to marshal this action plan. The structure under the ambassador-at-large should include deputies addressing cybersecurity, the digital economy, and digital rights to guarantee an able, cohesive, international expression of Germany's technology policy objectives.

Increase the agility of digital federalism. Germany must strengthen the interoperability, innovation complementarity, and technology-security assessments of federal and state (*Bund* and *Länder*) governments to build scalable technology on a European and, ultimately, global level. Domestic efforts in this area are, therefore, a foreign policy issue. Germany could, for example, support an "app store" for digital tools related to education, healthcare, and policing. The federal government could also strengthen conditionality among its funding incentives for technology procurement through cyber and vendor guidelines that align with national, EU, and NATO security concerns.

Establish a cross-committee, parliamentary Technology Foreign Policy Working Group. Such a body would ensure consistency in approaches to policy areas ranging from federalism to democratic technology alliances.

Chapter 2
Assessing the Strengths and Challenges of Germany's Innovation Ecosystem

Incentivize coordination among innovation-promoting institutions. Germany's innovation agencies should create a national strategic technology council and a formalized interagency meeting process to compare strategic objectives, test potential cooperation, identify broader obstacles, and consider research into dual-use technology and its applications.

Emphasize complementarity between the *Zeitenwende* and German innovation in dual-use technologies. The €100 billion *Zeitenwende* outlay must link defense modernization with basic research and development (R&D) capacity in dual-use innovation, including in defense software. As part of the mentality shift in the *Zeitenwende*, the *Länder* and universities must work with the federal government and the private sector on common-sense use of the *Zivilklausel*.

Commit to reliable capital investment focused on industrial platforms, the Internet of Things (IoT), and deep and green digital technology. Germany should consider a scheme to bundle the Future Fund with institutional investment in an embryonic German Sovereign Wealth Fund, with a proportion of financing specifically directed toward strategically important venture-capital endeavors.

Create sandboxes – research spaces shielded from the constraints of regulation, red tape, and public procurement requirements – at publicly funded research institutions and agencies. Research institutions and innovation agencies would benefit from public sector funding requirements for contracting and tendering, evaluation, and long-term planning that can keep pace with rapid global innovation.

Encourage private sector engagement with "expeditionary investment" in, and acquisition of, technology champions and startups outside Europe. Germany's leading firms, supported by the German government, need to adopt an expeditionary, or "going-out," mentality for foreign and direct investment (FDI) to gain access to innovation breakthroughs, diverse organizational and management philosophies, and key intellectual property (IP).

Consider high-end R&D access in geostrategic terms. The government should examine potential defensive instruments to prevent "IP leakage," particularly in deep technology. These instruments should guarantee, however, the continued importance of Germany's openness as a global research environment.

EXECUTIVE SUMMARY

Recast the Digital Single Market as a geopolitical priority. Germany should lead efforts to complete the digital single market, including those aimed at encouraging the free flow of data and sector-specific data spaces across the EU. Such efforts should also simplify startup registration and build a unified capital market that encourages cross-border investment.

Consider the information and communications technology (ICT) talent pipeline to be critical infrastructure. Research institutes must offer the computing power, resources, research infrastructure, competitive salaries, and hiring flexibility that their American, British, and Chinese counterparts do.

Chapter 3

Safeguarding Germany's Technology Stack and Innovation Industrial Base

Undertake a comprehensive mapping of goals and capacities in critical technology. Mirroring partners' efforts, the German government should gauge the strength and exposure of key critical technologies in terms of leadership, peer status with competitors, and necessity to mitigate dependency risks.

Increase strategic industrial policy cohesiveness between federal and state governments as well as among the *Länder*. Germany should prioritize ensuring that states' industrial policies align with national technology objectives. Senior state officials, research consortia, and industry could use this effort to identify synergies.

Expand transnational industrial consortia in Europe and among like-minded states. Germany should foster cross-border innovation-industrial consortia by advocating a streamlined Important Projects of Common European Interest (IPCEI) notification process and schemes for foreign suppliers from like-minded states to amplify positive spillover effects.

Focus on domestic – and European – competitive advantages and strategic interdependencies within a larger community of like-minded partners. Germany should design its industrial policy to promote a larger community of like-minded partners that has the EU at its core but includes key partners such as the United States, Japan, and South Korea. The policy should have three distinct goals: IT security, supply chain resilience, and industrial competitiveness.

Structure public procurement to mitigate IT-security and supply chain vulnerabilities. Germany's largest purchaser of IT systems is its federal government, which can leverage its purchasing power to reduce strategic vulnerabilities, particularly in security-critical layers of its technology stack.

Chapter 4

Shaping the Global Technology Rule Book in the Service of Europe

Address the political trade-offs associated with digital regulation choices. The most difficult aspects of digital regulation often pit key German priorities, such as privacy and security, against each other. Policymakers must be clear-eyed about how they rank objectives when crafting regulation.

Draft model clauses and modules that can be integrated into partner countries' regulation. This could involve creating an open source regulation repository that expedites the process for non-European partners to achieve adequacy with the EU on personal and industrial data flows, IoT security, and content moderation, and to address challenges regarding the General Data Protection Regulation (GDPR).

Conduct geopolitical impact assessments of draft German and European digital regulation. German and EU measures could inadvertently strengthen digital authoritarianism or enable unintended and unwanted global trends such as data localization, censorship, weakened cybersecurity, or internet fragmentation. Candid assessments of the impact of German and EU technology policy outside Europe could anticipate and mitigate such consequences.

Fight creeping state-centrism of European technical standard-setting. Technical standard-setting should not be left solely to the private sector. Yet Germany has an acute interest in balancing private sector leadership with national and European interests.

Bolster private sector technical standard-setting capacity. Germany should introduce tax incentives and public funding mechanisms for domestic companies, startups, and associations to participate in standard-setting bodies, seek chairmanships, field draft standards, and work with like-minded states.

Embed high European Cloud Certification and Gaia-X Architecture of Standards into global cloud governance efforts. As industrial data could become a new frontline in global technology regulation, Germany should examine ways to internationalize its data space model, Gaia-X, to include non-European powers, especially the United States. Germany should also support building the capacities of Global Gateway partner countries to use European cloud computing architectures, thereby increasing interoperability and safeguarding human rights.

Integrate digital regulation and technological standard-setting into the *Zeitenwende* and the National Security Strategy. Germany must consider more intently the effects of digital regulation on its national security posture and defense industry. The country must ensure it can adopt and deploy dual-use technology on par with peer nations such as France, Canada, Japan, and the United Kingdom.

Increase the engagement of Germany's foreign policy and national security communities in shaping and enforcing regulatory agreements. German intelligence, foreign policy, law enforcement, and defense agencies have roles in enforcing national technology regulations. It is time for these authorities to assume more prominence, including in the post-Privacy Shield Data Privacy Framework (DPF) era.

Establish a multistakeholder approach that incorporates civil society, the private sector, and other non-state actors. Germany – and Europe – have begun pioneering new models of managing and enforcing technology regulation. Such flexible structures allow for constant oversight that is subject to compromise.

Expand reviews and sunset clauses in digital regulation to encourage flexibility. Review and sunset clauses would compel regulators to consider the effectiveness and relevance of rules. Such clauses would also support consistency with regulation in other democracies.

Chapter 5

Optimizing Export Control, Investment Screening, and Market Access Instruments

Work with allies to create a 21st-century Multilateral Technology Control Committee. The new body, which could be incubated in the EU-US Trade and Technology Council (TTC) or the G7, would systematize information sharing and coordination on restricted access to strategic technology by authoritarian states such as Russia and China. Its remit should include information-sharing dashboards and recommendations on dual-use export and import controls of critical technology, investment screening, trustworthy vendors, and research protection.

Create Foreign-Direct Product Rule and "Entity List" Instruments for Germany. Germany has many key, hidden levers in high-tech value chains. Such instruments can help the country prepare for future potential chokepoints in quantum technology and biotech, sectors in which Germany could have important niche supply chain capabilities.

Start an action-oriented policy debate on research and outbound investment governance. With EU and NATO partners, Germany should look at proportionate means to monitor and evaluate outbound investment behavior in autocratic regimes while continuing to defend open investment markets. The Federal Ministry of Education and Research (BMBF) should further anticipate EU action on research integrity by creating review guidelines and making them publicly available.

Expand trustworthiness assessment processes beyond 5G mobile network equipment. The German National Security Strategy should allow for deeper development of national instruments to restrict the use of certain technologies (e. g., smart cities, screening, AI, and satellite technology) on the basis of political and security considerations. These schemes should differentiate between NATO, EU, and bilateral treaty allies and consolidated democracies on the one hand and non-EU/-NATO and authoritarian states on the other.

Encourage European participation in emerging Indo-Pacific technology access and control arrangements. Greater strategic convergence between Europe and

other key democratic actors is crucial for creating among them a robust, reliable market for critical technologies such as semiconductors. Through the EU, Germany should push for Europe to be an active part of enhanced geo-economic and technological engagement in the Indo-Pacific.

Chapter 6

Strengthening International Technology Alliances, Partnerships, and Norms

Advance the notion of a democratic technology trust zone. This trust zone would regulate flows of skills, capital, and data to boost competitiveness and trustworthiness for strategically important ICT infrastructure such as network equipment and that for cloud/edge service providers and smart city applications.

Establish a global connectivity doctrine with open internet access as a fundamental right. Germany should work with EU member states and other like-minded democracies to devise jointly financed "connectivity packages" that bundle digital infrastructure assistance with cyber capacity-building. Cooperation should also be established to narrow the digital divide in the Global South and maintain open information flows during authoritarian-driven internet shutdowns and in conflict zones.

Create a German Open Tech Foundation (GOTF). The recently launched Sovereign Tech Fund should be complemented with a German Open Tech Foundation to provide international funding for the development of democracy-affirming and privacy-enhancing technologies in line with the government's understanding of digital sovereignty. This funding should be directed primarily toward communities in the Global South.

Counter politicization of critical and emerging technologies standard-setting. As the weight of non-market economies in standard-setting bodies (SSBs) grows, Germany should initiate an international study group that identifies whether and which political instruments may be used by such actors to capture standard-setting for critical and emerging technologies. This should form the basis for coordinated engagement with SSBs on ensuring the primacy of technical criteria and preserving the SSBs' reputation for impartiality.

Work to avoid the emergence of a digital Non-Aligned Movement. In 2022, Germany has already revived its digital dialogue with India and included the country in this year's G7 guest list. Given India's 2023 G20 presidency, Germany should now build on its engagement to emphasize India's democratic responsibility to champion an inclusive digital agenda centered on climate-friendly technology, and open and free connectivity.

Engage collaboratively in EU-US technology dialogue, especially in the TTC. Germany should create a bilateral digital dialogue with the United States that can align and amplify policy deliverables from the TTC.

Create asymmetric technology alliances with subnational governments. Cities and states are increasingly assuming digital governance responsibilities that national governments are unwilling or unable to undertake. Germany, in line with the European Council's new digital diplomacy conclusions, should work with subnational governments to build technology alliances that reflect German and EU regulatory values, and support subnational adoption of cyber and internet governance norms.

Chapter 7

Emerging and Disruptive Technologies, the German Military, and the *Zeitenwende*

Commit two percent of the €100 billion *Sondervermögen* to fostering disruptive defense R&D. The German government should commit at least two percent of the *Sondervermögen* to acquiring disruptive defense technologies. This would incentivize venture capital funding for new defense startups and increased R&D spending by Germany's established defense companies.

Connect the ethical debate on military EDTs to operational realities. High-level discussions on ethics in Germany are frequently disconnected from operational realities. Debate should focus on appropriate degrees of machine autonomy and justifiable purposes for the use of EDTs.

Link dual-use implications of EDTs with innovation industrial policy. The new National Security Strategy

should include a section unifying technology and innovation industrial policies, including those relevant to defense, and link them to a governmental assessment of key national security threats.

Augment knowledge transfer among military and civilian R&D. The German government should expand links between the Munich-based Digitalization and Technology Research Center of the *Bundeswehr* (dtec.bw) and Bavaria's high-tech startups. The government should facilitate a separate Track II platform for innovators that facilitates discovering dual-use applications for EDTs developed with the support of innovation agencies, including SPRIND and the Cyber Innovation Hub. The government should also create incentives, such as fund matching, for German and European venture capital investment in defense technology startups.

Align defense procurement with technology innovation cycles. Defense budget fluctuations stifle the ability to support lengthy EDT innovation cycles. The government should establish a dedicated fund for disruptive defense technology with annual minimum budget guarantees through 2030.

Maintain allies' interoperability through joint principles and military formations. The German government must ensure that EDT-related transformations do not undermine interoperability with allied forces. It should promote development of common ethical principles and codes of conduct, such as those defined in NATO's AI strategy.

CHAPTER OVERVIEW

The Sprint and the Marathon

Geopolitical competition between incumbent and rising powers, democratic and authoritarian systems, and rules-oriented multilateralists and power-based unilateralists has led to a marked increase of weaponized interdependence.[1] Germany – and Europe – are confronted with a new reality in which access to and control over flows, hubs, and choke points – in trade, finance, energy, raw materials, oligarchic networks, and even food – are being deployed as part of an arsenal of low-intensity global conflict.

This is especially true in technological connectivity. The United States, China, and their Big Tech affiliates in AI, Cloud, platform, chip technology, and elsewhere have asymmetric control of key nodes. The increasingly general-purpose nature of certain foundational technologies for economic, political, and military competitiveness sharpens the inherent dangers of this situation for Germany and Europe.

Against this backdrop, Germany has begun to grapple with a new whole-of-government approach to digital technology. In August 2022, the German cabinet agreed to a first-of-its-kind Digital Strategy. The strategy, written by the BMDV, focuses on three action areas: a networked and digitally sovereign society; innovation in the economy, the workforce, science, and research; and the digital state. The strategy also establishes a number of concrete "Enabling Projects," particularly on norms and standards, data availability, and digital identities.[2]

But even as Berlin's Digital Strategy begins to tackle the need to break ministerial silos and integrate the private sector into a federated policy approach to digital technology, Germany remains too disconnected from the geopolitical threats that already confront it.[3] It falls short in anticipating technological developments and preparing for them in line with Berlin's policy objectives (see Figure 1). Recent German governments' cautious digital policies focused preponderantly on near-term digital conditions, and these policies proved insufficient for addressing emerging challenges, such as the impact of new technologies on innovation, the industrial base, and an international system inextricably linked through technology, economic competitiveness, ideology, and security. As such, these policies also constrained the ability to anticipate and shape important mid-term technological developments.

Moreover, German digital policymaking often exhibited a geographic myopia, characterized by a heavily domestic focus. To its credit, though, Germany's 2022 Digital Strategy attempts to break the narrow fixation on the infrastructure that enables digitization, with the following areas, or four "B's," at its core:

***Bund-Land* (German federalism):** establishment of an agreement among the national and *Länder* (state) governments on interoperable approval processes, IT interface standardization, and public administration multi-cloud strategy

***Bürokratie* (public administration IT consolidation and digitization):** government portals for submitted materials that will be interoperable with EU systems by 2025; establishment of a public administration cloud strategy (the *Deutsche Verwaltungscloud-Strategie* or DVS) and criteria for sustainable data centers based on secure and, ideally, open source software and data storage procurement standards; e-ID standards; publicly available data and implementation of the Open Access Law (*Online-Zugangsgesetz* or OZG)

***Breitband* (broadband and other connectivity infrastructure):** expansion of Germany's 7.5 million fiber optic connections to cover rural regions through the "White Spots" program; mobile connectivity in rural areas and on public rail; extended spectrum licensing; a *Gigabit-Grundbuch* (gigabit register that contains information relevant to enlarging digital infrastructure) with clear guidelines for expanding ICT connectivity infrastructure

1 Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," in: *International Security*, 44, no. 1 (July 2019), pp. 42-79: https://direct.mit.edu/isec/article-abstract/44/1/42/12237/Weaponized-Interdependence-How-Global-Economic?redirectedFrom=fulltext (accessed October 5, 2022).

2 Noticeably absent, however, was an accompanying budget for the strategy's implementation.

3 For instance, China is mentioned once in the 52-page document. Federal Ministry for Digital and Transport, "Digitalstrategie. Gemeinsam digitale Werte schöpfen" [Digital Strategy. Collectively creating digital values], (2022): https://digitalstrategie-deutschland.de/static/1a7bee26afd1570d3f0e5950b215abac/220830_Digitalstrategie_fin-barrierefrei.pdf (accessed October 5, 2022).

***Bildung* (digital education).** Digital Pact 2.0 until 2030 with cloud and software tools in a so-called National Education Platform based on Gaia-X and hardware maintenance; building on digital tools available to the *Länder*

While this is all necessary, Germany is coming to terms with the reality that an approach centered on the four B's is insufficient. The German government – in collaboration with the domestic private sector, research community, and civil society – must strengthen its ability to anticipate and react to developments in the short term (the "sprint") while developing strategic foresight to plan for mid-term trends and their impact (the "marathon"). Balancing the two undoubtedly poses challenges for policymakers. Too great a focus on short-term issues risks insufficient digital planning. Too great a focus on the mid-term risks overlooking the steps needed to undertake immediate action.

The friction between near-term and mid-term technological development extends to the German private sector's approaches to digital policymaking. This has led to the emergence of four gaps vis-à-vis xglobal peers that must be addressed:

Data gap: Studies on the direct impact of the the GDPR and other data regulation on innovation in Europe are inconclusive. At times, this regulation slows the availability and velocity of data processing. At other times, it opens new avenues for innovation.[4] But the depth of European data markets remains limited compared to that of other democracies, such as the United States. Moreover, the push for greater data localization – within the EU and globally – could exacerbate this trend. Efforts to encourage data altruism at the European level (through the Data Act and Data Governance Act), emancipate public data for commercial use, and push data spaces in areas such as health and mobility are all promising. But they remain aspirational. At the same time, data sharing faces a cultural barrier.

Adoption gap: German industry, particularly its *Mittelstand* and small businesses, continues to lag in cloud adoption, which is increasingly the gateway to industrial digitization and to the platform on which other digital services in AI, cybersecurity, and data analytics become available.[5] Germany as a whole ranks 20th out of 27 EU member states on cloud adoption.[6] German industry's ability to withstand the blow from its slow adoption of the initial software and internet revolution was possible because its niche capabilities preserved their global competitiveness. And yet, the potential impact of emerging technologies beginning to sweep across industries represents a significant – if not existential – risk to some core business models.

Investment and commercialization gap: While the government aims to invest upp to 3.5 percent of GDP in R&D, private sector-driven R&D is leading emerging-technology investment outside Europe. The US has 50 percent of top private sector investors in quantum computing. China has 40 percent. Europe has none. Europe attracts only 12 percent of global AI private sector funding compared to the United States' 40 percent and Asia's 32 percent.[7] The commercialization mismatch is clear: Europe is leading in patents in only two of ten key enabling technologies.[8] This occurs even as basic research output in Europe, with Germany as its leader, remains on par with the United States and China.[9]

Cyber gap: Persistent incidents in German IT systems – involving IP theft, ransomware attacks on municipalities and hospitals, politically-motivated

4 Crispin Niebel, "The impact of the general data protection regulation on innovation and the global political economy," in: *Computer Law & Security Review*, (April 2021), pp. 1-15: https://www.sciencedirect.com/science/article/abs/pii/S026736492030128X (accessed October 5, 2022).

5 Tyson Barker, "Into the clouds: European SMEs and the Digital Age," Atlantic Council, (October 2016): https://www.atlanticcouncil.org/wp-content/uploads/2016/10/Into_the_Clouds_web_1011.pdf (accessed October 5, 2022).

6 European Commission, "Digital Economy and Society Index (DESI) 2021 Integration of digital technology," SCRIBD: 3_DESI_2021_Thematic_chapters__Integration_of_digital_technology_umQXbSLQ9FpmtmS8rGgaTi7AKcg_80555.pdf (accessed October 5, 2022).

7 Sven Smit et. al, "Securing Europe's competitiveness: Addressing its technology gap," McKinsey Global Institute Report, (September 22, 2022): https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/securing-europes-competitiveness-addressing-its-technology-gap (accessed October 5, 2022).

8 Jan C. Breitinger, Benjamin Dierks, and Thomas Rausch, "World class patents in cutting-edge technologies: The innovation power of East Asia, North America, and Europe," Bertelsmann Stiftung, (June 3, 2020): https://www.bertelsmann-stiftung.de/en/publications/publication/did/world-class-patents-in-cutting-edge-technologies (accessed October, 26 2022).

9 The EU has 18 percent of global AI researchers who have published approximately 15,000 academic papers on AI; the United States has 20 percent of the global AI researchers' stock. Kaan Sahin and Tyson Barker, "Europe's Capacity to Act in the Global Tech Race Charting a Path for Europe in Times of Major Technological Disruption," DGAP Report No. 6, German Council on Foreign Relations (April 2021): https://dgap.org/sites/default/files/article_pdfs/210422_report-2021-6-en-tech.pdf (accessed October 5, 2022).

1 – DIGITAL TECHNOLOGY DEVELOPMENTS: GERMANY MUST ANTICIPATE AND PLAN FOR BOTH

THE SPRINT (NOW AND NEAR TERM)	THE MARATHON (MID-TERM)
Narrow AI: AI that focuses on a limited spectrum of tasks	General adoption of highly accurate AI algorithms on track to artificial general intelligence, the ability to perform any intellectual task a human can perform
Internet of Things (IoT): machine-to-machine (M2M), human2machine interface; greater use of industrial data	Biometrics: greater merger of personally identifiable information (PII) and non-PII data; human and machine connections to the digital world
5G: advanced IoT; smart cities, factories, and homes; autonomous driving, crisis management, and policing	6G: immersive augmented reality/virtual reality (metaverse) and hologram usage
American Big Tech dominance in Europe	Chinese and American Big Tech presence in Europe
Oligopolistic data-driven platform models: targeted advertising and data mining; potentially atomized social media landscape, and closed messaging services and groups	Fewer Western-dominated platform models: subscription-based, e-commerce-driven digital currency (potential for state tracking)
Hyperscaler-based cloud computing	Fusion of cloud/edge/telecommunications infrastructure
Brussels Effect: EU market size as the basis for regulatory power (US GDP relative to world GDP: 23 percent in 2010, 25 percent in 2020; EU GDP relative to world GDP: 21.5 percent in 2010, 17.1 percent in 2020)	Constrained EU regulatory hegemony due to accelerated relative GDP decline
Undersea cables; low Earth orbit (LEO) satellite networks and VSAT reception (very small aperture terminal; a small Earth station used to transmit and receive data)	Decentralized, distributed ledger-based internet (Web3); quantum internet
High-performance computing	Exascale computing: digital twinning; hyper-complex synthetic realities
Global internet (application and protocol layers): Domain Name System, Transmission Control Protocol/ Internet Protocol (TCP/IP), Internet Assigned Numbers Authority (IANA), Internet Engineering Task Force (IETF)	Splinternet: China's 6G internet redesign to build "intrinsic security" into the internet; Internet Governance Forum + (IGF+) 2025; World Summit on Information Society (WSIS+20)

Source: Author's own illustration

hacks such as the 2021 Bundestag election interference,[10] and unintended collateral damage[11] – have intensified since the pandemic. The volume and sophistication of attacks by state actors, such as China and Russia, and by state-adjacent and non-state actors are increasing. Germany has been at the forefront of drafting cyber controls and standards to confront this changing threat environment.[12] Within the EU, Germany is signaling the multi-domain consequences – from sanctions to attribution – for below-threshold action through the Cyber Diplomacy Toolbox. Outside the EU, Norway's Sovereign Wealth

10 *Der Spiegel*, "EU wirft Russland vor Bundestagswahl gezielte Cyberangriffe vor" [EU accuses Russia of targeted cyberattacks ahead of German federal elections], (September 24, 2021): https://www.spiegel.de/netzwelt/netzpolitik/eu-wirft-russland-vor-bundestagswahl-gezielte-cyberangriffe-vor-a-9ee768d4-007a-418c-9bdc-f99e4cd590b0 (accessed October 5, 2022).

11 Maria Sheahan, Christoph Steitz and Andreas Rinke, "Satellite outage knocks out thousands of Enercon's wind turbines," Reuters, (February 28, 2022): https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28 (accessed October 5, 2022).

12 This applies in areas from IoT to routers to recent Federal Office for Information Security (BSI) cyber guidelines on Low Earth Orbit satellites. Catherine Stupp, "Germany Offers Model for Space-Industry Cybersecurity Standards," *The Wall Street Journal*, (August 17, 2022): https://www.wsj.com/articles/germany-offers-model-for-space-industry-cybersecurity-standards-11660728604 (accessed October 5, 2022)

Fund has acknowledged that cyber security is a leading source of systemic economic risk.[13]

In each of these four instances, Germany's previous iterative ("*Schritt-für-Schritt*") approach proved ill-equipped to address emerging challenges such as the impact of new technologies on innovation and the country's industrial base, and an international system inextricably linked through digital technology, economic competitiveness, national security, and, increasingly, ideology. Success in these areas will come only if Germany ultimately shapes a confident, high-performing European digital economy embedded in an open, democratic, and rules-based order. The need to achieve this is particularly acute as prospects grow for internet fragmentation, data localization, and a growing role for technology in exporting governance models. The need is also acute because digital dependency is a geopolitical vulnerability.

Digital Sovereignty as Germany's Leitmotif in a Global Context

To tackle the four gaps, and near- and mid-term technological development, Germany needs an integrated approach that knits together its domestic and international digital technology capacities and objectives. Such an integrated strategy requires the attention and support of representatives across policymaking institutions including the Bundestag, ministries, the EU, the *Länder*, the private sector's incumbent and startup communities, and other partners in Europe and beyond. This is the only way to forge common goals and approaches.[14]

Germany should give allies and adversaries alike a clear understanding of the comprehensive whole of its international digital policy. This policy should be embedded in Germany's role as a leading EU member and built around six interrelated building blocks based on the principle of **"freedom to choose"**.[15]

Supporting an environment for indigenous innovation. The policy should create stronger links among state-backed R&D efforts, commercialization, and industrial policy in emerging technological areas such as AI, quantum, advanced chips, and cloud computing.

Promoting open competition of ideas and technologies. The policy should avoid lock-in effects and diversify vendors to build supply resilience into critical technology and raw materials sourcing. It should build strategic interdependencies with like-minded states, pragmatically promote open source software, force proprietary systems to become interoperable, and privilege a bottom-up, multistakeholder approach to setting standards.

Establishing clear rules that bring a democratic, human-centric order. The policy should regulate content moderation, market power of online platforms, industrial data, cybersecurity, cloud rules, and AI to instill digital trust among Europeans and to create a global model. It should restore German and European capacity for setting technical standards.

Restoring informational self-determination to European and global users. The policy should promote data protection, end-to-end encryption, and content moderation without significantly encroaching on free speech. It should advance freedom to choose as a core principle of ICT infrastructure cooperation with the Western Balkans, Eastern Partnership countries, and the Global South.

Limiting carbon emissions and guaranteeing technological sustainability. The policy should encourage the use of emerging technology that is "Green by

13 Adrienne Klasa and Robin Wigglesworth, "Norway's oil fund warns cyber security is top concern," *Financial Times*, (August 22, 2022): https://www.ft.com/content/1aa6f92a-078b-4e1a-81ca-65298b8310b2 (accessed October 26, 2022).

14 Katrin Suder, "Staat-up," TAE Advisory & Sparring GmbH, (July 22, 2021): https://www.linkedin.com/pulse/staat-up-katrin-suder/?trk=articles_directory&originalSubdomain=de (accessed February 21, 2022).

15 Henning Kagermann, Karl-Heinz Streibich, and Katrin Suder, "Digital Sovereignty: Status Quo and Perspectives," acatech IMPULSE, (March 25, 2021), p. 9: https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder (accessed April 12, 2022).

Design", with CO2 reduction at its heart. Such technology includes cutting-edge chips and closer-to-the-source computing, energy-efficient algorithms, AI-powered energy optimization in IoT, and quantum modelling to optimize sustainable agriculture.

Implementing penalties with teeth for rule breakers. The policy should apply proportionate sanctions, investment restrictions, export controls, and loss of access to IP, data, and markets to states and technology companies – including gatekeeper platforms, telecommunication and internet service providers, hardware providers, and messaging services – that violate rules.

This approach is not as evident as it seems. The EU in recent years has balanced two conceptions of digital sovereignty and occasionally papered over deep internal tensions concerning the bloc's strategic direction in this area. The ordoliberal tradition forms the basis of a "rules-centric" approach[16] that centers on strong support for competition, clearly defined regulation, fundamental rights and open markets, and an antipathy toward network effect-based cartelization, lock-in effects, and barriers to cross-border digital services.[17] This school of thought also rests on a multidimensional understanding of sovereignty in which the state, institutions, and individuals all have a claim to digital self-determination. Some of Germany's partners, notably France and parts of the European Commission, however, endorse the other conception that involves a more "player-centric", interventionist notion of digital sovereignty centered on technological import substitution industrialization (ISI), protective tendencies, and data localization within Europe.[18]

Both conceptions of digital sovereignty have at their heart a completion of the European Digital Single Market and scalability across Europe. Both see strengthening domestic innovation capacity and reducing external vulnerabilities as strategic objectives. Both also place greater emphasis on a state interventionist role in shaping the ICT environment. But as long as both traditions co-habitat in Europe's approach to digital sovereignty – papering over core tensions and contradictions – it delays, at times, hard choices about strategic policy for the sake of consensus building.

A "THIRD WAY" OR DEMOCRATIC TECHNOLOGY GOVERNANCE WITH AN EU-US CORE?

How Germany – and the EU – interpret digital sovereignty as a framework has a direct impact on the bloc's digital grand strategy and its strategic positioning. Policymakers sometimes posit Europe's policy approach to digital technology as its own geopolitical "third way" between a more libertarian, "American" approach to technology governance and Chinese techno-authoritarianism. But such an approach to digital policy has two strategic disadvantages.

First, it strengthens a logic of digital sovereignty centered on domestic localization of data, social media, digital services, and strategic technologies to bolster industrialization and political control. This path can lend legitimacy to more authoritarian notions of digital sovereignty, such as those Russia and China promote, that allow a strong, centralized state to permeate all aspects of life to maintain order. This also risks encouraging global digital mercantilism, which carves the world into digital service and data spheres of influence that could bar European rules and players from other geographic regions.

Second, the third-way approach can limit freedom of choice by restricting technologies, and data and digital services, that benefit users and the innovation industrial base. The global slide toward data localization, a splintered internet, and closed technology stacks carved into regional or national spheres of influence should worry European policymakers. Their counterparts in New Delhi are already responding to this trend with calls for an Indian "fourth way."[19] Other aspiring digital powers

16 Former German Chancellor Angela Merkel framed this broadly accepted understanding at the 2019 Internet Governance Forum (IGF) when she stated, "In my understanding, digital sovereignty does not mean protectionism or the dictates of government agencies as to what information can be disseminated, but rather describes the ability to shape the digital transformation in a self-determined manner, whether as an individual … or as a society." Germany reaffirmed this notion in a 2021 letter signed also by the leaders of Denmark, Estonia, and Finland. Angela Merkel et. al, "Joint letter to the EU President on Digital Sovereignty," *Politico*, (March 1, 2021): https://www.politico.eu/wp-content/uploads/2021/03/01/DE-DK-FI-EE-Letter-to-COM-President-on-Digital-Sovereignty_final.pdf (accessed October 5, 2022).

17 Henning Kagermann, Karl-Heinz Streibich, and Katrin Suder, "Digital Sovereignty: Status Quo and Perspectives," acatech IMPULSE, (March 25, 2021), p. 8: https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder (accessed April 22, 2022).

18 Ministère de l'Europe et des Affaires étrangères, "Building Europe's Digital Sovereignty," (February 7, 2022): https://www.diplomatie.gouv.fr/en/french-foreign-policy/europe/the-french-presidency-of-the-council-of-the-european-union/article/building-europe-s-digital-sovereignty-7-feb-22 (accessed February 22, 2022).

19 Justin Sherman, "India's Sudden Reversal on Privacy Will Affect the Global Internet," *Slate*, (September 5, 2022): https://slate.com/technology/2022/09/india-data-protection-bill-fourth-way.html (accessed October 5, 2022).

could follow suit. If the world falls into internet regionalism and digital mercantilism, Europe, with its dependence on US digital services and East Asian hardware, would find itself at an even greater disadvantage than it does now as it tries to build its own capacity in areas including IoT, the industrial Internet of Things (IIoT), and emerging technologies such as quantum computing, blockchain, and AI. Moreover, it could lead to digital protectionism that cuts off other open digital markets, potentially robbing Germany and the EU of access, innovation, and partners in governance.

These are all threats to German – and European – digital sovereignty, which must build on concepts that are inherently universal to maintain its power. Digital sovereignty must center on individual emancipation in a global, democratic values system, even as it aims to enhance German and European technological competitiveness and resilience.

To that end, Germany and the EU should work with other like-minded states – first and foremost with the United States – to harness their collective weight of market size, technology access, and innovation industrial bases. Such cooperation could also ensure openness by tying together the rules, values, and reciprocity that act as mutually reinforcing instruments in a democratic technology governance order.[20]

In short, a "third-way" paradigm that lends itself to equidistance between the United States and China is not an option for Germany. But as Germany stands with like-minded states, first and foremost the United States, it must also build in technology industry stabilizers that protect it – and Europe – from vulnerabilities caused by an increasingly tense technological competition in which Europe aims to play a leading role. This means creating new instruments for reciprocity, market access, and technology alliance formation, and new thinking about R&D for general-purpose technology.

FIT-FOR-PURPOSE POLICYMAKING STRUCTURES

In the past, the differentiation of policy areas and diffuse responsibility across ministries has hindered effective, coordinated action that integrates R&D, industrial policy, regulation, and values into a coherent posture that promotes Germany's economic competitiveness, national security, and democratic values. The current coalition government has attempted to reform past structural weaknesses across ministries with the aim of streamlining policy and budgeting for digital issues (See Figure 2). But the need to accommodate three parties divided responsibility for technology so that it is now more widely dispersed than in prior governments. The outcome, at least as seen in the coalition agreement, likely poses significant hurdles for establishing a clearly defined vision for Germany's digital transformation and, therefore, a strong international position in the global technology race.

The BMWK controls digital competition policy and the Federal Cartel Office (*Bundeskartellamt*). It oversees implementation of the Digital Markets Act (DMA) and has important responsibilities concerning data governance, AI, and the cloud, including Gaia-X and SPRIND, Germany's experimental technology hub. It manages industrial policy for the technology sector, including EU-level IPCEIs in areas such as semiconductors, edge computing, and hydrogen energy.[21] It also retains foreign economic policy, with control of the most important instruments for overseeing technology, national security, and trade. These instruments include dual-use export control, and foreign and direct investment screening regimes. All these levers are critical for shoring up Germany's and Europe's capacity to shape digital policy and digital sovereignty.

At the same time, the BMBF maintains crucial decision-making authority for funding and contracting for basic science at institutes such as the Max Planck Society, and for applied science at the Fraunhofer Society's 75 institutes, the Helmholtz Gemeinschaft, the Leibniz Gemeinschaft, and the German Research Foundation (DFG), among others. The BMBF leads

20 The OECD countries comprise around 50 percent of global GDP; the EU and US alone represent 42 percent of global GDP and 41 percent of global trade. Germany and Europe can consider new multilateral and more normative mechanisms and objectives to leverage the combined technological innovation, and market and regulatory power of the EU, the United States, the United Kingdom, Japan, and other like-minded states.

21 Thierry Breton, "IPCEI on microelectronics – A major step for a more resilient EU chips supply chain," LinkedIn, (December 20, 2021): https://www.linkedin.com/pulse/ipcei-microelectronics-major-step-more-resilient-eu-chips-breton/?published=t (accessed February 22, 2022).

the way, with the BMWK, on shaping the new Agency for Transfer and Innovation (DATI), but the latter also oversees efforts to raise R&D spending to 3.5 percent of GDP by 2025.[22] Meanwhile, management of public sector IT consolidation, cybersecurity, protection of critical infrastructure, and lawful access to and retention of data for law enforcement remains under the auspices of the Federal Ministry of the Interior and Community (BMI). And the Federal Ministry of Finance (BMF) retains control of data-related policy, which is crucial to data infrastructure affecting data localization, industrial planning, and the terms under which American and Chinese hyperscalers can participate in public sector cloud service offerings.

The government's decision to outsource all digital responsibility and devolve coordinating staff formerly housed in the chancellery is fueled at least in part by a sense that Germany's digital transformation stagnated in the Merkel era. The decision could be a step backwards, however, since the chancellery is also the best-positioned government office to force action. It has regularly convened the digital cabinet to marshal interagency efforts and has injected input from external stakeholders into strategy and efforts to establish a digital state.[23]

There has been some consolidation that could lead to an expanded BMDV becoming the incubator for a future all-encompassing digital ministry. The shift of the BMWK's European and international digital policy units, and competent executive staff, to the BMDV could allow for a new digital czar to set policy on the international stage at the Internet Governance Forum (IGF), in the EU Digital Ministers Council in Brussels, and at other external gatherings. The BMDV also oversees telecommunications, broadband, and the Digital Services Act, and chairs the government's digital cabinet with a €500 million embryonic budget.

Germany's success in the ongoing effort to forge a digital strategy will depend on the BMDV's ability to forge a "networked mentality" that can establish consensus within the federal government; among national, state, and local policymakers; and between the public and private sectors. And cooperation between the BMDV and BMWK will be particularly crucial for assembling consistent domestic and global strategies for data governance, startups, international standards, gaming, market access and market capture by techno-authoritarians, and industrial policies for the technology sector, including digital infrastructure, and internet governance.

Recommendations

Germany's ability to pursue its strategic objectives and shape the global technology order requires all levels of government to alter their mindsets and engage in deeper interdisciplinarity. This will require a fundamental rethink in their operating systems. Seven recommendations for achieving this are:

Push a clearly articulated "rules-centric" doctrine of digital sovereignty rooted in freedom to choose, open markets, and human rights. Strategic ambiguity around the concept of digital sovereignty has outlived its purpose. As Europe operationalizes strategic technology projects and issues rules on AI, cloud computing, semiconductors, 5G/6G mobile networks, and quantum computing, the German government must shed an ambiguity that has become counterproductive.

Ensure ministry staff and digital policy units, especially at the expanded BMDV, think geopolitically. The BMDV should establish interagency meetings to assess the geopolitical implications of digital and technology regulation and policies.[24] This requires boosting the AA's and the BMVg's role in technology policymaking.[25] The German government should extend these ministries' mandates to areas beyond

22 Die Sozialdemokratische Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und die Freien Demokraten (FDP), "Koalitionsvertrag 2021-2025: Mehr Fortschritt Wagen" [Coalition Agreement 2021-2025: Dare to Make More Progress], (November 24, 2021): https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1 (accessed April 12, 2022).

23 Ryan Budish, Urs Gasser, and Melyssa Eigen, "German Digital Council: An 'Inside -Out' Case Study," Berkman Center No. 2021-3, (April 28, 2021): https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836185 (accessed February 22, 2022).

24 Policy areas such as data protection; critical technology research and development; platform regulation; cybersecurity; federal-, state-, and communal-level public procurement of hardware and digital services for education, healthcare, and taxation; and cloud and data spaces have significant geopolitical implications that are insufficiently recognized in current policymaking.

25 This should take into account alliance equities such as NATO and the EU-US relationship; broader institutional relationships in the United Nations, the Organization for Security and Co-operation in Europe, the G7, the G20, and the Council of Europe; the EU-ASEAN relationship; and, in conflict zones, hostile actors such as Russia and techno-strategic competitors such as China.

5G equipment, cyber norms, non-proliferation of weapons of mass destruction (WMD), and EDT procurement. Their portfolios should include technology research and development, technical standards, and civilian vendors for infrastructure beyond mobile network equipment.

Draft a Comprehensive Technology and Foreign Policy Action Plan that links the Digital Strategy with the pending National Security Strategy. The BMDV, with the BMWK, BMBF, BMI, AA, and BMVg, in consultation with other stakeholders, drafted the first-ever integrated German digital strategy. The BMDV, AA, and BMWK should now draft an action plan that links domestic and European technology-industrial policy and regulation with foreign policy issues relevant to techno-authoritarianism, international standard-setting, internet governance, and technology alliances. The action plan must set budgetary priorities that guarantee Germany's post-COVID-19 fiscal consolidation does not adversely affect a technological transformation that can meet the challenges of the next wave of global geopolitical and economic competition.

Establish the position of a technology ambassador-at-large with three senior deputies that can operationalize German digital technology and foreign policy. The AA should establish an ambassadorship-at-large, with state secretary rank, specifically to marshal the action plan. The structure under the ambassador-at-large should include deputies addressing cyber security, the digital economy, and digital rights who coordinate closely with other ministries to guarantee an able and cohesive international expression of Germany's technology policy objectives.[26]

Increase the agility of digital federalism. Germany must strengthen the interoperability, innovation complementarity, and technology-security assessments of federal and state (*Bund* and *Länder*) governments to build scalable technology on a European and, ultimately, global level. Domestic efforts in this area are, therefore, a foreign policy issue. Germany could, for example, support an "app store" for digital tools related to education, healthcare, and policing. The federal government could also strengthen conditionality among its funding incentives for technology procurement through cyber and vendor guidelines that align with national, EU, and NATO security concerns.

Establish a cross-committee, parliamentary Technology Foreign Policy Working Group. Such a body would ensure consistency in approaches to policy areas ranging from federalism to democratic technology alliances. The group, comprising key cross-party members of the Digital, Foreign Affairs, Economic, Interior, Finance, and Defense Committees, would focus on issues relevant to all represented portfolios.

26 The US State Department, for example, recently established a Bureau of Cyberspace and Digital Policy centered around three subsections: international cyberspace security, ICT policy, and digital freedom. This development was based largely on the 2020 Cyberspace Solarium Commission report that noted deficiencies in US foreign technology policy: https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy Office of the Spokesperson, "Establishment of the Bureau of Cyberspace and Digital Policy, US Department of State Media Note, (April 4, 2022): https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy (accessed October 5, 2022).

2 – RESPONSIBILITIES FOR DIGITAL ISSUES IN THE GERMAN GOVERNMENT

GRAND COALITION 2017 – 2021

FEDERAL MINISTRY FOR ECONOMIC AFFAIRS AND ENERGY (BMWI)

BECOMES → FEDERAL MINISTRY FOR ECONOMIC AFFAIRS AND CLIMATE ACTION (BMWK)

CHANCELLOR'S OFFICE

- No further buildup of competencies in digital policy
- A smaller part of IT planning returns to BMI
- No minister of state for digitization

Responsibilities of Group 6.2 for digital policy

FEDERAL MINISTRY OF TRANSPORT AND DIGITAL INFRASTRUCTURE (BMVI)

BECOMES → FEDERAL MINISTRY FOR DIGITAL AND TRANSPORT (BMDV)

Only two sub-departments responsible for digital policy:

- **DG1 for Digital Society and Infrastructure**, responsible for spectrum policy, mobile communications, infrastructure laws, and broadband rollout
- **DG2 for Mobility 4.0**, responsible for automated driving, satellite policy, and digitization of the construction and games industries

"AMPEL" COALITION 2021 – PRESENT

FEDERAL MINISTRY FOR ECONOMIC AFFAIRS AND CLIMATE ACTION (BMWK)

Oversees:

- **Regulatory** and **competition policy, Federal Cartel Office, DMA jurisdiction**
- Data policy, AI, and cloud, including Gaia-X and SPRIND (Division VI Sub-Department B)
- **Technology industry policy**, including IPCEI in the areas of semiconductors, edge computing, and hydrogen energy (Division IV)
- **Dual-use export controls** and **FDI screening** (Division V)

Games industry ↑

Competencies for the digital sector

Department VI for Digital and Innovation Policy

- Former head of Department VI to become civil servant state secretary at BMDV
- Parts of Division VI (Subdivisions A and B) may have responsibility for **EU digital projects**, will move to the BMDV
- Responsibilities for **national, European,** and **international digital policy**; **telecommunications**; and **Digital Services Act**

FEDERAL MINISTRY OF THE INTERIOR AND COMMUNITY (BMI)

Oversees:

- Managing public sector IT consolidation
- Issues related to **cybersecurity, critical infrastructure protection**, and **lawful access to and storage of data** for law enforcement

FEDERAL MINISTRY FOR DIGITAL AND TRANSPORT (BMDV)

Oversees:

- **Central coordination** of **digital policy**
- Two departments responsible for digital policy: Department for **Digital and Data Policy** and Department for **Digital Connectivity**

FEDERAL MINISTRY OF FINANCE (BMF)

Retains control over **data center policy**

FEDERAL MINISTRY OF FOOD AND AGRICULTURE (BMEL)

Responsibility for general and specific **product safety** (relevant for **AI regulation**)

FEDERAL MINISTRY OF THE ENVIRONMENT (BMUV)

↑ **Consumer Protection** Division

FEDERAL MINISTRY OF JUSTICE (BMJ)

FEDERAL MINISTRY OF EDUCATION AND RESEARCH (BMBF)

One-stop shop for **3.5 percent of GDP in R&D in 2025**

Retains funding decisions on contract awards for:

- **Basic research** conducted by the institutes of the Max Planck Society
- **Applied research** conducted by the 75 institutes of the Fraunhofer-Gesellschaft and research networks such as the Helmholtz Association, the Leibniz Association, and the German Research Foundation

Source: Author's own illustration

CHAPTER 2

The Geopolitics of Digital Technology Innovation

Assessing Strengths and Challenges of Germany's Innovation Ecosystem

CHAPTER OVERVIEW

Key Takeaways

1 The COVID-era public and private investment influx into Germany's digital technology R&D is reversing amid inflation, fiscal consolidation, and geopolitical pressures coming from the *Zeitenwende*.

2 Germany's future in an EU that is among the top-tier technology powers requires a profound and rapid transition of the country's R&D strengths into data-intensive, systems-centric areas of IoT and deep technology that are linked to the domestic manufacturing base. New policy approaches in three areas – money, markets, and minds – are needed.

3 New technologies such as robotics, artificial intelligence (AI), advanced material science, biotech, and quantum computing tend to have broad general-purpose applications. But uncoordinated funding vehicles, universities' civil clauses, and restrictive visa and onboarding guidelines for skilled foreign workers slow innovation in these sectors and hamper German techno-geopolitical competitiveness.

4 In the mid-term, Germany could look at a scheme to bundle the Future Fund together with new institutional investment in a sort of embryonic German Sovereign Wealth Fund, with a proportion of funding specifically geared toward strategically important VC endeavors.

Introduction

Confidence in Germany's technology ecosystem was, until recently, at an all-time high. By building on a robust research and development (R&D), investment, and startup base, the country's digital sector was on course to displace manufacturing in terms of DAX-market capitalization by 2030.[27] The benefits of this would have extended well beyond stock traders' portfolios. A booming digital sector was to form a central plank of Germany's future techno-geopolitical power: success would build the launch pad for German efforts to establish a European digital sovereignty based on "freedom-to-choose" technologies, enhanced resilience, and avoidance of technology dependencies that geopolitical rivals could exploit. The situation now is looking more tenuous.

Russia's war, rising energy prices, and inflation are taking a toll on the worldwide availability of capital for the technology sector. Private investors are withdrawing from the German digital sector at an alarming rate. The German federal government is also turning toward fiscal consolidation with an eye on a balanced 2023 budget. At a time when Berlin is prioritizing defense modernization and renewable energy transformation, support for the country's innovation industrial base could weaken dangerously if sufficient resources are withheld from the R&D behind digital technologies.

Germany has a highly differentiated economy fueled by cluster-based innovation, political federalism, a family-centric *Mittelstand*, and diffuse national research networks. This decentralized structure for innovation has, of course, historically been a strength. Highly developed niche capabilities proved globally competitive in the industrial era. But that era has largely ended. Today, at a time when network effects are key to international competitiveness in data-intensive platforms, AI, and cloud computing, Germany must better exploit its comparative advantages in the digital sector to address the three interconnected challenges of money, markets, and minds.

This is not just about Germany's position in the world. Innovation is the key to global geostrategic ambitions. Ultimately, the trajectory of the German innovation ecosystem will define Europe's evolving role as a great power in strategic technologies and as a champion for democratic technology governance.

27 Ryan Browne, "Start-up founder predicts a shakeup in Germany's blue-chip DAX index, with tech taking over by 2030," CNBC, November 17, 2021: https://www.cnbc.com/2021/11/17/germanys-dax-index-will-be-taken-over-by-tech-in-2030-says-wefox-ceo.html (accessed April 22, 2022).

The State of Play

Innovation requires an ecosystem comprising money, markets, and minds that is able to transition Germany's R&D strengths into advantages in data-intensive, systems-centric areas of the Internet of Things (IoT) and deep technology that boost the domestic manufacturing sector. COVID-19 brought positive shifts in the structure of German and European innovation, especially in money. Indeed, across Europe, startup funding increased from approximately €40 billion in 2020 to €106 billion in 2021, creating an explosion of 321 European unicorns, venture capital-backed companies with a valuation of at least $1 billion. Germany alone had 55. It also had 26 decacorns, which were valued at more than $10 billion.[28] Venture capital investment in Germany more than tripled between 2020 and 2021, reaching €17.4 billion in 2021.[29] During this time, funding of deep technology, which includes robotics, AI, sensors, advanced material science, biotech, and quantum computing, also doubled in Europe and accounted for 21 percent of total venture capital raised in 2021. The money flow was so profound that it shifted frontier technologies to the areas of quantum and post-quantum cryptography, virtual reality health care, AI-based drug research, cognitive computing, and silicon photonics. Germany found itself particularly well positioned in robotics and sensor technologies due to the work of companies such as Q.ANT and Franka Emika,[30] and the country is now developing capabilities in areas such as next-generation personal aircraft (at Lilium), biopharma (at BioNTech), and defense AI (at Helsing.ai).[31]

Despite being a European technology innovator in certain sectors,[32] Germany still lags behind competitors in other geographic regions. US and Chinese technology players may be market leaders, but those from the UK, Canada, South Korea, and Israel also race to capture, control, and commercialize innovation in areas ranging from social media platforms to deep technology. Even Europe's largest technology company, ASML (market capitalization $352 billion), pales in size to Microsoft ($2.5 trillion) or China's Tencent ($601 billion). Europe, in fact, has only 7 percent of the world's technology market capitalization.[33] And although it annually generates roughly the same number of startups as the United States, Europe has a higher startup stagnation rate (45 percent compared to 37 percent).[34] That difference – partially attributed to easier access outside Europe to markets, late-stage capital, and talent – has led to a "scale-up" trap that has cost the EU approximately one million jobs and €2 trillion in GDP over the last two decades.[35]

Germany also lags in financing. Its largest venture capital funds are small compared to those in the US and China.[36] Its pension fund investment remains low, too.[37] Meanwhile, 61 percent of all European late-stage investment that involves companies on the verge of market success includes at least one US investor, and 95 percent of all European late-stage funding exceeding $250 million involves an American or an Asian investor.[38] US capital accounts for more than 50 percent of total investment in Germany and is particularly present in late-stage

28 Atomico, State of European Tech 2021 (December 9, 2021), p. 28: https://soet-pdf.s3.eu-west-2.amazonaws.com/State_of_European_Tech_2021.pdf (accessed April 22, 2022).

29 Ernst & Young GmbH, "Startup-Barometer Deutschland" [Startup-Barometer Germany], January 2022: https://assets.ey.com/content/dam/ey-sites/ey-com/de_de/news/2022/01/ey-startup-barometer-2022.pdf (accessed April 22, 2022).

30 Henning Kagermann, Karl-Heinz Streibich, and Katrin Suder, "Digital Sovereignty: Status Quo and Perspectives," acatech IMPULSE, (March 25, 2021), p. 13: https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder (accessed April 22, 2022).

31 Germany ranks second, behind the United Kingdom, as a European location for unicorns with primary (25) or secondary (26) hubs. Two of Europe's top five digital hubs are in Germany.

32 In publicly traded technology companies, Germany leads Europe with three (SAP, Infineon, and Delivery Hero). Germany's private sector technology landscape includes established players such as SAP, Deutsche Telekom, Infineon, and Bosch, and digital service entrants such as Delivery Hero, N26, HelloFresh, and Zalando. Of the 10 largest technology deals in Europe in 2021, four involved German companies (Celonis, Gorillas, N26, and Trade Republic), followed by two each in the UK and the Netherlands. Europe's largest venture capital-backed exit was AUTO1Group's initial public offering in February 2021.

33 Oliver Noyan, "Europe tech investment to reach $100 billion in 2021," *EURACTIV*, December 9, 2021: https://www.euractiv.com/section/digital/news/europe-tech-investment-is-reaching-100-billion-annually (accessed April 22, 2022).

34 European Commission, "Europe's next leaders: the Start-up and Scale-up Initiative", COM(2016) 733 final, November 22, 2016: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A733%3AFIN (accessed April 22, 2022).

35 Ibid.

36 World Fund ($406 million), Bayern Kapital ($238 million), Heal Capital ($122 million), Atlantic Food Labs ($117 million), Earlybird ($88 million), and Visionaries Club ($85 million).

37 Just 4 percent of total funds are from pension funds in the DACH region compared to 28 percent in Scandinavia.

38 Atomico, State of European Tech 2021 (December 9, 2021), p. 57: https://soet-pdf.s3.eu-west-2.amazonaws.com/State_of_European_Tech_2021.pdf (accessed April 22, 2022).

3 – KEY CRITICAL EMERGING TECHNOLOGY R&D HUBS

Source: Authors' own illustration

investment.[39] Worryingly, this investment is drying up as European central banks respond to inflation, and geopolitical risk arising from Russia's invasion of Ukraine decreases global institutional investors' willingness to fund the digital sector.

• **BAVARIA'S CONSORTIUM-BASED QUANTUM INITIATIVE** binds the research networks of the Fraunhofer Society, the Max Planck Society, and the Technical University of Munich (TUM) into a Center for Quantum Computing and Quantum Technologies (ZQQ). The Center is at the heart of a Munich-based techno logy park that also includes private sector players such as IBM, whose Q System One is used in Ehningen.[40] While Q System One operates with 27 qubits, IBM aims to finalize its 1000+ qubit-chip as soon as 2023.[41]

• **CYBER VALLEY** is Europe's largest AI research cluster. It brings together the Max Planck Institute for Intelligent Systems, the University of Tübingen, and the University of Stuttgart with private sector actors such as Daimler, Bosch, Amazon, and BMW. Cyber Valley is developing a €180 million campus in Tübingen.

• **THE JÜLICH RESEARCH CENTER'S COLLABORATION** with Canadian company D-Wave led to Europe's first 5000-qubit quantum computer. The ultimate aim is a moonshot integration of the device into Jülich's supercomputing infrastructure, which is set to go online in mid-2024. The Federal Ministry of Education and Research has allocated €76.3 million to Jülich's QSolid collaborative project, in which 25 companies and research institutions – including the Leibniz Institute of Photonic Technology, the Karlsruhe Institute of Technology, Ulm University, the Free University of Berlin, and the University of Cologne – are joining forces to build a complete quantum computer based on cutting-edge technology.

• **THE GERMAN RESEARCH CENTER FOR ARTIFICIAL INTELLIGENCE (DFKI)** is one of the world's oldest and largest AI research bodies. It has facilities in seven cities that work in fields including image recognition, simultaneous translation, robotics, and cognitive assistants.

39 Atomico, State of European Tech 2021 (December 9, 2021), p. 253: https://soet-pdf.s3.eu-west-2.amazonaws.com/State_of_European_Tech_2021.pdf (accessed April 22, 2022).

40 Max Planck Society, "Munich Quantum Valley – a leap forward for quantum science and technology," (January 12, 2021): https://www.mpg.de/16258573/munich-quantum-valley (accessed April 27, 2022).

41 Jay Gambetta, "IBM's roadmap for scaling quantum technology," IBM, (September 15, 2020): https://research.ibm.com/blog/ibm-quantum-roadmap (accessed April 27, 2022).

Germany's embryonic technology champions are consequently compelled to seek non-European funding as they grow from startup to mature market player. They are also compelled to face an uncomfortable paradox: the greater their success, the greater the stake held by American and Chinese venture capital and institutional investors. At the same time, German and European finance pursues only a limited "going out" foreign and direct investment (FDI) strategy to seek opportunities in regions beyond national or EU territory. Lack of capital, fear of risk, regulatory differences, and domestic dependencies all hamper going further afield. European venture capital flowing into the US is much less than that which is flowing the other way. The result is that Europe is largely absent from global technology investment. It is often on the sidelines in the competition for innovation.

An additional disadvantage Germany faces is its limited ability to draw on talent outside Europe, which puts it behind in the global competition for the best minds. Europeans comprise an overwhelming 85.9 percent of German start-up workers, while only 6.6 percent hail from Asia, 2.2 percent from North America, and 5.4 percent from elsewhere.[42] In contrast, two thirds of Silicon Valley workers in engineering and computer science were born outside the United States. Moreover, 52 percent of US unicorns have at least one founder born outside the country. In Germany, one in five founders has a migration background,[43] and a mere 15 percent of German founders are women. Equally striking, only 1.3 percent of European funding went to founders belonging to ethnic minorities.[44]

It is true that Germany's technical research system has matured in recent years, facilitated by liberalized university admissions policies for international STEM (science, technology, engineering, and mathematics) students and a strong economy. Here, Germany has been helped by geopolitical tailwinds: developments that have pushed IT talent out of southern eurozone countries, the Middle East, and, most recently, war-torn Ukraine and authoritarian Russia. But Germany still lacks the flexible labor conditions, salaries, benefits, and research resources to attract and retain top talent. The United States, Canada, and the United Kingdom are still winning that race at a time of a global IT labor shortage.

The information and communications technology (ICT) talent gap is a key hindrance for Germany's global technology position and, ultimately, for European security. The EU has set a target of having 20 million ICT specialists by 2030,[45] but Germany is producing just 70,000 of them annually. Silicon Saxony has a worker gap of almost 30,000 in its semiconductor sector.[46] Saxony-Anhalt, the site of Germany's future semiconductor production base, faces an even more acute struggle of attracting European and global talent from areas like South and East Asia, the Middle East, and Africa. In both German regions, political and social environments that, in some instances, tolerate right-wing extremism, racism, and xenophobia, add to the challenges.[47] Insufficient staffing at Germany's cyber agencies, such as the Federal Office for Information Security (BSI), the Cyber Innovation Hub of the German Armed Forces, and the recently established Cyber Agency in Halle, remains another top strategic constraint, and one that may lead to difficult choices when setting and pursuing priorities.

Some of the most dynamic innovation ecosystems in digital technology have developed in small, open economies facing a persistent security threat from a geopolitical rival. That existential threat can create a sense of national mission that facilitates an interdisciplinary approach to state-supported R&D and overcomes the challenges of a small domestic market. This is the case in Taiwan, Estonia, South Korea, and Israel, all of which have developed globally competitive technology innovation ecosystems, often closely linked to their defense sector. As a middle power that lacks a sense of imminent geostrategic danger, Germany relies on the EU market to bolster its ambition to be a hub for innovation. But the limits of EU regulatory convergence have become more evident,

42 Bundesverband Deutsche Startups e.V., *"Deutscher Startup Monitor 2021"* [German Startup Monitor 2021] (October 2021): https://deutschestartups.org/wp-content/uploads/2021/10/Deutscher-Startup-Monitor_2021.pdf (accessed April 24, 2022).

43 Tom Schmidtgen, "Every fifth start-up has a founder with a migration background on average," *Startbase*, (April 28, 2021): https://www.startbase.com/news/jedes-fuenfte-start-up-hat-gruenderin-oder-gruender-mit-migrationshintergrund/ (accessed April 24, 2022).

44 Atomico, State of European Tech 2021 (December 9, 2021), p. 134: https://soet-pdf.s3.eu-west-2.amazonaws.com/State_of_European_Tech_2021.pdf (accessed April 22, 2022).

45 European Commission, "2030 Digital Compass: the European way for the Digital Decade," COM(2021) 118 final, March 9, 2021: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (accessed April 24, 2022).

46 Joe Miller, "'Silicon Saxony' aims to be EU chipmaking hub," *Financial Times*, December 16, 2021: https://www.ft.com/content/75841b94-196e-466f-ad1b-72d3809c33fc (accessed April 24, 2022).

47 Sonderkommission zu institutionellem Antisemitismus, Rassismus und Fremdenfeindlichkeit, *Bericht der Sonderkommission zu institutionellem Antisemitismus, Rassismus und Fremdenfeindlichkeit in der Landespolizei Sachsen-Anhalt* [Report of the Special Commission on Institutional Anti-Semitism, Racism and Xenophobia in the Saxony-Anhalt Police Force] (March 2021): https://mi.sachsenanhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/MI/MI/2._Aktuelles/20210228_Bericht_Sonderkommission_Druckversion.pdf (accessed April 24, 2022).

and Germany should shift its market-building strategy toward using open standards and open source software as a means to lower barriers for digital technology R&D on the supply side. Greater economies of scale can also help to counterbalance the strengths of Germany's technology competitors in areas such as market size (US, China) or mission-driven cohesion (Israel, Taiwan, South Korea).

The Current Policy Approach

German innovation policy is most intensely focused on basic R&D.[48] The country already allocates 3.13 percent of GDP for spending on it, and the *Ampel* government has set an ambitious goal of increasing that to 3.5 percent. Current German spending accounts for 31 percent of total European R&D expenditure.[49]

Commercializing research remains a challenge for Germany, however. For decades, the Central Innovation Program (ZIM) has aimed to promote R&D within the *Mittelstand*. But ZIM is underfunded and cannot meet demand for its services.[50] It has accepted no new funding applications since October 2021. To help remedy the situation, the government launched the EXIST program in 2017, which fosters entrepreneurship and commercialization of academic research. A signature entity of the governing coalition, the planned Agency for Transfer and Innovation (DATI), represents another effort to commercialize German research. DATI would offer opportunities to test incentives for commercializing university research, support would-be academic entrepreneurs, and connect these individuals to the private sector. Finally, the Ministry of Economic Affairs and Climate Action's Digital Hub Initiative aims to coordinate innovation among Germany's 12 recognized, geographically-dispersed innovation hubs, which each specialize in a specific sector, to give local R&D and commercial technological strengths the capacity for nationwide scalability.[51]

In addition, the Venture Tech Growth Financing Program, a pre-COVID-19 joint initiative of the government and the *Kreditanstalt für Wiederaufbau* (KfW), the country's investment and development bank, provides startups with loans worth €50 million annually. Already in its first 100 days, the *Ampel* government outlined an ambitious approach with its first government-wide Start-Up Strategy, with a 10-point to-do list on everything from capital to data access.[52] Most importantly, the Start-Up Strategy envisions that state and private pension funds will be required to mobilize a portion of their investment into VC. Together with the 2021 *Zukunftsfund*, this is an important stop-gap measure for the collapse in post-COVID venture capital, particularly for high-risk deep tech areas.

Paradoxically, the *Ampel* government has also begun to deprioritize funding for projects that facilitate technology ecosystems through scalability, interoperability, and open source development. In a fit of absentmindedness or, perhaps, by design, the coalition initially cut funding for DATI, digitizing education, the Gaia-X cloud architecture of standards, and the Sovereign Tech Fund to support open source software development for security, resilience, and technological diversity. Sacrificing these efforts to implement Germany's post-COVID-19 fiscal consolidation could prove shortsighted by adversely affecting German downstream technology and cybersecurity innovation. Such limitations on R&D ecosystems in dual-use applications have traditionally weakened defense innovation, one of the greatest global sources of technological discovery, with spillover effects into economic and geopolitical competitiveness.

This trend is not new in Germany. The country's universities and *Hochschulen*, led by the University of Bremen in 1986, have instituted so-called "civil

48 Basic R&D is defined as research aimed at generating a more complete, theoretical understanding of fundamental aspects of technology as opposed to applied research, which tends to be more easily commercialized.

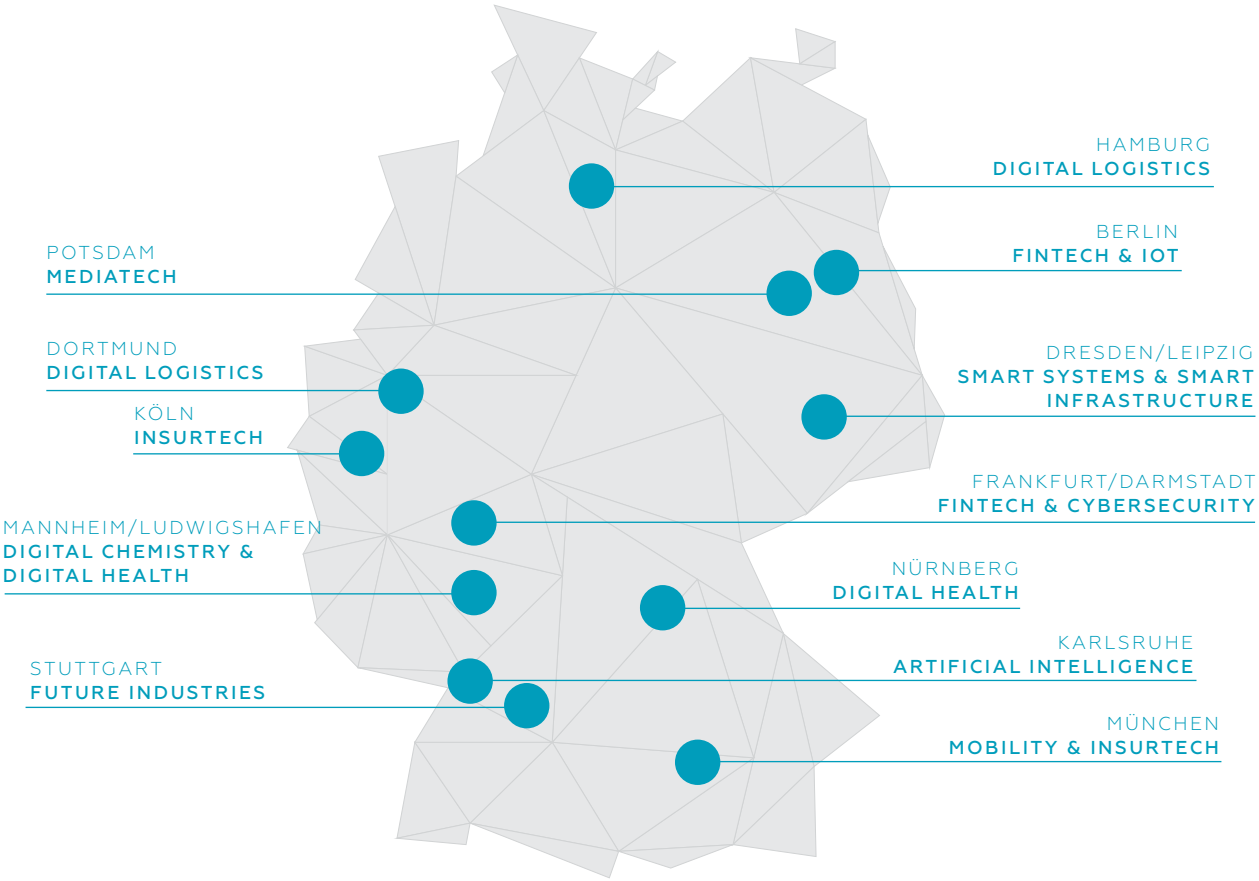
49 Federal Ministry of Education and Research, Research and Innovation (2021): https://www.datenportal.bmbf.de/portal/en/research.html (accessed April 25, 2022).

50 Federal Ministry of Economic Affairs and Climate Action, *"Zentrales Innovationsprogramm Mittelstand"* [Central Innovation Program Mittelstand], (October 7, 2021): https://www.zim.de/ZIM/Redaktion/DE/Meldungen/2021/4/2021-10-06-aussetzung-zur-antragsannahme.html (accessed April 24, 2022).

51 Federal Ministry of Economic Affairs and Climate Action, *"Zwölf hubs, ein digitales netzwerk,"* [Twelve hubs, one digital network], https://www.de.digital/DIGITAL/Redaktion/DE/Dossier/digital-hub-initiative.html (accessed April 26, 2022).

52 Federal Ministry of Economic Affairs and Climate Action, *"Start-up-Strategie der Bundesregierung,"* [Start-up-Strategy of the Federal Government], (June 21, 2022): https://www.bmwk.de/Redaktion/DE/Dossier/Digitalisierung/start-up-strategie.html (accessed July 19, 2022)

4 – GERMANY'S TWELVE DIGITAL HUBS
A STRONG NETWORK OF TECHNOLOGICAL EXPERTISE AND INNOVATION



Source: Bundesministerium für Wirtschaft und Klimaschutz
(https://www.de.digital/DIGITAL/Redaktion/DE/Dossier/digital-hub-initiative.html)

clauses" (*Zivilklausel*) to restrict research to non-military applications.[53] More than 70 German higher education institutions, including Berlin's Technical University and the University of Tübingen, both of which conduct leading AI research, now have civil clauses.[54] The strict separation of civil and military research is inconsistent with breakthroughs in critical and foundational technologies such as AI, quantum encryption, and advanced materials. The dual-use nature of these emerging and foundational technologies makes an artificial wall of separation between civil and military technology increasingly meaningless. Further, it is geopolitically disadvantageous given the increasingly central role that defense technology plays as a driver of general digital innovation ecosystems in countries such as the United States, China, Israel, the United Kingdom, and France.

Not everything on the academic front is bleak, however. Improved public administration funding, hiring processes, and competitive salaries have facilitated university education for foreign students and visas for skilled immigrants. Both developments are important since they provide entryways into the technology sector. Germany has also unwittingly gained from geopolitical developments since the 2010-12 eurozone crisis and the 2015-16 refugee crisis brought in highly-skilled European and global talent.[55]

53 Ursula Schröder, "Akademie kritisiert Zivilklauseln" [Academy criticizes civil clauses], Forschung und Lehre (May 19, 2022): https://www.forschung-und-lehre.de/politik/akademie-kritisiert-zivilklauseln-4820 (accessed July 10,2022).

54 Initiative Hochschulen für den Frieden-Ja zur Zivilklausel, "Bestehende Zivilklauseln" [Existing civil clauses], (2022): http://zivilklausel.de/index.php/bestehende-zivilklauseln (accessed July 10, 2022).

55 Paula Hoffmeyer-Zlotnik and Janne Grote, *Attracting and retaining international students in Germany*, Federal Office for Migration and Refugees (2019): https://www.bamf.de/SharedDocs/Anlagen/EN/EMN/Studien/wp85-internationale-studierende.pdf?__blob=publicationFile&v=18 (accessed April 26, 2022).

Recommendations

Germany must focus efforts in three areas if it is to bolster its global standing for fostering technology: 1) creating stronger funding streams for commercializing basic research, allowing dual-use R&D, and providing more durable financing for technology companies; 2) addressing scalability within the German federal system and throughout Europe via the digital single market; and 3) training, attracting, and retaining highly skilled IT specialists who power a future innovation industrial base. Specific measures include the need to:

Incentivize coordination among innovation-promoting institutions. Deeper cooperation among Germany's innovation agencies is key. The Cyber Agency and disruptive innovation hub SPRIND have already declared an intention to strengthen their collaboration.[56] Another step would be to create a national strategic technology council and a formalized interagency meeting process that includes the Central Office for Information Technology in the Security Sector (*Zentrale Stelle für Informationstechnik im Sicherheitsbereich*, or ZITiS) as well as Future Fund (*Zukunftsfund*), DATI and the Sovereign Tech Fund. The current government's coalition envisions the establishment of the latter two. All these agencies would compare strategic objectives, test potential cooperation, identify broader obstacles, and consider research into dual-use technology and its applications. The greater transparency that would come from this would help avoid duplicative funding while increasing knowledge of, and access to, successful programs. The federal government should also create a dashboard of state (*Länder*) initiatives and promote asymmetric R&D and industrial alliances both among the German states and with the private sector in allied countries.

Emphasize complementarity between the *Zeitenwende* and German innovation in dual-use technologies. The €100 billion *Zeitenwende* outlay must link defense modernization with basic R&D capacity in dual-use innovation, including defense software. As part of the mentality shift in the *Zeitenwende*, *Länder* and universities must work with the federal government and the private sector on common-sense use of the *Zivilklausel*. Research universities must recognize the more general-purpose nature of technology and its funding sources.

Commit to reliable capital investment focused on industrial platforms, IoT, and deep and green digital technology. Despite the headwinds of austerity, inflation, and a global economic downturn, the German government should create domestic public investment incentives for strengthening its innovation industrial base. DATI, the Future Fund and the Sovereign Tech Fund aim to do this, but they are all in danger of being caught in fiscal consolidation and interministerial infighting. The technology sector would, in any case, welcome more government financing schemes. German startups identify public capital as their preferred source of funding (49.7 percent), followed by operative cashflow (43.4 percent), strategic investors (42.5 percent), and venture capital (42.2 percent).[57] The government must provide strategic lifelines to allow for long-term planning and bolder innovation in key digital sectors. The Future Fund, itself, has aims to provide €10 billion in funding for start-ups. In the mid-term, Germany could look at a scheme to bundle the Future Fund together with institutional investment in a sort of embryonic German Sovereign Wealth Fund, with a proportion of funding specifically geared toward strategically important VC endeavors.

Create sandboxes – protected research spaces shielded from the constraints of regulation, red tape, and public procurement requirements – at publicly funded research institutions and agencies. Federal contracting requirements limit Germany's ability to develop a globally competitive innovation ecosystem. Bureaucratic sclerosis, approval delays, and arbitrary timelines can squeeze, if not choke, innovation. Research institutions and innovation agencies would benefit from public sector funding requirements for contracting and tendering, evaluation, and long-term planning that can keep pace with rapid global innovation. Expedited processes would also help determine if government investment is prudent.

56 Marcel Roth, "Cyberagentur und Innovationsagentur Sprind wollen stärker zusammen arbeiten [Agency for Innovation in Cybersecurity and innovation agency Sprind want to cooperate more strongly]," Mitteldeutscher Rundfunk (January 15, 2022): https://www.mdr.de/nachrichten/sachsen-anhalt/podcast/podcast-digital-leben-folge-fuenfzig-cyberagentur-sprind-zukunft-laguna-hummert-zusammenarbeit-100.html (accessed April 26, 2022).

57 Bundesverband Deutsche Startups e.V., *Deutscher Startup Monitor 2021* [German Startup Monitor 2021] (October 2021), p. 36: https://deutscherstartupmonitor.de/ (accessed July 11, 2022).

Encourage private sector engagement with "expeditionary investment" in, and acquisition of, technology champions and start-ups outside Europe. For most US and Chinese technology companies, mergers and acquisitions (M&A) has been central to building market power and absorbing innovation from other sources. Germany's leading firms, supported by the German government, need to adopt an expeditionary or "going out" mentality for FDI to gain access to innovation breakthroughs, diverse organizational and management philosophies, and key intellectual property (IP).

Consider high-end R&D access in geostrategic terms. Offensive measures such as IP provision and adoption incentives and private sector collaboration aside, the new government should examine potential defensive instruments to prevent "IP leakage," particularly in deep technology.

Recast the Digital Single Market as a geopolitical priority. Europe's digital market fragmentation remains a stumbling block to scalability, a key hurdle to the bloc realizing its geopolitical potential in technology. Germany should lead efforts to complete the digital single market, including those aimed at encouraging the free flow of data and sector-specific data spaces across the EU, simplifying start-up registration, and building a unified capital market that encourages cross-border investment. These efforts will be especially critical for creating more pan-European open standards/open source software, thereby broadening the R&D supply base for resilient European-wide innovation.

Consider the ICT talent pipeline to be critical infrastructure. Germany's immigration policies have begun to help its digital innovation ecosystem. The country has drawn human capital thanks to a university system that accommodates international students, liberalized residency and work requirements, and the ease of working in English. Germany now must elevate the attraction and retention of top IT talent to a national strategic objective. To do so, research institutes must offer the computing power, resources, research infrastructure, competitive salaries, and hiring flexibility that their American, British, and Chinese counterparts can.

CHAPTER 3

Technology and Industrial Policy in an Age of Systemic Competition

Safeguarding Germany's Technology Stack and Innovation Industrial Base

CHAPTER OVERVIEW

Key Takeaways

1 As one of the world's most globalized economies, Germany is confronting a challenging international environment characterized by aggressive subsidies, a global race for control of key technologies such as advanced chips, and vulnerable supply chains for critical components. Increased energy costs – induced by Russia's war on Ukraine – are also straining Germany's industrial model.

2 Germany's industrial economy is simultaneously undergoing a fundamental transformation from precision-based engineering to systems-based manufactured products. With this shift, a competitive digital technology stack is becoming a key repository for future industrial competitiveness. Yet, the country struggles to capture value in fast-growing markets like that for cloud and edge infrastructure. It also faces risks from its exposure to untrustworthy technology vendors and potential geopolitical disruptions to fragile hardware supply chains.

3 The German government is consequently drawing the contours of a new technology-industrial policy. This effort, however, suffers from uneven implementation and the complexities of eff ectively coordinating subnational (across the *Länder*) and supranational (across the EU) industrial policy.

4 To effectively preserve its economic competitiveness, the German government should conduct a systematic assessment of the country's strengths and vulnerabilities in critical technology, increase the cohesiveness between federal and state government initiatives, and work internationally – within the EU and with like-minded partners beyond – to leverage comparative advantages.

Introduction

Berlin's stance on industrial policy is evolving significantly. Specifically, its digital policy, long focused on data rules, competition, and open markets, is now confronting a new global environment characterized by aggressive subsidies, a global race for market share in key technologies such as advanced chips, and vulnerable supplies of critical components. China has become a direct competitor as it moves up the value chain following a transition from labor-intensive manufacturing to advanced production in autonomous and electric vehicles, smart machinery, robotics, and network equipment sectors. The United States, for its part, is investing heavily in its innovation industrial base to defend its technological primacy in domains such as cutting-edge chip design and AI.

These challenges have forced Germany to undertake a more active industrial policy. At stake is the country's future economic prosperity, as its technology-industrial base grapples with a shift from precision-based engineering to systems-based manufactured products reliant on data and algorithms, digital infrastructure, and semiconductor supply chains. Unless the country can skillfully use technology-industrial policy to safeguard its strong position in global high-tech value chains, its economic base and geopolitical influence will diminish. To avoid this, the German government must reconcile such a policy with the open-market and choice-based principles underpinning its domestic economy as well as the geopolitical imperatives for fostering strategic interdependencies with close allies and partners.

The State of Play

Germany's industrial transformation is forcing the country to bring together its excellence in the automotive, machinery, medical engineering, and other sectors with technologies, such as AI and emerging digital ecosystems.[58] This has created acute challenges to its industrial competitiveness, in part because the country's mid-sized businesses – its famous *Mittelstand* "hidden champions" – display relatively low levels of new technology adoption. For instance, a mere 6 percent of them have implemented AI strategies aimed at retaining competitiveness.[59] A large majority (77.1 percent) say, too, that they are ambivalent about the benefits of data sharing despite its importance for securing a competitive edge by optimizing industrial processes and developing new products.[60] Moreover, the country's landscape of industrial Internet of Things (IoT) and data-sharing platforms is fragmented. Initiatives for European data spaces such as Gaia-X advance slowly, reflecting internal quarrels over the participation of non-European players and the political challenge of advancing a common European ecosystem based on interoperability and trust.[61]

Germany, however, has advantages in its existing innovation industrial base. The country embraces networking and automation as the world's fourth-largest spender on IoT,[62] which comprises internet-connected devices such as sensors and meters, and it accounts for a third of Europe's operational industrial robots.[63] Domestic AI development also meets half of German industrial demand.[64] According to estimates, AI-based solutions could provide a major economic boost by increasing German GDP by 11.3 percent, or €430 billion, through 2030.[65] But policies to accelerate the translation of Germany's R&D strengths into data-intensive and systems-centric applications in its domestic industrial base are key to securing the country's position as a top-tier technology power.[66]

With this shift to data-driven value creation, a competitive digital technology stack is becoming a key repository for future industrial competitiveness. A fundamental concern in this regard, however, is the availability of secure and reliable cloud and edge computing infrastructure.[67] This is not just because Germany's continued leadership in core industries, such as autonomous driving, manufacturing, and energy grid management,

58 AI, a key driving force behind this transformation, is anticipated to contribute to a rise in global GDP of about 16 percent by 2030, making it the most significant driver for the global economy. Jacques Bughin et al., "Notes from the AI frontier: Modeling the impact of AI on the world economy," McKinsey & Company Discussion Paper (September 2018): https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy (accessed May 19, 2022).

59 J.P. Singh, "Deutschland kann Krise – aber auch KI?" [Germany Can Handle a Crisis – But Can AI?], *Tagesspiegel Background*, September 6, 2021: https://background.tagesspiegel.de/digitalisierung/deutschland-kann-krise-aber-auch-ki (accessed May 19, 2022). More broadly, a mere 15 percent of German industrial companies are estimated to have implemented AI solutions, compared with 25 percent of US companies, and 23 percent of Chinese companies. acatech, "Künstliche Intelligenz in der Industrie" [Artificial Intelligence in Industry], acatech Horizonte (July 2020), p. 54: https://www.acatech.de/publikation/acatech-horizonte-ki-in-der-industrie/download-pdf/?lang=de (accessed May 19, 2022).

60 According to a 2018 survey of 111 small- and medium-sized enterprises. Companies worry most about third-party access to their data (90.7 percent). Institut der deutschen Wirtschaft, "Datenwirtschaft in Deutschland. Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?" [The Data Economy in Germany. Where do companies stand on data use and what are their biggest obstacles?], (February 2021), p. 40: https://www.iwkoeln.de/fileadmin/user_upload/Studien/Gutachten/PDF/2021/Hemmnisse_der_Datenwirtschaft_Studie.pdf (accessed May 19, 2022)

61 Silke Hahn, "Gaia-X in der Unternehmerdiskussion: Tolle Vision, wann kommt die Realität?" [Entrepreneurs Discuss Gaia-X: Great vision, when will reality come?], *Heise Online*, February 2, 2022: https://www.heise.de/news/Gaia-X-in-der-Unternehmerdiskussion-Tolle-Vision-wann-kommt-die-Realitaet-6340570.html (accessed May 19, 2022).

62 Germany accounts for approximately 5 percent of global IoT spending and is currently surpassed only by the United States, China, and Japan. United Nations Conference on Trade and Development, *Digital Economy Report 2019. Value Creation and Capture: Implications for Developing Countries*, (July 2019), p. 7: https://unctad.org/system/files/official-document/der2019_en.pdf (accessed May 19, 2022).

63 Germany had approximately 230,000 operational industrial robots in 2021. International Federation of Robots, "Jeder dritte Industrie-Roboter in der EU wird in Deutschland installiert" [Every Third Industrial Robot in Europe is Installed in Germany], (October 28, 2021): https://ifr.org/downloads/press2018/Germany-2021-OCT-IFR_press_release_industrial_robots.pdf (accessed May 19, 2022).

64 Results of surveys of 235 German companies from 2021 show that approximately 46 percent of external AI applications bought or rented by German companies are from German developers. Only the United States accounts for another significant share of AI solutions providers (38 percent). Achim Berg, "Künstliche Intelligenz. Wo steht die deutsche Wirtschaft?" [Artificial Intelligence. Where does the German economy stand?], (April 2021), p. 10: https://www.bitkom-research.de/system/files/document/Bitkom%20Charts%20K%C3%BCnstliche%20Intelligenz%2021%2004%202021_final.pdf (accessed May 19, 2022).

65 The automotive and healthcare industries, using 2018 German GDP as a baseline, are expected to be those most impacted. PwC, "Künstliche Intelligenz sorgt für Wachstumsschub. Wie groß ist das Potenzial und wie kann Ihr Unternehmen davon profitieren?" [Artificial Intelligence Provides a Growth Spurt. How big is the potential and how can your company profit from it?], (February 2019): https://www.pwc.de/de/digitale-transformation/business-analytics/kuenstliche-intelligenz-sorgt-fuer-wachstumsschub.html (accessed May 19, 2022).

66 Tyson Barker and David Hagebölling, "The Geopolitics of Digital Technology Innovation Assessing Strengths and Challenges of Germany's Innovation Ecosystem", DGAP Report, (August 31, 2022): https://dgap.org/en/research/publications/geopolitics-digital-technology-innovation (accessed October 31, 2022).

67 More than four out of five companies in Germany use cloud computing. Bitkom Research, "Trendstudie Digitalisierung 2019" [Digitalization Trend Study 2019], (November 2019): https://www.bitkom-research.de/de/Trendstudie-Digitalisierung-19 (accessed May 19, 2022).

increasingly depends on cloud-based big data processing.[68] It is also because *decentralized* cloud infrastructure, in particular, will underpin Germany's rapidly growing industrial IoT and the requirements for highly secure and low-latency computing carried out close to the data source, the so-called "edge."[69] Germany is forecasted to remain Europe's largest and fastest growing market for edge computing through 2025,[70] when the majority of business data will be processed outside traditional, centralized data centers.[71]

And yet, Germany, like all of Europe, struggles to capture value in the fast-growing market for cloud and edge technology. German cloud providers such as T-Systems[72] and SAP[73] are turning to operational partnerships with US hyperscalers to reconcile advanced cloud technology with data protection requirements, especially with regard to limiting the legal grounds and technical possibilities for foreign access to data stored on European servers.[74] Meanwhile, the shift to edge computing is also altering the sources of comparative advantage. Unlike more general-purpose cloud infrastructure, edge computing is characterized by wide geographic distribution of data centers and tends to be adapted to specific verticals and applications.[75] This could impact competition between large cloud providers and incumbent telecommunication companies.

Germany's conflicted strategy for secure telecommunications networks, which increasingly fuse with the cloud-based data-processing infrastructure, presents another challenge.[76] Chinese vendors currently play a significant role in German telecommunications networks, with Huawei alone providing almost half of their 4G base stations.[77] Germany is attempting to limit exposure to Chinese firms in 5G networks but is not ready to shift to European providers.[78] German telecommunications operators, after all, have a strong commercial interest in diversifying their equipment providers and limit reliance on European companies Nokia and Ericsson, the second- and third-largest 5G base station vendors.[79] Accordingly, Berlin has supported the O-RAN Alliance,[80] a major industry and research initiative aimed at defining interoperable standards for mobile networks.[81] The support comes despite questions about the security of O-RAN's architecture[82] and discord with key partners, including France and

68 The European cloud market, of which Germany represents around one fifth, is projected to increase tenfold to roughly €500 billion by 2030. Martin Möhle, "Cloud Computing in Germany 2021," *Future Processing*, January 11, 2021: https://www.future-processing.com/blog/cloud-computing-in-germany-2021 (accessed May 19, 2022).

69 Edge computing refers to data processing at the "edge" of networks, closer to the location where data is collected. One key benefit of this is that time-consuming data transfers over long distances are avoided, enabling greater speed and low latency.

70 Reply, "From Cloud to Edge" (December 2020), p. 5: https://www.reply.com/en/Shared%20Documents/from-cloud-to-edge-EN.pdf (accessed May 19, 2022).

71 Some estimates suggest that 75 percent of data processing could move to the edge by 2025. Rob van der Meulen, "What Edge Computing Means for Infrastructure and Operations Leaders," Gartner (October 3, 2018): https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders (accessed May 19, 2022).

72 T-Systems, "Investition in Technologie und gemeinsame Innovation, um Kundenbedürfnisse in Deutschland zu erfüllen" [Investment in Technology and Joint Innovation to Meet Customer Needs in Germany], (September 8, 2021): https://www.t-systems.com/de/de/newsroom/news/t-systems-und-google-cloud-bauen-souveraene-cloud-fuer-deutschland-450414 (accessed May 19, 2022).

73 SAP, "Startschuss zur ersten souveränen Cloud-Plattform für den öffentlichen Sektor in Deutschland: SAP und Arvato Systems kündigen Partnerschaft an" [Start to the First Sovereign Cloud Platform for the Public Sector in Germany: SAP and Arvato Systems announce partnership], (February 3, 2022): https://news.sap.com/germany/2022/02/cloud-plattform-public sector-arvato (accessed May 19, 2022).

74 Notably, these partnerships aim to offer cloud services to German companies and the public sector that limit legal grounds and technical possibilities for accessing data under laws such as the US's CLOUD Act and FISA Act, and the Chinese Cybersecurity Law.

75 Brandon Moser, "Edge Computing Examples Across Vertical Industries," (September 9, 2021): https://www.digi.com/blog/post/edge-computing-examples-across-vertical-industries (accessed October 5, 2022).

76 5G has been rolled out for public mobile networks since 2019, but many applications remain available only in campus networks that connect people and systems in private spaces such as production facilities, hospitals, universities, and ports. Federal Ministry for Economic Affairs and Energy (BMWi), "Leitfaden 5G-Campusnetze – Orientierungshilfe für kleine und mittelständische Unternehmen" [5G Campus Networks Guidelines – Guidance for Small and Medium-sized Enterprises], (April 2020): https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/leitfaden-5G-campusnetze-orientierungshilfe-fuer-kleine-und-mittelstaendische-unternehmen.pdf?__blob=publicationFile&v=8 (accessed May 19, 2022).

77 Germany is not an outlier in this regard. About half of all European countries have a similar amount of Chinese vendor equipment. Deutsche Welle, "Germany pressures Huawei to meet security requirements," June 21, 2019: https://www.dw.com/en/germany-pressures-huawei-to-meet-security-requirements/a-49294841 (accessed May 19, 2022).

78 This is happening through stricter requirements to ensure the "trustworthiness" of equipment vendors under Germany's IT-Security Law 2.0 (2021), among other measures.

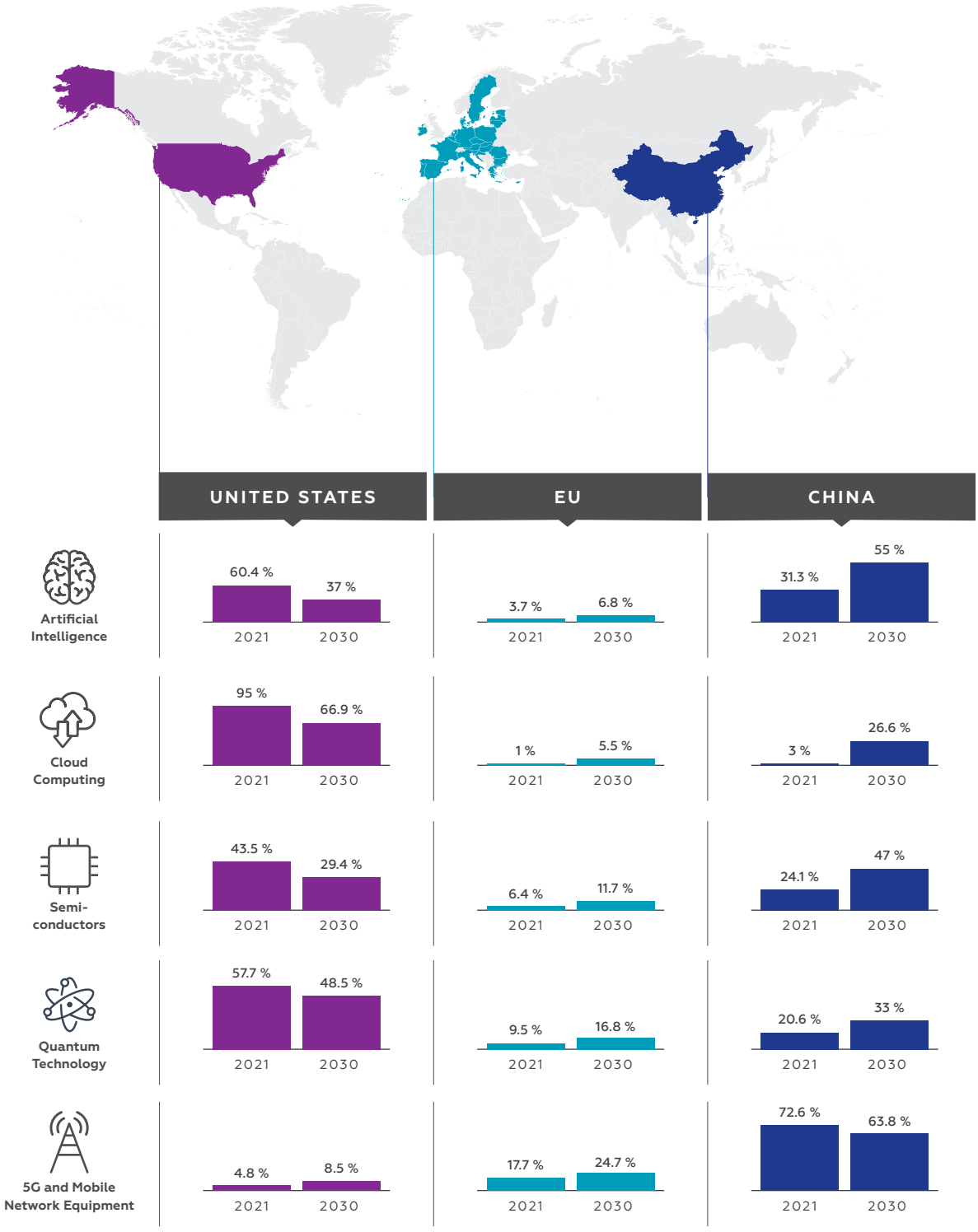
79 Zoefie Cheng, "Market Share of Top Three Suppliers of Base Stations Projected to Undergo Slight Decline in 2021 While Fourth-Ranked Samsung Scores Wins in Overseas Markets, Says TrendForce," TrendForce, (July 28, 2021): https://www.trendforce.com/presscenter/news/20210728-10872.html (accessed May 19, 2022).

80 Federal Ministry for Digital and Transport (BMDV), "BMVI startet Open RAN-Förderung" [BMVI launches Open RAN Funding], (November 9, 2021): https://www.bmvi.de/SharedDocs/DE/Pressemitteilungen/2021/126-bmvi-startet-open-ran-foerderung.html (accessed May 19, 2022).

81 Founded in 2018, the O-RAN Alliance is an initiative by network operators, vendors, and research institutions aimed at devising industry standards for "open, virtualized and fully interoperable mobile networks."

82 Germany's Federal Office for Information Security (BSI) raises concerns in a 2021 risk analysis study about Open RAN security. The study notes that Open RAN's specifications are not developed in accordance with the paradigm of "security/privacy by design/default" and that it is a system that displays "numerous security risks." Stefan Köpsell et al., "Open-RAN Risikoanalyse 5GRANR" [Open-RAN Risk Analysis 5GRANR], Federal Office for Information Security (February 2022), p. 73: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/5G/5GRAN-Risikoanalyse.pdf;jsessionid=9E7EE4E27FFCF263EC0710664967F076.internet472?__blob=publicationFile&v=9 (accessed May 19, 2022).

5 – EXPERT ASSESSMENT OF EUROPE'S LEADERSHIP IN KEY TECHNOLOGIES, 2021 VS 2030



Source: Authors' illustration based on data from Kaan Sahin and Tyson Barker, "Europe's Capacity to Act in the Global Tech Race," German Council on Foreign Relations (April 2021): https://dgap.org/sites/default/files/article_pdfs/210422_report-2021-6-en-tech.pdf (accessed September 14, 2022).

the European Commission, over O-RAN's ramifications for Europe's 5G champions.

Germany also faces risks in the fragile supply chain for semiconductors, the foundational technology that powers industrial IoT, smart grids, electric and autonomous vehicles, and other industrial components and products. Europe's share of global semiconductor manufacturing capacity has fallen from 44 percent in 1990 to just 8 percent today.[83] In 2020, Infineon was the only German company (and one of only four European companies) among the 20 largest semiconductor manufacturers in terms of revenue.[84] More than three quarters of chip production now occurs in Asia, primarily in Taiwan, South Korea, and China.[85] Disruptions in this geopolitically precarious region would have a profound economic impact on Germany, one likely much greater than that of severed Russian gas supplies.

Germany and its EU partners need a strategic and measured approach to industrial policy in this highly complex and diversified market. Given high capital barriers to entry,[86] re-shoring (cutting-edge) manufacturing requires substantial and sustained subsidies.[87] This means diversifying global sourcing options should be a priority, as is identifying comparative advantages in the semiconductor value chain. Crucially, Germany still boasts legacy strengths in certain supplier markets and production segments. Precision-engineered components and specialized chemical products from German companies such as Zeiss and BASF are critical ingredients for semiconductor production.[88] And Infineon, Bosch, STMicroelectronics, and NXP excel in specialized chips,[89] including those for industrial applications, automotive, and defense.[90]

Yet, Germany must not lose sight of future disruptions. An increasing number of (industrial) companies design their own specialized chips while intellectual property holders and Electronic Design Automation (EDA) tool vendors are almost exclusively located in the United States.[91] Developments in quantum and high-performance computing give Germany an opportunity to secure a stronger position in the hardware segment in the future.[92] But German companies, despite strengths in basic research, lack competitive hardware products,[93] a sector that changes increasingly rapidly.[94]

83 Antonio Varas et al., "Government Incentives and US Competitiveness in Semiconductor Manufacturing," Boston Consulting Group (September 2020), p. 7: https://www.semiconductors.org/wp-content/uploads/2020/09/Government-Incentives-and-US-Competitiveness-in-Semiconductor-Manufacturing-Sep-2020.pdf (accessed May 19, 2022).

84 GlobalData, "Top 20 semiconductor companies by revenue recorded healthy growth, days Global Data," (July 8, 2021): https://www.globaldata.com/top-20-semiconductor-companies-revenue-recorded-healthy-growth-says-globaldata (accessed June 21, 2022).

85 Alex Irwin-Hunt, "In charts: Asia's manufacturing dominance," *Financial Times*, March 24, 2021: https://www.ft.com/content/2b0c172b-2de9-4011-bf40-f4242f4673cc (accessed May 19, 2022).

86 Taiwan's TSMC accounts for roughly 90 percent of cutting-edge chip manufacturing. Yang Jie et al., "The World Relies on One Chip Maker in Taiwan, Leaving Everyone Vulnerable," The *Wall Street Journal*, June 19, 2021: https://www.wsj.com/articles/the-world-relies-on-one-chip-maker-in-taiwan-leaving-everyone-vulnerable-11624075400 (accessed May 19, 2022).

87 For example, TSMC's Arizona fabrication plant, currently under construction, is estimated to cost $12 billion. Sebastian Moss, "TSMC starts work on $12bn Arizona semiconductor fab, gets funding for Japanese chip R&D," DCD, June 2, 2021: https://www.datacenterdynamics.com/en/news/tsmc-starts-work-on-12bn-arizona-semiconductor-fab-gets-funding-for-japanese-chip-rd (accessed May 19, 2022).

88 Zeiss, "Semiconductor Manufacturing Optics": https://www.zeiss.com/semiconductor-manufacturing-technology/products/semiconductor-manufacturing-optics.html (accessed September 30, 2022); BASF, "Chemical Solutions for Semiconductors": https://electronics-electric.basf.com/global/en/electronics/semiconductors_solutions.html (accessed September 30, 2022).

89 Automotive, industrial, and communications electronic system markets are among the most rapidly expanding, exceeding even the growth of the consumer segment. ICInsights, "Outlook Remains Bright for Automotive Electronic Systems Growth," November 19, 2018: https://www.icinsights.com/news/bulletins/Outlook-Remains-Bright-For-Automotive-Electronic-Systems-Growth (accessed May 19, 2022).

90 Jan-Peter Kleinhans and Nurzat Baisakova, "The global semiconductor value chain. A technology primer for policy makers," Stiftung Neue Verantwortung (October 2020).

91 Jan-Peter Kleinhans, "The lack of semiconductor manufacturing in Europe. Why the 2nm fab is a bad investment," Stiftung Neue Verantwortung (April 2021), p. 20: https://www.stiftung-nv.de/sites/default/files/eu-semiconductor-manufacturing.april_.2021.pdf (accessed May 19, 2022).

92 Quantum computing (QC) remains in an early stage, but its potential is significant. Building on quantum physics, QC uses "qubits," which, as opposed to classical "bits," can take on different values at one time. This unlocks computing possibilities that greatly exceed those of classical digital computing. Quantum computers are exponentially more performant in certain computational tasks that are key to German industrial competitiveness, including drug development, real-time processing of industrial and car sensor data, and supply chain management. The technology has great economic potential and will transform cryptography, rendering breakable even advanced classical encryption methods.

93 The Fraunhofer research consortium, for example, depends on US cloud-based quantum computing resources and physical access to IBM's Q System One in Ehningen. Fraunhofer Gesellschaft, "Fraunhofer Competence Network Quantum Computing: Understanding and using qubits!": https://www.fraunhofer.de/de/institute/kooperationen/fraunhofer-kompetenznetzwerk-quantencomputing.html (accessed May 19, 2022).

94 While IBM's Q System One operates with 27 qubits, the company aims to finalize its 1000+ qubit-chip as soon as 2023. Jay Gambetta, "IBM's roadmap for scaling quantum technology," IBM (September 15, 2020): https://research.ibm.com/blog/ibm-quantum-roadmap (accessed May 19, 2022).

The Current Policy Approach

The German government is aware of all these shifts and is drawing the contours of a new industrial policy. In a range of high-level documents, most notably its "High-Tech Strategy 2025" (released in 2018)[95] and "Industrial Strategy 2030" (released in 2019),[96] Berlin adopted a more strategic outlook on critical technologies that dovetails with the bigger €750 billion NextGenerationEU plan.[97] German policy remains anchored in its long-standing ordoliberal principles of open markets and freedom of choice, but it now acknowledges a greater role for state intervention to preserve industrial value creation. Pandemic-related economic disruption solidified this outlook, leading Germany to frame its €130 billion recovery stimulus package as a "package for the future" that prioritizes digital investment for economic recovery.[98]

Germany has promised significant public investment in critical technology. The country's first-ever AI strategy, released in 2018, featured a €3 billion investment, later increased to €5 billion,[99] through 2025 to support talent development, computing facilities, and internationally competitive AI ecosystems.[100] The federal government also committed in 2019 €650 million to strengthen Germany's quantum physics research.[101] That funding was increased in 2021 to €2 billion, with the explicit goal of obtaining a competitive "Made in Germany" quantum computer by 2025.[102]

And yet, this transition to a more state-led technology-industrial policy still faces challenges. Germany may outspend other EU member states in this domain, but it struggles with uneven implementation. While the country has, for example, achieved its goal of hiring 100 AI professors,[103] it has, as of mid-2021, only disbursed €250 million of its €5 billion AI investment package.[104] Besides bureaucratic holdups, this reflects the government's lack of a coherent process for following through on strategic priorities.

In addition, Germany's federated structure complicates synergies between federal and state (*Länder*) policy. German federalism can create healthy competition among *Länder* that highlights different strengths and that experiments with policies to attract international investment and talent for cutting-edge technology. But to realize the desired "leveraging effect" between federal and *Länder* initiatives, such competition must be embedded in a coordinated approach that assesses potential synergies.[105] A potentially significant advantage exists in the interlocking of federal funding priorities and *Länder* investment policies that have launched regional initiatives. These efforts include Bavaria's

95 Federal Ministry for Education and Research (BMBF), "Forschung und Innovation für die Menschen. Die Hightech-Strategie 2025" [Research and Innovation for People. The High-Tech Strategy 2025], (September 2018): https://www.bmbf.de/SharedDocs/Publikationen/de/bmbf/1/31431_Forschung_und_Innovation_fuer_die_Menschen.pdf?__blob=publicationFile&v=6 (accessed May 19, 2022).

96 Federal Ministry for Economic Affairs and Energy (BMWi), "Industriestrategie 2030. Leitlinien für eine deutsche und europäische Industriepolitik" [Industrial Strategy 2030. Guidelines for a German and European Industrial Policy], (November 2019): https://www.bmwk.de/Redaktion/DE/Publikationen/Industrie/industriestrategie-2030.pdf?__blob=publicationFile (accessed May 19, 2022).

97 European Commission, "State of the Union: Commission proposes a Path to the Digital Decade to deliver the EU's digital transformation by 2030," (September 15, 2021): https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4630 (accessed May 19, 2022).

98 The Federal Government, "Milliardenhilfe beschlossen" [Billions in Aid decided] (June 2020): https://www.bundesregierung.de/breg-de/themen/coronavirus/konjunkturpaket-geschnuert-1757558 (accessed May 19, 2022).

99 Federal Ministry for Economic Affairs and Climate Action (BMWK), "Kabinett beschließt Fortschreibung der KI Strategie der Bundesregierung" [Cabinet Approves Updated German Government AI Strategy], (December 2, 2020): https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2020/12/20201202-kabinett-beschliesst-fortschreibung-ki-strategie-bundesregierung.html (accessed May 19, 2022).

100 The Federal Government, "Die entscheidende Zukunftstechnologie des 21. Jahrhunderts" [The Most Critical Future Technologies of the 21st Century] (December 2, 2020): https://www.bundesregierung.de/breg-de/suche/fortschreibung-ki-strategie-1824340 (accessed May 24, 2022).

101 Stefan Krempl, "Zitis: Staatliche Hacker sollen Verschlüsselung mit Quantencomputer knacken" [Zitis: State Hackers to Crack Encryption with Quantum Computer], Heise Online, September 26, 2018: https://www.heise.de/newsticker/meldung/Zitis-Staatliche-Hacker-sollen-Verschluesselung-mit-Quantencomputer-knacken-4175352.html (accessed May 19, 2022).

102 Sebastian Grüner, "Deutschland fördert Quantencomputer mit 2 Milliarden Euro" [Germany Funds Quantum Computers with 2 Billion Euros], Golem.de, May 11, 2021: https://www.golem.de/news/grundlagenforschung-deutschland-foerdert-quantencomputer-mit-2-milliarden-euro-2105-156422.html (accessed May 19, 2022).

103 Werner Pluta, "Forschungsministerium besetzt 100 zusätzliche KI-Professuren" [Research Ministry Fills 100 Additional AI Professorships], Golem.de, May 6, 2022: https://www.golem.de/news/kuenstliche-intelligenz-forschungsministerium-besetzt-100-zusaetzliche-ki-professuren-2205-165144.html (accessed May 19, 2022).

104 As of May 31, 2021. German Bundestag, "Schriftliche Fragen mit den in der Woche vom 07. Juni 2021 eingegangenen Antworten der Bundesregierung" [Written Questions with Federal Government Answers for the week of June 7, 2021] (Circular 19/30613, June 11, 2021), p. 159: https://dserver.bundestag.de/btd/19/306/1930613.pdf (accessed May 19, 2022).

105 A "leveraging effect" ("*Hebelwirkung*") is posited, for example, in the government's AI strategy. However, only the 2020 strategy update makes substantial reference to areas – other than education, which is primarily a state responsibility – that could involve collaboration with the states.

6 – GERMANY'S PARTICIPATION IN DIGITAL TECHNOLOGY IPCEIS

FIELD	TIMELINE	MEMBER STATES	GERMAN FUNDING	TECHNOLOGY FOCUS	PROJECTS
Microelectronics I	**2018:** EU Commission approval **2020:** start of projects **2022:** end of projects (planned)	**4 EU member states:** France, Germany, Italy, and Austria (joined 2021) + United Kingdom	Total: ≈ €3.6 billion Government: €1 billion Private: €2.6 billion	Energy efficient chips; Power semiconductors; Sensors; Advanced optical equipment; Compound materials	EU: 43 Germany: 18
Microelectronics II	**2021:** pre-notification **2022/23:** pending EU Commission approval **2023+:** start of projects (planned)	**20 EU member states:** Austria, Belgium, Czech Republic, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, and Spain	Total: €10 billion Government: €450 million (for 2023) Private: n/a	Photonics, next generation sensors, processors, AI/ML/DL; Next generation power, actuators, energy efficiency; Softwarised networks, 5G/6G enabling technology, optical connectivity, short range wireless	EU: n/a Germany: 32
Cloud Infrastructure and Services	**2022:** pending EU Commission approval (pre-notified) **2022:** start of projects (planned) **2026:** end of projects (planned)	**12 EU member states:** Belgium, Czech Republic, France, Germany, Hungary, Italy, Latvia, Luxembourg, Netherlands, Poland, Slovenia, and Spain	Total: n/a Public: €750 million Private: n/a	Establishing a cloud-edge infrastructure, especially for industrial applications through: Digital infrastructure; Interconnections; Foundation services; Platforms and smart processing services	EU: ≈80 Germany: 22

Source: Authors' compilation based on publicly available information

€300 million financing for its Munich Quantum Valley[106] to promote quantum sciences and technologies, and an initial €160 million package for Baden-Wuerttemberg's Cyber Valley, currently Europe's largest AI research consortium.[107]

Coordination at the supranational level likewise remains an important challenge to effective implementation. EU institutions have clout in defining the digital rulebook, but the member states drive industrial policy. Germany has a played a key role in overcoming this division of labor and advancing more coherent policymaking. This includes, notably, a commitment to several Important Projects of Common European Interest (IPCEIs),[108] including those for microelectronics, cloud infrastructure, and batteries. But the IPCEI for cloud infrastructure and services (IPCEI-CIS),[109] with €750 million of German funding, is entangled in disputes about the French-German GAIA-X initiative,[110] which allows American and Chinese hyperscalers to participate in establishing standards for Europe's federated data

106 Bavarian State Ministry of Science and the Arts, "Munich Quantum Valley: Münchener Initiative will Quantencomputer in Bayern entwickeln" [Munich Quantum Valley: Munich initiative wants to develop quantum computers in Bavaria], (January 11, 2021): https://www.stmwk.bayern.de/pressemitteilung/12124/munich-quantum-valley-muenchener-initiative-will-quantencomputer-in-bayern-entwickeln.html (accessed May 19, 2022).

107 Ministry of Science, Research and the Arts Baden Württemberg, "Fünf Jahre Cyber Valley" [Five Years of Cyber Valley], (December 15, 2021): https://mwk.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/fuenf-jahre-cyber-valley (accessed May 19, 2022).

108 An IPCEI may receive member state subsidies if it is an integrated European project that addresses a market failure in a key sector or technology, and if it has positive spillover effects for the EU economy as a whole.

109 Federal Ministry for Economic Affairs and Energy (BMWi), "Förderbekanntmachung zur geplanten Förderung im Bereich Cloud und Edge Infrastruktur und Services im Rahmen des IPCEI-CIS" [Funding Announcement for Planned Funding in Cloud and Edge Infrastructure and Services within the IPCEI-CIS Framework], (April 2022): https://www.bmwk.de/Redaktion/DE/Downloads/F/forderbekanntmachung-zur-geplanten-forderung-im-bereich-cloud-und-edge-infrastruktur-und-services-im-rahmen-des-ipcei-cis.pdf?__blob=publicationFile&v=6 (accessed May 19, 2022).

110 Gaia-X European Association for Data and Cloud AISBL, "About Gaia-X": https://www.gaia-x.eu/what-is-gaia-x (accessed May 19, 2022).

infrastructure. Moreover, the IPCEIs for microelectronics[111] face slow German and European Commission bureaucracy, and questions remain about these projects' alignment with the €17 billion Intel fab project in Magdeburg, to which German public subsidies are slated to contribute approximately €6.8 billion.[112]

On top of these policy inconsistencies, Germany's other fiscal and geopolitical priorities compete for federal funding. The current German government faces intense pressure to promote fiscal consolidation starting in 2023 even as the recent *Zeitenwende* envisions a €100 billion special fund (*Sondervermögen*) for modernizing Germany's armed forces in the face of rising geopolitical conflict.[113] Russia's invasion of Ukraine has also put inflationary pressures on energy and food, which is simultaneously accelerating and frustrating Germany's climate transformation goals. There is a growing sense that technology-industrial policy could become less of a priority.

Recommendations

Germany must use its industrial policy tools effectively to develop and secure access to critical technologies and preserve its economic competitiveness. To that end, it should:

Undertake a comprehensive mapping of goals and capacities in critical technology. Mirroring partners' efforts, the German government should kick-start an interagency effort to map out three industrial policy ambitions: technological leadership, peer status with competitors, and necessity to mitigate dependency risks.[114] These assessments should match strategic economic and security priorities with domestic and partner capabilities.

Increase strategic industrial policy cohesiveness between federal and state governments as well as among the *Länder*. Germany should prioritize ensuring that states' industrial policies align with national technology objectives. The Federal Ministry for Education and Research (BMBF) should establish a dashboard of state-level industrial initiatives that highlights unmet potential for asymmetric R&D and industrial alliances. Senior state officials, research consortia, and industry could use this tool to identify and realize synergies among initiatives in individual research fields and across industries, for example between hardware- (e.g., quantum computing) and software-related (e.g., natural language processing) R&D efforts.

Expand transnational industrial consortia in Europe and among like-minded states. The EU has a technological choice: hang together or hang separately. As the EU's largest economy, Germany has significant agency to advance a strategic and coherent European technology-industrial policy. It should foster cross-border innovation industry consortia by advocating a streamlined IPCEI notification process, ensuring adequate staffing for caseloads, and dedicating funds that match its high-tech ambitions. Where like-minded states provide key value chain components, Germany should encourage the European Commission to create an IPCEI scheme involving foreign suppliers to amplify positive spillover effects.

Focus on domestic – and European – competitive advantages and strategic interdependencies within a larger community of like-minded partners. Global supply chains are often too complex to reshore complete technology stacks. Germany should design its industrial policy to promote a larger community of like-minded partners that has the EU at its core but includes key partners such as the United States, Japan, and South Korea. This community should have

111 As a co-initiator of the IPCEI for Microelectronics, the German government is mobilizing nearly €1 billion through 2023 to support the building of modern chip factories and production of energy-efficient microelectronic components. It is also a major participant in a new IPCEI Microelectronics II that targets high-performance and specialized chips, e.g., for AI and autonomous driving applications. Federal Ministry for Economic Affairs and Energy (BMWi), "IPCEI Mikroelektronik: Zwei europäische Großprojekte für eine Schlüsseltechnologie der Zukunft" [IPCEI Microelectronics: Two Major European Projects for a Key Technology of the Future] (September 2021): https://www.bmwi.de/Redaktion/DE/Downloads/I/infopapier-ipcei-mikroelektronik.pdf?__blob=publicationFile&v=6 (accessed May 19, 2022).

112 Joachim Hofer, „Die Chip-Industrie entdeckt Deutschland – das neue Intel-Werk ist nur der Anfang" [The Chip Industry Discovers Germany – The New Intel Plant is Just the Beginning], Handelsblatt, October 7, 2022: https://www.handelsblatt.com/technik/it-internet/halbleiter-die-chip-industrie-entdeckt-deutschland-das-neue-intel-werk-ist-nur-der-anfang/28711740.html (accessed October 31, 2022).

113 Christian Mölling and Torben Schütz, "Zeitenwende in der Verteidigungspolitik. Bundeswehr-Sondervermögen effektiv und nachhaltig ausgeben" [Turning Point in Defense Policy. Spending the Bundeswehr Special Fund Effectively and Sustainably], DGAP Policy Brief No. 16, German Council on Foreign Relations (May 2022): https://dgap.org/sites/default/files/article_pdfs/dgap-policy%20brief-2022-16-dt_1.pdf (accessed May 19, 2022).

114 For the US example, see The White House, *National Strategy for Critical and Emerging Technologies* (October 2020): https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf (accessed May, 19 2022).

three goals: IT security, supply chain resilience, and industrial competitiveness. Within these areas, industrial policy aimed at boosting competitiveness should link directly to German comparative advantages such as edge computing and industrial domain expertise (e.g., in the automotive, medical, and energy grid sectors) for specialized chips.

Structure public procurement to mitigate IT-security and supply chain vulnerabilities. Germany's largest purchaser of IT systems is its federal government, which can leverage its purchasing power to reduce strategic vulnerabilities, particularly in security-critical layers of its technology stack. Procurement requirements should support the scaling of a secure European cloud infrastructure for public services. Reforms should eliminate disadvantages for open source solutions by making security, openness, and interoperability key criteria. Reforms should also facilitate the entry of (smaller) European competitors through a simplified tendering process and more transparent approval timelines.

CHAPTER 4

Germany's Role in Europe's Digital Regulatory Power

Shaping The Global Technology Rule Book in the Service of Europe

CHAPTER OVERVIEW

Key Takeaways

1 Four elements help to map the strengths and, at times, the limits of German power in digital rule-making. First, Germany anticipates EU digital regulation and attempts to establish facts on the ground. Second, Germany has outsized influence in the formal stages of EU digital regulatory policymaking. Third, the EU, in turn, provides Germany with a launch pad for influencing worldwide regulatory norms. Fourth, a belated reawakening of the capacity of the German private sector and affiliated technical standard bodies to influence global technical standards is occurring.

2 Germany, as an EU member state, is engaging in three significant areas of data governance and cybersecurity: digital identities and open data, lawful access to electronic messaging systems, and rules for sovereign cloud usage.

3 Germany's largely successful role as a key incubator for the EU's regulatory approach to digital technology and, therefore, as a proponent of the "Brussels Effect" of influencing global markets is not widely appreciated or understood at home. The lag among regulations, technology, and international context is evident in areas such as data protection, content moderation, and market power of online platforms. Even meaningful regulatory debates on quantum, the metaverse (AR/VR), and 6G have yet to arise in Germany.

4 Germany must change its approach to digital regulation to more accurately reflect the dynamic, general-purpose nature of emerging digital technologies against an increasingly fraught international landscape in which technological rules are a dimension of geopolitical power. This includes more fully addressing political trade-offs associated with digital regulation choices, expanding reviews and sunset clauses in digital regulation to encourage flexibility, and making greater use of multi-stakeholder regulatory approaches that incorporate civil society, companies, and other non-state actors. Germany must also increase the engagement of its foreign policy and national security communities in EU technology diplomacy and in global regulation enforcement.

Introduction

Germany is an important – perhaps the most important – force for setting the EU's digital regulatory approach, which forms a basis for European power in the geopolitics of technology. Germany has been at the heart of the EU's ambitious effort to root digital regulation in human rights, rule of law, and democracy. This regulation of platforms, algorithms, and data governance is set out in the EU's Digital Services Act (DSA), the Digital Markets Act (DMA), the Data Governance Act (DGA), the Artificial Intelligence Act (AI Act), the Data Act and the Cloud Rulebook.[115] Germany's central role in shaping these rules means that the EU will succeed in updating its rule book only if Germany likewise updates its own thinking. That includes acknowledging just how geopolitical regulation has become, and how other powers balance regulation and innovation and, at times, profit with the costs of the EU being a regulatory first mover. As the bloc tackles the next wave in data governance on cloud, edge computing and the Internet of Things (IoT), Germany and, therefore, the EU have the chance to shape a regulatory framework that fosters European values and global competitiveness.

The State of Play

Germany is a confident, assiduous, and skilled actor in shaping digital regulation at the national and, particularly, the EU level. It understands the levers of regulatory power on digital technology in Brussels, and through various channels – federal and state governments, the private sector, and German civil society – Germany has the tools to shape the European rule book in a way that is consistent with an ordoliberal, rule-centric approach to digital sovereignty. But to the extent that the rule book becomes the basis for global digital regulation, German awareness breaks down. Four elements help to map the strengths and, at times, the limits of German power in digital rule-making.

115 Tyson Barker, "2021 Is the Year the Internet Gets Rewritten," Foreign Policy, January 19, 2021: https://foreignpolicy.com/2021/01/19/2021-is-the-year-the-internet-gets-rewritten (accessed June 1, 2022).

First, Germany routinely attempts to anticipate EU digital regulation trajectories and to frame digital regulation debates in Brussels around its own concerns, more so than probably any other member state. The EU, in turn, tends to monitor the German debate to pave the way for smooth legal passage of its own priorities. Consequently, German legal traditions (e.g., in the evolution of privacy as the basis for the General Data Protection Regulation (GDPR))[116] and normative ordoliberal thinking (e.g., skepticism of cartels and digital market concentration) enjoy strong influence at the EU level. At the same time, Germany finds itself in something of an echo chamber, believing that its priorities – and not cross-border liberalization of digital services with non-EU like-minded states or regulatory scrutiny of the cyber risks of ICT infrastructure manufactured by China's state-controlled enterprises, for example – are shared European priorities.

Of course, the EU rule book does not always reflect German priorities in the end, and other actors – the Commission, the European Parliament, the private sector including US technology companies, and other member states such as France and tech-savvy Nordic-Baltic states and Ireland – have typically influenced the transition from EU debate to legislation. Tension between the DMA and the 10th amendment to the German Competition Act is one example of this. So, too, is the friction between the DSA's illegal-content regulation and that of Germany's Network Enforcement Act (NetzDG). Still, German anticipation of EU legal debates is marked in almost every way by Berlin's own domestic digital technology policymaking, from the screening of digital foreign direct investment (FDI) to due diligence of technology supply chains.[117] The country's Data Ethics Commission, for example, sketched in 2017 a framework for AI risk categories and assessment that was reflected in the EU's 2020 AI White Paper and its 2021 draft AI Act.[118] Germany's IT Security Law 2.0 and Gaia-X, respectively, primed EU discourse on the Network and Information Security 2 (NIS 2) Directive and the European Cybersecurity Certification Scheme for Cloud Services (EUCS).

Second, Germany, the EU's largest member state, is, in fact, overrepresented in the bloc's digital regulatory policymaking. Germans occupy positions as key European Commission civil servants; well-positioned European Council staff; and members of the European Parliament (MEPs) serving as rapporteurs on key digital legislative packages[119] and influential committee chairs;[120] and key parliamentary secretariat staff. And, although many of these officials represent a broad ideological spectrum, they retain a German political sensibility. Only France rivals Germany in its use of key personnel to shape EU digital policymaking, particularly at the Commission (e.g., DG CONNECT) and in key regulatory agencies such as the Body of European Regulators for Electronic Communications (BEREC).

At times, these officials and representatives reflect the unadulterated interests of German institutions, including important German corporate players.[121] This bias is not problematic in itself but rather a natural byproduct rooted in the connective tissue that binds Germany's European policymakers in Brussels and the political discourse of the German business community. Companies can be good motors for German digital power, but they can also, if left unchecked, redirect German national leverage toward narrow corporate aims. And, more problematic still, they can perpetuate shared corporate blind spots. That includes their heightened sensitivity to potential Chinese retaliation against regulatory scrutiny of data processing and cybersecurity practices of Chinese companies operating in the EU. Businesses in Germany's non-EU allies – Australia, Canada and the United Kingdom – are less worried about this because they are less dependent on Chinese markets. Market codependence with China has forced Germany to strike a balance between its need for Chinese consumers and its commitment to its own values in digital technology.

International and geopolitical concerns do, of course, frame German – and European – digital regulation, but these still bear the scars of past experiences dealing with the United States and suspicions regarding data protection and espionage. Following the 2013 Snowden revelations, Germany's data privacy concern has been primarily aimed at the United States. Recent EU initiatives, particularly the DSA,

116 Informational self-determination.

117 Federal Ministry of Labour and Social Affairs, "CSR-Supply Chain Act," (July 22, 2021): https://www.csr-in-deutschland.de/EN/Business-Human-Rights/Supply-Chain-Act/supply-chain-act.html (accessed June 1, 2022).

118 Tyson Barker, "The Digital Technology Environment and Europe's Capacity to Act," DGAP Report No. 7, German Council on Foreign Relations (November 2021), p. 23: https://dgap.org/sites/default/files/article_pdfs/Mercator%20Study%20Tech_Highres.pdf (accessed June 1, 2022).

119 The GDPR, DMA, and the NIS Directive, for example.

120 The Committee on Internal Market and Consumer Protection and the Committee on International Trade, for example.

121 These include Deutsche Telekom, SAP, Infineon, Bosch, Axel Springer, and Bertelsmann.

the DMA, and European cloud proposals, also mainly affect American technology firms given their market dominance. But the extent to which this is perceived as a means of curtailing US tech influence can raise questions, and the overweening focus on the US simply does not reflect today's geopolitical threats (Box 1). The co-regulatory design – and broad implementing authority for the Commission – in the DSA and DMA provide both with flexibility to evolve in ways that reflect new risks in ever-changing information ecosystems online and the dynamism of platform market power. As the two laws enter into force, an early test for EU platform regulation will be to what extent the DSA and DMA are fit for purpose to respond to the platform landscape of 2023, not 2015.

Third, the EU provides Germany, like other member states, with a launch pad for influencing worldwide regulatory norms. Global technology companies have famously made the EU's GDPR the basis for data protection, including in jurisdictions outside the EU. Four years after the GDPR entered into force, countries such as Argentina, South Korea, Japan, and Kenya, and subnational powers such as California, with its California Privacy Rights Act (CPRA), use the GDPR as the basis for their own data protection regulation. Even the growing pressure on Washington to establish a federal US data protection law is driven, in part, by Europe. And the 2020 Schrems II decision, which struck down the 2016 Privacy Shield Framework for transatlantic transfers of personal data, forced the United States to make substantial changes to managing European grievances and to expanding checks on intelligence services' data collection. The EU, as a regulatory first mover, has bent the global regulatory environment toward itself. This is a success for German concerns, but there are drawbacks. Many non-EU states, and most EU member states for that matter, struggle to meet GDPR standards, and this disrupts free data flows. Furthermore, other potentially more fruitful channels are open for the EU to build an international rule book.

On this front, the EU and like-minded states such as Australia, Canada, and the United Kingdom have begun (intergovernmental) regulatory discourse in fields reaching beyond data protection. These fields include content moderation, platform governance, the market power of individual firms, data protection, and risk-based approaches to AI. But this is a laborious effort as differences in internal legislative processes, regulatory competencies, federal structures, and constitutional limits lead to different outcomes.

At the same time, China has learned to parrot EU regulatory principles in pursuit of a far less high-minded set of goals. Its discourse on technology giants' market power and data protection mirrors the debate in Germany and Europe, but its goal is to mollify international criticism while consolidating the Communist Party's absolutist power. China's 2021 Blocking Statute, which invalidates extraterritorial sanctions within the country, was modeled on EU law.[122] Chinese regulation on personal data protection (including the 2020 Global Initiative on Data Security),[123] competition, algorithms, and, most recently, on "positive energy" content governance[124] borrow from European deliberations and, at times, even take the letter of European law. Still, these efforts are designed to conscript the Chinese technology sector and other actors into the service of party-state interests.

Fourth, Europe's rule-setting power would be much smaller without Germany and its private sector's influence in global technical standard-setting bodies. The German Institute for Standardization (DIN), the German Commission for Electrical, Electronic & Information Technologies (DKE), and the Association for Electrical, Electronic & Information Technologies (VDE) comprise a core of national bodies that feed into their European and international counterparts. Germany is one of six permanent members of the International Organization for Standardization (ISO) Council and holds 18% of ISO secretariats, 19% of International Electrotechnical Commission (IEC) secretariats, and 29% of IEC working group chairs.[125] It also fields candidates for key positions, such as its 2022 bid for the director of the International Telecommunications Union's (ITU) Telecommunication Standardization Bureau.[126]

122 Kelly Austin et al., "China's 'Blocking Statute' – New Chinese Rules to Counter the Application of Extraterritorial Foreign Laws," Gibson Dunn, January 13, 2021: https://www.gibsondunn.com/chinas-blocking-statute-new-chinese-rules-to-counter-the-application-of-extraterritorial-foreign-laws (accessed June 1, 2022).

123 Embassy of the People's Republic of China in the United States of America, "Global Initiative on Data Security," September 8, 2020: https://www.mfa.gov.cn/ce/ceus//eng/zgyw/t1812951.htm (accessed June 1, 2022).

124 Maria Siow, "Positive energy: the darker side of China's social media catchphrase," South China Morning Post, June 21, 2020: https://www.scmp.com/week-asia/people/article/3089846/positive-energy-darker-side-chinas-social-media-catchphrase (accessed June 1, 2022).

125 International Organization for Standardization, "DIN," August 4, 2022: https://www.iso.org/member/1511.html (accessed August 10, 2022).

126 International Telecommunication Union, "Elections," (2022): https://www.itu.int/pp22/en/elections/candidates (accessed June 1, 2022).

GERMANY'S HEAVY US FOCUS

The transatlantic technological relationship remains the world's primary artery of digital activity. Undersea information and communications technology (ICT) cables crossing the North Atlantic carry 55 percent more data flows than transpacific routes. But global digital activity, like all economic activity, is shifting away from the United States and toward the Indo-Pacific and Global South, even as Germany's regulatory enforcement posture remains intently Atlantic-centric.

Germany's January 2021 Data Strategy focused heavily on Gaia-X as a means of emancipating Europe from US cloud services (and the provisions of the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which provides conditions for US authorities to access certain data in other countries), in part through the use of open source software such as OpenStack. The current German discussion about data localization, platform dependence, and encryption continues to be overshadowed by the National Security Agency revelations in 2013, former US President Donald Trump's election in 2016, and the Cambridge Analytica scandal in 2017.

The EU's regulatory enforcement effort is likewise primarily focused on the Euro-Atlantic. GDPR enforcement among Germany's 17 Data Protection Authorities (DPAs) remains directed at US service providers and platforms. This has been justified given the dominant role of US digital services in the European market over the past decade. But the preponderance of DPA scrutiny of US technology firms contrasts with the lack of scrutiny of systemic violations by firms from adequacy states such as the United Kingdom, Canada, and Japan, and even by European firms themselves. Perhaps most interesting has been the proportionate lack of scrutiny of systemic violations, particularly in legal access requirements, by authoritarian states such as China and Russia.

There are, however, some indications that the spotlight is slowly shifting away from the United States. The EU's draft AI regulation, informed by Germany's 2020 EU presidency and the Federal Government's Data Ethics Commission, pays greater attention to Chinese practices than similar EU regulation has in the past. The Commission draft's most stringent provisions address social scoring, which it bans, and remote real-time biometric identification, which only law enforcement agencies in narrowly defined situations may use. These measures are implicitly based on China's actions. The promotion of good moral behavior has long been characteristic of Chinese society, but AI-powered biometric identification combined with extensive video surveillance and a social scoring system forms a powerful and dangerous tool for social control.

But in the same way that Germany is sometimes blind to the abundant influence of its private sector in shaping European regulation, it has been slow to recognize the relative decline in influence of Team Germany – and, consequently, Team Europe – in international standard-setting. The role of Germany's private sector has been shrinking as especially Chinese state-owned and state-adjacent enterprises have gained control of key technical working groups and fielded model standards.[127] China's push for regional standard-setting arrangements through its Belt and Road Initiative could also create lock-in effects for third-party countries that tilt toward a mercantilist digital international system that favors China and techno-authoritarianism. This is part of a broader design that Henry Kissinger has called China's "patient accumulation of relative advantage."[128] Germany, like the rest of Europe, has only belatedly realized that technical standard-setting is freighted with geopolitical danger, and this realization has come at a time when German private sector participation in international standard-setting bodies has atrophied.

127 Tim Rühlig, "Technical standardisation, China and the future international order. A European perspective," E-Paper, Heinrich Böll Stiftung Brussels (February 2020): https://eu.boell.org/sites/default/files/2020-03/HBS-Techn%20Stand-A4%20web-030320.pdf (accessed June 1, 2022).

128 Tom McTague, "Joe Biden Has a Europe Problem," The Atlantic, January 21, 2021: https://www.theatlantic.com/international/archive/2021/01/joe-biden-europe/617753 (accessed June 1, 2022)

The Current Policy Approach

The present German government's digital regulation debate is focused on a number of data governance and cybersecurity questions related to seamless digital interaction with public administration, lawful access to electronic messaging systems, and rules for sovereign cloud usage. This marks a change in focus from recent waves of EU regulation, in the sense that it recontextualizes data protection much more in terms of cybersecurity and away from state, and state-adjacent private, actors. This could provide opportunities for a recalibration of Germany's European role to clearly define democratic principles of data governance in ways that are flexible and consistent with Germany's understanding of digital sovereignty. So, what, precisely, is Germany doing?

A DIGITALLY ENABLED STATE

First, on the demand side, German efforts are focused on establishing cross-sectoral and secure electronic digital identities (eIDs) that draw on the experience of the Nordic and Baltic EU member states, and Ukraine, which have adopted eIDs.[129] Germany's eID Act came into force in September 2021 and laid the legal foundation for digital identification via smartphones with secure authentication technology supported by the Federal Printing Office (*Bundesdruckerei*). The government promised limited digital ID services by the end of 2021, but they remain offline. Problems with digital driver's licenses, an ID wallet, and a Smart eID persist.[130] On the supply side, Germany's 2017 law on improving online access to public administration services (OZG) obliged federal, state, and local governments to offer administrative services digitally by the end of 2022, a deadline that governments at all levels are likely to miss.[131] The OZG aims to connect government portals so that businesses and citizens can use a single user account to access online services.[132] There is a risk here that bureaucratic foot-dragging in its implementation, lack of coordination among government agencies and, ultimately, non-uniform and uneven data availability could also lead to suboptimal use by researchers and the private sector.

LAWFUL ACCESS TO ONLINE COMMUNICATION

Another measure worth noting is the attempt by the German federal government to define conditions under which law enforcement agencies may compel messaging services to provide access to encrypted communications, a lingering point of tension between the law and end-to-end encryption. This has also been a topic of conversation for the EU since the disclosure of the FBI's "Lawful Access" document of January 2021 that revealed which data law enforcement authorities may obtain from various messenger services.[133] Services such as Apple, Signal, and Telegram continue to demur.[134]

Last year, the European Commission itself announced a draft law on "chat control," which then quickly disappeared from the agenda, possibly due to the massive protests of more than 30 civil society

129 The Federal Ministry of Economic Affairs and Climate Action estimates that developed economies with a well-functioning digital identity infrastructure can increase their gross domestic product by 3 to 4 percent. Federal Ministry for Economic Affairs and Climate Action, "Im Fokus: Sichere digitale Identitäten" [In Focus: Secure digital identities], (October 2021): https://www.bmwk.de/Redaktion/DE/Schlaglichter-der-Wirtschaftspolitik/2021/11/05-im-fokus-digitale-identitäten.html (accessed June 1, 2022).

130 Viola Heeger, "Digitale Identitäten: Deutschland im Verzug" [Digital identities: Germany behind schedule], Tagesspiegel Background Digitalisierung & KI, December 20, 2021: https://background.tagesspiegel.de/digitalisierung/digitale-identitaeten-deutschland-im-verzug (accessed June 1, 2022).

131 Federal Ministry of the Interior and Community, "Onlinezugangsgesetz (OZG)" [Online Access Act (OZG)], (2022): https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-node.html (accessed June 1, 2022).

132 At the European level, the eIDAS regulation (Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market, which repealed Directive 1999/93/EC) contains binding Europe-wide regulations in the areas of "electronic identification" and "electronic trust services." The regulation created a uniform framework for the cross-border use of national electronic identification measures and, therefore, for the use of the German online ID card and trust services.

133 Martin Holland, "FBI über Messenger: An welche Daten von WhatsApp & Co. US-Strafverfolger kommen" [FBI via Messenger: What data from WhatsApp & Co. US law enforcement officers obtain], Heise Online, December 2, 2021: https://www.heise.de/news/FBI-ueber-Messenger-An-welche-Daten-von-WhatsApp-Co-US-Strafverfolger-kommen-6282456.html?wt_mc=rss.red.ho.ho.atom.beitrag.beitrag (accessed June 1, 2022).

134 Apple's iMessage service offers end-to-end encryption and provides user data only under subpoenas, and chat info is available only if backed up in iCloud. Telegram can provide possible IP addresses and phone numbers. Signal releases only dates and times of the most recent message. With WhatsApp, the world's most popular messenger service, however, investigators can access user data, blocked accounts, contacts, and message destinations.

organizations.[135] But the Commission tabled in May 2022 a proposal to "[lay] down rules to prevent and combat child sexual abuse."[136] The intent is to hold providers of interpersonal communication, in particular, accountable "to detect, report and remove online child sexual abuse on their services."[137] This may subsequently compel messaging and hosting services such as WhatsApp and Signal to soften their encryption procedures or to introduce other controversial solutions, such as hash matching or scans of end-users' devices ("client-side scanning," or CSS).[138] Critics claim the proposal will undermine democratic principles by placing all European citizens under suspicion and undermining internet confidentiality and security.

SOVEREIGN CLOUD AND INDUSTRIAL DATA

Policy efforts in Germany and the EU have been circling each other in an effort to create a cloud infrastructure based on European rules and complemented by a federated European data infrastructure that may limit the market dominance of hyperscalers, with their vast capacity for processing data, through interoperability and portability requirements. The ultimate goal is a competitive cloud landscape under European rules that forms a foundation for infrastructure for the industrial internet and IoT.

Whether this German-led cloud approach will end up giving heft to the country's own ordoliberal, rules-centric notion of digital sovereignty remains unclear. Gaia-X, which is an industry-driven spin-off of a Franco-German government initiative, is one option for an interoperable cloud standards architecture for Europe and, perhaps, beyond. But Gaia-X's tack toward rules-centric digital sovereignty, in part by including US and Chinese players in its governance, has not lived up to the expectations of some European actors, including those in France. It has led some European actors to form rival initiatives, such as the European Cloud Industrial Alliance (EUCLIDIA) and EUCS. These are based on the French cloud certification regime, SecNumCloud, which is meant to isolate public administration from non-European cloud service providers. Moreover, despite announcements of related services such as a federated cloud infrastructure architecture (Structura-X) and sector-specific collaborations in mobility (Catena-X), agriculture (AgriGaia), and finance (EuroDat), Gaia-X seems beset by the deficiencies of similar, previous efforts: low adoption, uncertain private demand, and waning German political support.

Meanwhile, the German debate on data localization is growing. International data flows remain controversial, reflecting Germany's deep ambivalence about the value and benefits of data access. Some in the German government, and politicians, legal experts and NGOs in Germany, are joined by more vociferous voices in France who question whether US cloud providers should store sensitive data at all. Their concerns lie in post-Schrems uncertainty on the protection and privacy of transatlantic data flows and the US CLOUD Act's authorization for US law enforcement to access data stored on servers of US cloud service providers in Europe.[139]

Germany is consequently considering rules for cloud usage in its public administration and sensitive sectors, as the EU looks to create a cloud certification process that considers questions about data localization. Germany joined France, Italy, and Spain – against the Netherlands, Sweden, and Ireland – to back "sovereignty requirements" in EUCS and Gaia-X's Labelling Framework, which would essentially back data localization requirements. The strongest certification, EUCS's "High" and Gaia-X's "Level 3," would limit choice and potentially cut the EU off from hyperscalers – since Amazon, Microsoft and Google are based in the United States – and from European companies with an American footprint, including Deutsche Telekom, SAP, and Bertelsmann. While these certification schemes are currently voluntary, the expectation is that they will, in some form, be required for the provision of public services in the EU in future, with serious implications for data usage across digital

135 Thomas Rudl and Markus Reuter, "Warum die Chatkontrolle so gefährlich ist" [Why chat control is so dangerous], Netzpolitik, November 4, 2021: https://netzpolitik.org/2021/eu-kommission-warum-die-chatkontrolle-so-gefaehrlich-ist (accessed June 1, 2022).

136 European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM(2022)209 final, (May 2022): https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF (accessed June 1, 2022).

137 Ibid., p. 2.

138 Stefan Krempl, "Chatkontrolle: Informatiker und IT-Verbände gegen EU-weite Massenüberwachung" [Chat control: Computer scientists and IT associations against EU-wide mass surveillance], Heise Online, March 29, 2022: https://www.heise.de/news/Chatkontrolle-Informatiker-und-IT-Verbaende-gegen-EU-weite-Massenueberwachung-6656545.html (accessed June 1, 2022).

139 Some have even cited the Chinese firewall's level of control as a positive model for a European internet. Nick Sohnemann et al., New Developments in Digital Services, European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies (May 2020): https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648784/IPOL_STU(2020)648784_EN.pdf (accessed March 11, 2021).

supply chains. Digital smart-city, health, and education services are among those that will be affected.

GERMANY'S GEOPOLITICAL BLIND SPOTS IN RULE-MAKING

As German policymaking moves forward on digital identities, cybersecurity, law enforcement and cloud governance, three blind spots are evident. These blind spots can impact Germany and the EU's ability to balance governance with innovation and maximize their shaping power.

First, Germany's largely successful role as a key incubator for the EU's regulatory approach to digital technology and, therefore, as a proponent of the "Brussels Effect" of influencing global markets, is not widely appreciated or understood in Germany itself. To the contrary, German debate on technology tends to be inward-looking and gives little thought to how Germany influences the EU and the world. Policy deliberations often leave it to technocrats to reactively elevate national preferences to the European level. The discourse also tends to exclude the potential global implications of German rules, and it fails to assuage German fears about digitalization and data flows, which continue to find expression in EU law.

Second, there are lingering geopolitical issues surrounding the implementation and enforcement of existing rules, particularly of the GDPR, the DSA, and the DMA, which reflect a mismatch between the rules set and the context in which they were set. The preponderant Euro-Atlantic nature of German and EU enforcement aligns with the international digital state of affairs between 2012 and 2015. Since then, Chinese and Russian state-adjacent players have become significant players in cloud services, platform services, closed messaging systems, and smart infrastructure technology. IoT has also assumed more global importance. Regulatory enforcement has not kept up, creating German and European vulnerability in digital governance.

Third, shaping emerging technology rules can be slow to arise in Germany in a meaningful way, even if the country is adept at anticipating the EU debate. The Federal Agency for Information Security (BSI) issued first-of-its-kind model standards for cyber security protection of low earth orbit satellites that are meant to inform European model standards with the European Space Agency.[140] And publicly funded R&D in quantum encryption will help drive standards on post-quantum cryptography, including with partners such as the US National Institute of Standards and Technology (NIST).[141] Nevertheless, the lag between technological development and governance generally remains pronounced in Germany, Europe, and like-minded states. This is hardly supportive of the strategic regulatory environment that Germany and Europe want. Given that Germany's and the EU's market size is in decline relative to the rest of the world, so, too, is their regulatory power. In the midterm, the growing role of demand in India and the Global South will recast their roles in setting global regulations, norms, and market power.

Recommendations

Three factors determine Germany's potential for global rule-making reach: the coherence of its vision, enforcement consistency in Germany and the EU, and the ability to make rules that preserve and strengthen European innovation, including for emerging critical technologies, without abetting protectionism. To embed its regulation and standards in a more hard-nosed geostrategic approach, Germany should:

Address the political trade-offs associated with digital regulation choices. The most difficult aspects of digital regulation often pit key German priorities, such as privacy and security, against each other. This forces policymakers to rank objectives. Debate on issues such as privacy, law enforcement, and national security should consider context, permit transparent oversight, and build on the principle that illegal activity offline is also illegal online.

140 Catherine Stupp, "Germany Offers Model for Space-Industry Cybersecurity Standards," The Wall Street Journal, August 17, 2022: https://www.wsj.com/articles/germany-offers-model-for-space-industry-cybersecurity-standards-11660728604 (accessed September 12, 2022).

141 Barbara-Henrika Alfing, "Bochum researchers win worldwide post-quantum cryptography competition," Ruhr Universität Bochum, July 6, 2022: https://news.rub.de/english/press-releases/2022-07-06-future-proof-data-encryption-bochum-researchers-win-worldwide-post-quantum-cryptography-competition (accessed September 12, 2022).

Draft model clauses and modules that can be integrated into partner countries' regulation. This could involve creating an open source regulation repository that expedites the process for non-European partners when it comes to achieving adequacy with the EU on personal and industrial data flows, IoT security, and content moderation, and to addressing aforementioned challenges with the GDPR. Model regulatory clauses and modules should be crafted to prohibit their misuse by authoritarians to justify mass surveillance, censorship, and data theft. Germany should also support the ability of other European states to regulate in their own sovereign ways, and the EU could help partner countries assess the impact of their own regulation.

Conduct geopolitical impact assessments of draft German and European digital regulation. As we have argued, German and EU measures could inadvertently strengthen digital authoritarianism or enable unintended and unwanted global trends such as data localization, censorship, weakened cybersecurity, or internet fragmentation. Authoritarian states such as China and Russia have already shown that they are ready to exploit such unintended consequences, picking and mixing rules to justify mass surveillance, censorship, and digital control over their citizens. Candid assessments of the impact of German and EU technology policy outside Europe could combat such misuse.

Fight creeping state-centrism of European technical standard-setting. The international power of European bodies such as the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI) stems largely from their openness to private sector actors, including non-European firms. It is not simply that technical standard-setting should be left solely to the private sector. But Germany has an acute interest in balancing private sector leadership with state and European interest. It must lead the effort to preserve the pluralistic nature of European standard-setting. Tipping the balance too much toward the state risks greater inefficiencies and, consequently, diminished German and European power in this area. It could also set an unhelpful precedent for authoritarian regimes.

Bolster private sector technical standard-setting capacity. Germany should introduce tax incentives and public funding mechanisms for domestic companies, startups, and associations to participate in standard-setting bodies, seek chairmanships, field draft standards, and work with like-minded states. Financial support could include grants from the Federal Ministry of Economic Affairs and Climate Action (BMWK) and the Federal Ministry for Digital and Transport (BMDV).

Embed high European Cloud Certification and Gaia-X Architecture of Standards into global cloud governance efforts. As industrial data could become a new frontline in global technology regulation, Germany should look at ways to internationalize its data space model, Gaia-X, to include non-European powers, especially the United States. The EU-US Trade and Technology Council (TTC) could develop democratic data spaces for industrial data based on Gaia-X architecture in national hubs in like-minded non-European powers. And Germany's G7 presidency, in its final phase, could launch work on the free flow of data via trustworthy European regulation of, and architecture for, data storage, processing, and transfer. Japan could continue this work during its 2023 G7 presidency. Finally, Germany could support building the capacities of Global Gateway partner countries to use European cloud computing architectures to increase interoperability and preserve human rights. This aim aligns with the government's promise to strengthen digital sovereignty in the Global South.

Integrate digital regulation and technological standard-setting into the Zeitenwende and the National Security Strategy. Germany must consider more intently the effects of digital regulation on its national security posture and defense industry. The country must ensure it can adopt and deploy dual-use technology on par with peer nations such as France, Canada, Japan, and the United Kingdom. This will require more flexibility in addressing national security interests. Provisions of the AI Act, for example, may prohibit the adoption of deep learning that other states' militaries may exploit. And the unbundled digital services that German competition law and the DMA mandate will have unintended consequences for companies' ability to reinforce their cybersecurity. Germany must better balance its technology regulation with national, EU, and NATO security interests. Germany did this successfully when creating criteria for trustworthy telecommunications equipment in its 2021 IT Security Law 2.0.

Increase the engagement of Germany's foreign policy and national security communities in shaping and enforcing regulatory agreements. The German intelligence, foreign policy, law enforcement, and

defense agencies have roles in enforcing technology regulations drawn up in Germany. Just as the United States should promote greater involvement of privacy rights groups in framework discussions, the German government should realize that it is time for those authorities to assume more prominence, and the post-Privacy Shield Transatlantic Data Privacy Framework (TDPF) era will offer a first chance. The German foreign and national security communities have a direct stake in maintaining an open EU-US data bridge that provides private actors with judicial access to US courts, enforceable rights, and limitations on indiscriminate personal data collection. They must take a leadership role in ensuring that the TDPF is a durable solution given the opportunity it presents to create clear regulations for free Euro-Atlantic data flows.

Establish a multistakeholder approach that incorporates civil society, companies, and other non-state actors. Germany and Europe have begun pioneering new models of managing technology regulation. Industrial regulation was highly regimented, appropriate for the engineering-oriented, stable technologies of the factory floor. Digital regulation, however, must be agile, ecosystem-based, and incentive-oriented. Following the DSA/DMA model, it must involve a thicket of relationships, responsibilities, and oversight that can more quickly raise alarms as blind spots in regulation arise. These flexible structures allow for constant oversight that is subject to compromise.

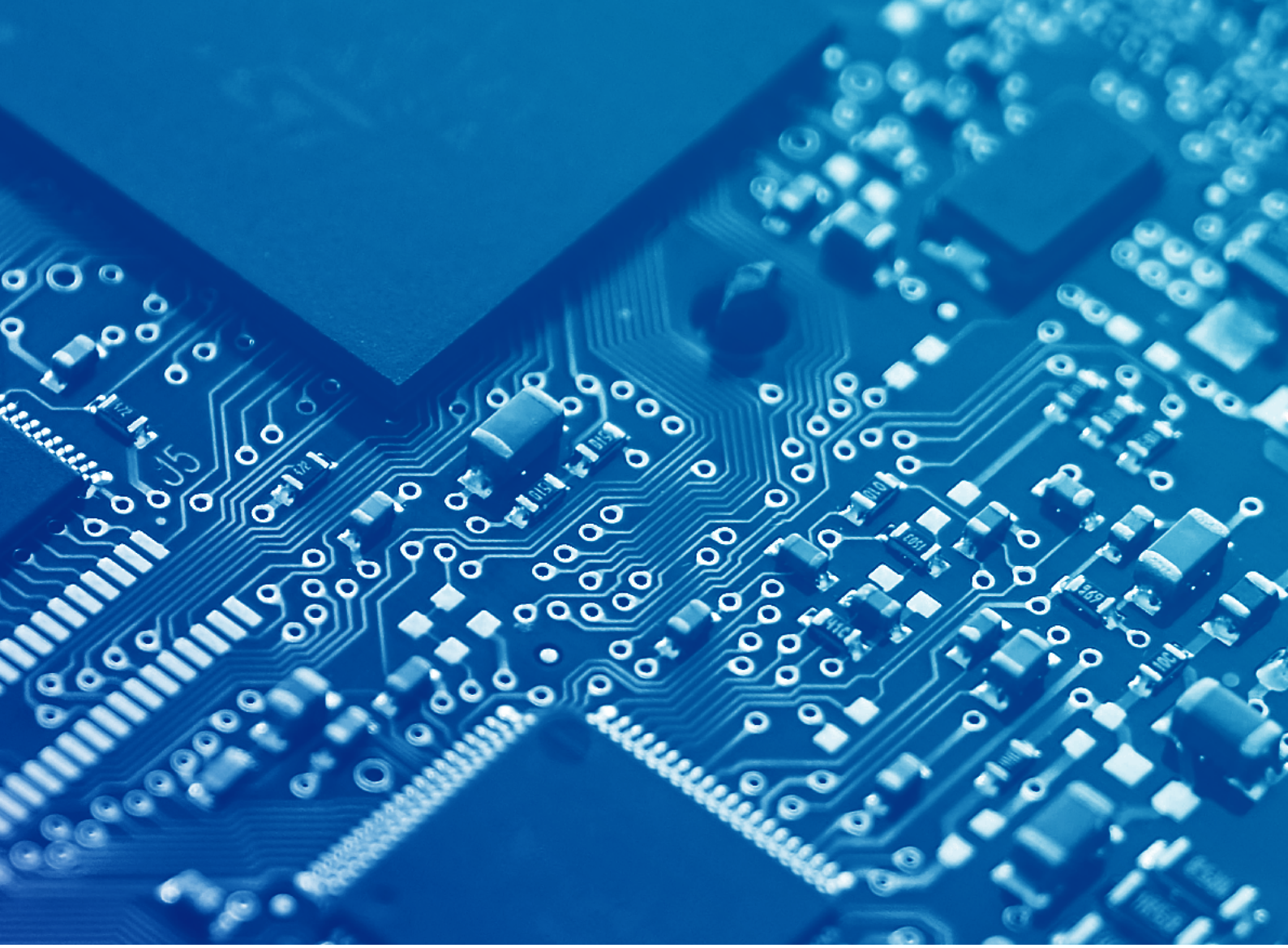
Expand reviews and sunset clauses in digital regulation to encourage flexibility. Given the rate of change in digital technology, regulatory and legal flexibility is key. Review and sunset clauses would compel regulators to consider the effectiveness and relevance of rules. Such clauses would also support consistency with regulation in other democracies. The aforementioned example of the GDPR shows the need for this effort, which also aligns with the imperative of ensuring regulatory certainty and with the importance of reform for future-proofing regulation.

7 – GERMAN AND EU DIGITAL TECHNOLOGY REGULATION (2015 – TODAY)

German Initiative	Stated Aims	EU Initiative	Stated Aims
2015 **IT-Security Law** (IT-Sicherheitsgesetz)	• Set leading standards on IT system security • Protect digital infrastructures, especially in critical technology areas (critical infrastructures/KRITIS) • Establish new warning obligations for telecoms	2016 **NIS Directive**	• Mandate national supervision of critical infrastructure sectors and critical digital service providers • Set requirements for member-state cybersecurity capabilities, including cybersecurity strategies and Computer Security Incident Response Teams (CSIRTS) • Cross-border collaboration
2017 **Network Enforcement Act** (Netzwerkdurchsetzungsgesetz, NetzDG)	• Set up content moderation frameworks for criminally punishable expression such as hate speech and fake news • Establish reporting obligations and penalties for online platforms	2020 **Digital Services Act (DSA) proposal**	• Reform EU-wide digital platform legislation • Set standards on content moderation, advertising, and algorithms • Define obligations including notice-and-action procedures for illegal content
2017 **Data Ethics Commission** (Datenethikkommission)	• Develop ethical guidelines for data policy • Provide a framework to deal with algorithms, AI, and digital innovation • Resolve data ethics questions • Define an approach for overcoming social conflicts within data policy	2021 **Draft AI Act** (derived from the Commission's 2020 AI White Paper)	• Propose a "human-centric" legal framework for trustworthy AI • Address the risks associated with certain uses of AI • Give users confidence to embrace AI-based solutions while encouraging businesses to develop them
2018 **National Research Data Infrastructure** (Nationale Forschungsdateninfrastruktur, NFDI)	• Network data holdings domestically and internationally • Systematically develop, sustainably store, and make accessible scientific and research data	2018 **European Open Science Cloud (EOSC)**	• Provide European researchers, innovators, companies, and citizens with an open, multidisciplinary environment • Provide European science, industry, and public authorities with world-class data infrastructure, high-speed connectivity, and powerful high-performance computers
2019 **Gaia-X initiative**	• Develop a common software governance framework with the objec tive of ensuring European digital sovereignty • Implement a common set of rules that can be applied to existing technology stacks • Obtain transparency, controllability, portability, and interoperability across data and services.	2021 **Alliance for Industrial Data, Edge and Cloud**	• Strengthen the position of EU industry on cloud and edge technologies • Meet the needs of EU businesses and public administrations processing sensitive data • Foster the development and deployment of next-generation cloud and edge capacities for public and private sectors • Important Project of Common European Interest for Next Generation Cloud Infrastructure and Services (IPCEI-CIS) contributes to the review of the EU Industrial Strategy
2019 **Federal Blockchain Strategy**	• Aim to use the opportunities offered by blockchain and mobilize its potential for digital transformation • Five fields of action: blockchain in the financial sector; funding of projects and real labs; clear reliable framework conditions; digital administrative services; knowledge, networking, and collaboration		
2021 **Federal Data Strategy** (Datenstrategie der Bundesregierung)	• Enhance the innovative and responsible use of data • Develop data competency and establish a data culture • Make data infrastructure effective and sustainable • Put state data infrastructure on a sustainable footing and enhance the data competency of civil servants	2022 **Data Act**	• Ensure fairness through rules for the use of data generated by IoT devices • Develop a framework to promote business-to-government data sharing • Support business-to-business data sharing • Evaluate the Integrated Planning and Reporting (IPR) framework with a view to further enhancing data access and use
		2020 **Data Governance Act proposal**	• Increase trust in data sharing • Strengthen data-sharing mechanisms across sectors and the EU, increasing data availability and overcoming technical obstacles to reuse data
		2021 **EU Cloud Code of Conduct**	• Contribute to an environment of trust and transparency in the European cloud computing market • Simplify the risk-assessment process of Cloud Service Providers (CSPs) for cloud customers.
2021 **IT-Security Law 2.0** (IT-Sicherheitsgesetz 2.0)	• Patch gaps to protect critical infrastructures (KRITIS) • Expand competencies of the Federal Office for Information Security (BSI), allowing for stronger cooperation with law enforcement	2021 **NIS Directive reform**	• Broaden NIS mandate to address fragmentation and implementation snags • Coordinate information sharing, reporting obligations, and sanction regimes across the EU • Set more rigorous requirements for critical infrastructure, such as supply chain security

Source: Authors own illustration

German Initiative	Stated Aims	EU Initiative	Stated Aims
2021 **Telecommunications-Telemedia Data Protection Act** (Telekommunikation-Telemedien-Datenschutz-Gesetz, TTDSG)	• Merge provisions on the protection of telecommunications secrecy and data privacy previously contained in the Telecommunications Act (TKG) and in the Telemedia Act into a new parent law • Adapt existing provisions to the European General Data Protection Regulation and to new definitions in the Telecommunications Act	2017 **e-Privacy Regulation proposal**	• Enforce privacy rules on new players, such as WhatsApp, Facebook Messenger, and Skype • Standardize EU privacy protection • Guarantee protection of communications content and metadata • Streamline cookie consent regulation • Protect users more effectively against spam
		2020 **Data Governance Act proposal**	• Safely enable the sharing of sensitive data held by public bodies, and regulate data sharing by public actors • Increase trust in data intermediaries • Strengthen data-sharing mechanisms across the EU
2021 **10th Amendment to the Restriction of Competition Act** (Gesetz gegen Wettbewerbsbeschränkungen, GWB)	• Give the Federal Cartel Office (*Bundeskartellamt*, BKartA) the ability to take preventive measures to curb the market power of large digital platforms • Introduce changes concerning antitrust investigations procedures, leniency, and cartel damage claims.	2020 **Digital Markets Act (DMA)**	• Curb digital gatekeepers' unfair business practices • Create a fairer business environment for businesses dependent on gatekeepers • Allow for freer innovation by technology startups • Eliminate unfair terms and conditions limiting technology development • Expand range of customer choices of service providers
2021 **Amendment to the Telecommunications Act** (TKG)	• Create a tailored and forward-looking legal framework for the German telecommunications market • Strengthen the rights of end users • Accelerate the rollout of fiber-optic and mobile networks	2018 **EU Directive 2018/1972:** Establishing the European Electronic Communications Code	• Consolidate and reform the framework for regulating electronic communication networks and services
2020 **Draft Law implementing EU Directive 2018/1972**	• Expand very-high-capacity networks and their use • Ensure sustainable and effective competition and the interoperability of telecommunications services • Ensure accessibility and security of networks and services • Promote the interests of end users		
2021 **17th Amendment to the Foreign Trade and Payments Act** (Außenwirtschaftsverordnung, AWG)	• Comprehensively protect critical infrastructure and key technologies from foreign investment • Extend notifiable acquisitions to new industries in the cross-sectoral screening • Reduce relevant thresholds for notification obligations • Extend sector-specific screening • Standardize deadlines for cross-sectoral and sector-specific screening	2019 **FDI Screening Regulation**	• Preserve Europe's strategic interests while keeping the EU market open to investment • Address European concerns about the impact of foreign acquisitions • Regulate the notification of existing national investment screening mechanisms to the European Commission (EC) • Establish formal contact points and secure channels in each member state and within the EC for the exchange of information • Develop procedures for member states and the EC to quickly react to FDI concerns
		2021 **Regulation (EU) 2021/821** Control of exports, brokering, technical assistance, transit, and transfer of dual-use items	• Update previous regulatory framework to modernize the EU export controls regime for dual-use items • Set up a regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items • Subject dual-use items to effective control when they are exported from or in transit through the EU • Implement new catch-all controls • Set up national control lists and place new controls on technical assistance including on military end-use • Ensure more information exchange and transparency
2017 **Open Data Act**	• Oblige federal authorities to publish on publicly accessible networks unprocessed data that was obtained when fulfilling public-law duties or through third parties • Establish judicial foundation for obtaining data from all public authorities subject to federal government oversight	2019 **Open Data Directive**	• Strengthen the EU's data economy by increasing the amount of publicly held and publicly funded data available for reuse • Require public bodies to make data available for reuse where possible • Provide real-time access to dynamic data via adequate technical means • Increase the supply of valuable public data for reuse, including from public undertakings • Tackle the emergence of new forms of exclusive arrangements



CHAPTER 5

Germany's Economic Security and Technology

Optimizing Export Control, Investment Screening and Market Access Instruments

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.[142] 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).

142 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).[143] 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.[144] 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.[145] Germany tightened exports after 2015, which led to FinFisher's bankruptcy in 2022.[146] But bureaucratic silos and a lack of systemic foresight remain big hurdles to timely regulation of domestic technology and its use.

143 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).

144 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).

145 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).

146 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).

8 – 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.[147]

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)[148] and Foreign Trade and Payments Ordinance (*Außenwirtschaftsverordnung*, or AWV)[149] to strengthen and modernize foreign direct investment (FDI) control.[150] 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.[151] 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.[152]

147 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).

148 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).

149 Ibid.

150 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).

151 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).

152 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,"[153] 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.[154]

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.[155] 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.[156] 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.[157] 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.

153 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).

154 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).

155 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).

156 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).

157 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.[158] 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.[159] 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.[160]

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.

158 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).

159 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.

160 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).

Amid pandemic-related supply chain bottlenecks, 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.[161] Germany has also updated its supply chain due diligence to consider human rights, including the use of forced labor.[162]

The European Commission, for its part, has pushed for greater onshoring and friend-shoring of technology and strategic inputs, including through industrial policy.[163] 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.[164]

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.[165] 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.[166] Meanwhile, political pressure for rapid 5G rollout is high as

161 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).

162 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).

163 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).

164 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).

165 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).

166 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).

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.[167] 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.[168]

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.[169] 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.[170] 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.[171] Cases of research infiltration by proxies of authoritarian militaries has become an EU concern.[172] 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.[173] 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 with potential docking

167 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).

168 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).

169 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).

170 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).

171 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).

172 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).

173 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).

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.[174]

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.[175] 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,[176] 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*.[177]

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.[178]

174 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).

175 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).

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

177 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).

178 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).

CHAPTER 6

Germany's Global Technology Diplomacy

Strengthening International Technology Alliances, Partnerships, and Norms

CHAPTER OVERVIEW

Key Takeaways

1 The fusion of technological, geopolitical, and ideological ambitions is straining internet governance discourses, cyber norms diplomacy, technical standard-setting, and the global connectivity infrastructure.

2 The German government has made support for global, open, and secure digital connectivity a centerpiece of its foreign policy. However, it has yet to make the shaping of a corresponding international technology agenda a strategic policy priority.

3 To shape a global technology order that reflects Germany's interests as a high-tech industrial economy and democratic society, the government should focus on realizing synergies with EU international digital policy, strengthening coordination with like-minded partners, and engaging with the Global South on an inclusive and democratic global digital agenda.

Introduction

Russia's war against Ukraine rocked Germany's stability-minded "change through trade" doctrine. The conflict consequently unleashed significant knock-on effects on Germany's technology foreign policy, which has important geopolitical and ideological dimensions. China is already pushing for technological leadership in its quest to surpass the United States as a great power by the midpoint of this century. Authoritarian regimes are also harnessing digital technology, once hailed as an enabler of civic challenges to oppression, to tighten their domestic grip on power.

The fusion of technological, geopolitical, and ideological ambitions is straining internet governance discourses, cyber norms diplomacy, technical standard-setting, and the global connectivity infrastructure. Germany must step up its international efforts and work closely with its partners and allies to counter this trend. The country must become an active shaper of a governance landscape that reflects its interests and values as a high-tech player, globalized economy, and liberal democracy.

The State of Play

At the heart of the fragmentation that is rattling international digital governance is the struggle for control over global digital connectivity. The internet's original conception as an open, global, decentralized, and multistakeholder-governed infrastructure clashes with some states' push for exclusive sovereign control over information flows and political expression. China and Russia jointly clarified that they would deem unacceptable "any attempts to limit their sovereign right to regulate national segments of the Internet and ensure their security."[179] Equally worrying is the increasing implementation of interventionist content-monitoring regimes and internet shutdowns similar to that which occurred during anti-government protests in Belarus (summer 2020),[180] Kazakhstan (winter 2021-22)[181] and Iran (fall 2022).[182]

These opposing visions translate into intensifying powerplays around the internet itself, notably within

179 "Russia and China call for internationalization of Internet governance — statement," TASS, February 4, 2022: https://tass.com/economy/1398177 (accessed June 22, 2022).

180 Andrei Makhovsky and Tom Balmforth, "Internet blackout in Belarus leaves protesters in the dark", Reuters, August 11, 2020: https://www.reuters.com/article/us-belarus-election-internet-idUSKCN2571Q4 (accessed September 15, 2022).

181 Elizabeth Zach and Amalia Oganjanyan, "Internet blackout in Kazakhstan amid protests silenced a DW Akademie partner for nearly a week," Deutsche Welle, March 4, 2022: https://www.dw.com/en/internet-blackout-in-kazakhstan-amid-protests-silenced-a-dw-akademie-partner-for-nearly-a-week/a-61017740 (accessed September 15, 2022).

182 Matt Burgess, "Iran's Internet Shutdown Hides a Deadly Crackdown", Wired, September 23, 2022: https://www.wired.co.uk/article/iran-protests-2022-internet-shutdown-whatsapp (accessed 27.10.2022).

the bodies that administrate and develop it.[183] Democratic states of the Global North, including Germany, have responded by reaffirming their support for technical internet governance built around a cluster of multistakeholder bodies, including the Internet Society (ISOC), the Internet Corporation for Assigned Names and Numbers (ICANN),[184] and the Internet Engineering Task Force (IETF). Some are also advancing ambitious regulatory initiatives, such as the EU's Digital Markets Act, to limit large technology companies' centralization and mediation of private and corporate online activity. Importantly, democratic states are building a common political vision through the Christchurch Call for a free, open, and secure internet, the Paris Call for Stability and Security in Cyberspace, and, most recently, the Elmau G7 Resilient Democracies Statement.[185]

These efforts pit democracies against major authoritarian powers, in particular China, Russia, and Iran, that prioritize a vision based on national sovereignty and state control. Internationally, these powers are upping their efforts to shift governance functions away from multistakeholder bodies supported by Germany and its partners. Chinese company Huawei, for example, used the International Telecommunications Union (ITU) to propose a "NewIP" initiative[186] that would renew the internet protocol (IP) suite. This could not only duplicate the work of multistakeholder bodies and undermine interoperability with the existing IP architecture but, some fear, also embed greater opportunities for information control in the internet's logical layer.[187] China is also promoting its cyber sovereignty agenda through parallel institution-building. A recent example is the foundation of the Wuzhen-based World Internet Conference as an international organization.[188]

These fault lines characterize international cyber norms diplomacy, too. Agreement on the OEWG's final report last year was the first time that consensus on cyber norms had been reached in a process open to all UN member states. Notably, the report included agreement on language and on recommendations for responsible state behavior that emanated from UN Governmental Groups of Expert (GGE) meetings.[189] However, differences persist, particularly on the involvement of non-governmental stakeholders and a focus on implementation, both of which Germany supports.[190] A French-Egyptian proposal, supported by Germany, for a Program of Action[191] that aims to invigorate cooperation through a permanent UN forum is at risk of fading into obscurity if not urgently advanced.

Divisions also remain in the area of cybercrime. After a decade of failed attempts, Russia secured approval in December 2019 for a UN General Assembly resolution[192] deciding the elaboration of a new cybercrime convention.[193] Negotiations on the convention commenced this year and will continue until the 78th General Assembly session in 2023.[194] But the resolution is a blow to Germany's goal of strengthening the existing Budapest Convention, and there is concern that a new convention could undermine fundamental freedoms under the pretext of tackling cyber-

183 David Hagebölling, "Internet Governance. Foreign Policy & the Backbone of the Digital Word," DGAP Memo No. 14, German Council on Foreign Relations (September 2021): https://dgap.org/sites/default/files/article_pdfs/dgap-memo-btw21_14_dh_en_0.pdf (accessed June 22, 2022).

184 The 78th ICANN Annual General Meeting will take place in Hamburg October 21-23, 2023.

185 G7 Germany, "2022 Resilient Democracies Statement," (June 27, 2022): https://www.g7germany.de/resource/blob/974430/2057608/61edf594f5ca30fb7b2ae4b79d16f1e6/2022-06-27-g7-resilient-democracies-statement-data.pdf?download=1 (accessed 15 August 2022).

186 Huawei, "New IP-Initiative," 2022: https://www.huawei.com/de/deu/magazin/aktuelles/new-ip (accessed June 22, 2022).

187 Madhumita Murgia and Anna Gross, "Inside China's controversial mission to reinvent the internet," Financial Times, March 27, 2020: https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f (accessed June 27, 2022).

188 World Internet Conference, "Xi sends congratulatory letter to inauguration of World Internet Conference organization," (July 13, 2022): https://www.wuzhenwic.org/2022-07/13/c_788406.htm (accessed August 15, 2022).

189 United Nations General Assembly, "Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report," A/AC.290/2021/CRP.2, March 10, 2021: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (accessed June 22, 2022).

190 Valentin Weber, "How to Strengthen the Program of Action for Advancing Responsible State Behavior in Cyberspace," Just Security, February 10, 2022: https://www.justsecurity.org/80137/how-to-strengthen-the-programme-of-action-for-advancing-responsible-state-behavior-in-cyberspace (accessed June 22, 2022).

191 Governments of France, Egypt and other states, "The future of discussions on ICTs and cyberspace at the UN," August 8, 2020: https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf (accessed July 27, 2022).

192 This UNGA resolution was co-sponsored by Belarus, Cambodia, China, the Democratic People's Republic of Korea, Myanmar, Nicaragua, and Venezuela. United Nations General Assembly, "Countering the use of information and communications technologies for criminal purposes. Report of the Third Committee," A/74/401, November 25, 2019: https://undocs.org/en/A/74/401 (accessed June 22, 2022).

193 United Nations General Assembly, "Countering the use of information and communications technologies for criminal purposes," A/RES/74/247, January 20, 2020: https://undocs.org/A/Res/74/247 (accessed June 22, 2022).

194 United Nations, "General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns over 'Rushed' Vote at Expense of Further Consultations," May 26, 2021: https://www.un.org/press/en/2021/ga12328.doc.htm (accessed June 22, 2022).

crime.[195] Another setback came from the 14th Beijing BRICS statement of June 2022, which reaffirmed these states' support for the Ad Hoc Committee on a new cybercrime convention.[196]

The internet governance and cyber norms discourse also reflects a worrying global trend among G77+ states, many of which are democratic but position themselves between intergovernmental and multistakeholder visions of internet governance. The G7 Democratic Resilience Statement won the backing of the +5 countries (Argentina, India, Indonesia, Senegal, and South Africa) invited to Germany's Elmau summit.[197] But many of those same countries have been reluctant to place the Paris Call and the Declaration for the Future of the Internet (DFI)[198] – signed by Germany, the EU, and more than 60 countries as an effort to articulate a positive and human rights-centered vision for the internet – among the central elements of a global digital order. [199]

The rising ideological fragmentation also translates into efforts to stake out technology-infrastructural spheres of influence, particularly across the Global South. The digital component of China's Belt and Road Initiative (BRI) seeks to connect dozens of countries through Chinese fiber optic cables, satellite navigation systems, data centers, and 5G/6G network infrastructure as well as to promote technologies for smart cities and ports, predictive policing, and health data analytics.[200] This digital BRI extends across the EU's immediate neighborhood, including the Balkans[201] and North Africa,[202] and into Germany itself, with Duisburg seen as the BRI's European endpoint.[203]

To respond to the BRI, the G7, under the German presidency, committed to collectively mobilize $600 billion in public and private investment over the coming five years through its Partnership for Global Infrastructure Investment (PGII).[204] But questions remain as to how these funds will be mobilized and, crucially, how ambitious and competitive the PGII's information and communications technology (ICT) component will be against BRI's digital component, which has already disbursed an estimated $79 billion in investments.[205] Moreover, how the PGII interlinks with the EU's €300 billion Global Gateway initiative launched in late 2021 is yet to be seen.[206] Given the challenging geopolitical context, combining various national, EU, and G7 initiatives into a coherent and competitive strategic response to China's BRI remains a key challenge for Germany and like-minded countries.

Such infrastructure geopolitics are accompanied by a relative decline in the ability of Germany and its European partners to shape global technical standards. China, especially, has been highly successful at positioning technical experts in key Standard-setting Bodies (SSBs). Between 2011 and 2018, China's share of International Standards Organization (ISO) Technical Committee/Subcommittee and Working Group secretariats, respectively, almost doubled and more than tripled.[207] Chinese representatives for the first time in 2020 took on a greater number of new ISO technical

195 Council of the European Union, "EU priorities at the United Nations during the 76th United Nations General Assembly, September 2021 - September 2022 – Council conclusions (12 July 2021)," (July 2021): https://www.consilium.europa.eu/media/51240/st10393-en21.pdf (accessed June 22, 2022).

196 BRICS, "XIV BRICS Summit Beijing Declaration," (June 23, 2022): http://www.brics.utoronto.ca/docs/220623-declaration.html (accessed August 15, 2022).

197 G7 Germany, "2022 Resilient Democracies Statement," (June 27, 2022): https://www.g7germany.de/resource/blob/974430/2057608/61edf594f5ca30fb7b2ae4b79d16f1e6/2022-06-27-g7-resilient-democracies-statement-data.pdf?download=1 (accessed September 15, 2022).

198 "A Declaration for the Future of the Internet," (April 22, 2022): https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf (accessed September 15, 2022).

199 In fact, the DFI was unable to attract the Global South's systemically important democratic technology powers, which include India, South Africa, Brazil, Indonesia, Malaysia, and Mexico.

200 Tyson Barker, "Withstanding the Storm: The Digital Silk Road, Covid-19 and Europe's Options", in Alessia Amighini (ed.), "China After COVID-19. Economic Revival and Challenges to the World", June 2021, pp. 108-138: https://dgap.org/sites/default/files/article_pdfs/ispi-report-2021-china-after-covid.pdf (accessed June 22, 2022).

201 Stefan Vladisavljev, "Surveying China's Digital Silk Road in the Western Balkans," War on the Rocks, August 3, 2021: https://warontherocks.com/2021/08/surveying-chinas-digital-silk-road-in-the-western-balkans (accessed June 22, 2022).

202 Tin Hinane El Kadi, "The Promise and Peril of the Digital Silk Road," Chatham House, June 6, 2019: https://www.chathamhouse.org/2019/06/promise-and-peril-digital-silk-road (accessed June 22, 2022).

203 Philipp Oltermann, "Germany's 'China City': how Duisburg became Xi Jinping's gateway to Europe," The Guardian, August 1, 2018: https://www.theguardian.com/cities/2018/aug/01/germanys-china-city-duisburg-became-xi-jinping-gateway-europe (accessed September 15, 2022).

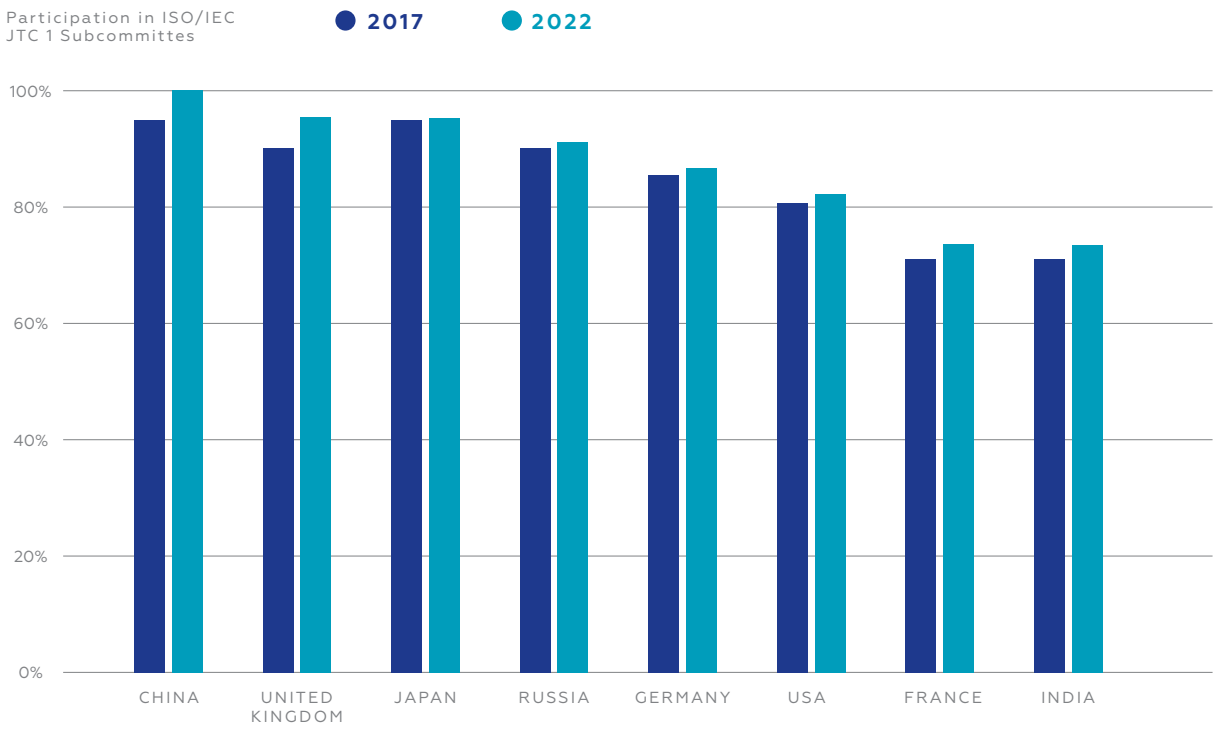
204 G7 Germany, "G7 Leaders' Communiqué," June 28, 2022, pp. 15-16: https://www.g7germany.de/resource/blob/974430/2057914/09bf78deb629910db2c445a1e7595f0b/2022-06-28-leaders-communique-data.pdf?download=1 (accessed June 28, 2022).

205 Sheridan Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain," Bloomberg, January 10, 2019: https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain (accessed September 15, 2022).

206 European Commission, "Global Gateway," (December, 2021): https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/global-gateway_de (accessed June 22, 2022).

207 Tim Rühlig, "The Shape of Things to Come. The Race to Control the Technical Standardisation", December 2021, p. 24: https://www.europeanchamber.com.cn/en/publications-archive/966/The_Shape_of_Things_to_Come_The_Race_to_Control_Technical_Standardisation (accessed June 22, 2022).

9 – COUNTRY REPRESENTATION IN ICT STANDARD-SETTING WITHIN THE ISO/IEC FRAMEWORK



Source: Authors' illustration based on data compiled from the official ISO and IEC websites

leadership positions than Germany.[208] Notably, China is the only country that participates in every subcommittee of the Joint Technical Committee (JTC 1), which is central to the development of ICT standards within the ISO/International Electrotechnical Commission (IEC) framework, including for cloud computing, the Internet of Things, and AI.[209] Chinese nationals have also recently held, or are holding, the top leadership position at the ISO,[210] the ITU,[211] and the IEC.[212]

For Germany and Europe, the creeping shift from standard-setter to standard-adopter risks inflicting substantial adjustment costs on industry.[213] Germany still accounts for more secretariats than the United States, China, and other major countries in the ISO and IEC.[214] But China's state-centric standardization system has allowed Beijing to expand influence strategically in domains such as AI and 5G networking.[215] This is also a political concern. Standards can enshrine values, such as privacy

208 Ibid., p. 25.

209 Data compiled from ISO and IEC websites.

210 Xinhua, "ISO elects first Chinese president," Xinhua, September 21, 2013: http://www.china.org.cn/world/2013-09/21/content_30091790.htm (accessed June 22, 2022).

211 International Telecommunication Union (ITU), "Office of the Secretary-General," 2022: https://www.itu.int/en/osg/Pages/default.asp (accessed September 3, 2022).

212 International Electronical Commission (IEC), "IEC Leadership," 2022: https://www.iec.ch/leadership (accessed June 22, 2022).

213 On adjustment costs and the power politics of international standard-setting, see Walter Mattli and Tim Büthe, "Setting International Standards: Technological Rationality or Primacy of Power?," World Politics, 56(1) (2011), pp. 1-42: https://www.cambridge.org/core/journals/world-politics/article/setting-international-standards-technological-rationality-or-primacy-of-power/950CCFEEFE34691BF6E2584141B0023A (accessed June 22, 2022).

214 Tim Rühlig, "The Shape of Things to Come. The Race to Control the Technical Standardisation", December 2021, p. 24: https://www.europeanchamber.com.cn/en/publications-archive/966/The_Shape_of_Things_to_Come_The_Race_to_Control_Technical_Standardisation (accessed June 22, 2022).

215 Valentina Pop et al., "From Lightbulbs to 5G, China Battles West for Control of Vital Technology Standards," The Wall Street Journal, February 8, 2021: https://www.wsj.com/articles/from-lightbulbs-to-5g-china-battles-west-for-control-of-vital-technology-standards-11612722698 (accessed June 22, 2022).

protection (or the lack thereof), and may turn into national security threats when they (deliberately) include cyber vulnerabilities that become unknowingly adopted around the world.[216]

Yet, amid this fragmentation, a new institutional architecture for the governance of emerging technologies is starting to develop. AI is a key example of this, given the G7-initiated Global Partnership on AI (GPAI), the Organisation for Economic Co-operation and Development's Council on AI, the Council of Europe's Ad Hoc Committee on AI (CAHAI), and major technology companies' AI principles. Similar governance ecosystems are expected to develop and create norms and standards for quantum technologies, the use of cryptocurrencies, a distributed ledger-based internet (Web3), and smart and green technologies. This will open a critical diplomatic playing field for Germany, the EU, and their partners.

The Current Policy Approach

Germany's commitment to multilateralism and a rules-based order strongly shapes its approach to international technology policy. The *Ampel* government has made strengthened multilateralism and support for global, open, and secure digital connectivity a centerpiece of its foreign policy.[217]

Consistent with this outlook, Germany is a key player in the construction of a multilateral architecture for technology cooperation. Following the UN High-Level Panel on Digital Cooperation, Germany, with the United Arab Emirates, championed proposals for a framework for global digital cooperation that include a reformed Internet Governance Forum (IGF).[218] Germany convened the IGF in 2019 and is considering hosting the 2025 gathering. Germany is also advancing the establishment of a normative order in cyberspace. It is a supporter of the Paris Call for Trust and Security in Cyberspace[219] and is engaged in the Organization for Security and Cooperation in Europe, the Council of Europe's work on artificial intelligence (CAHAI) and data protection (Convention 108+), and the UN OEWG on ICT in the context of international security.

At the same time, Germany is struggling to leverage its participation in smaller and more informal groups to develop a forward-looking technology agenda with like-minded states. Germany's 2017 G20 presidency demonstrated the country's ability to anchor technology as a core issue, including by hosting the G20's first-ever digital ministers' meeting.[220] However, the government's prism on digital issues remains primarily commercial. During its current G7 presidency, Berlin boosted its rhetoric on challenges such as internet fragmentation and digital authoritarianism.[221] In substance, however, Germany chose not to make digital issues a strategic policy priority.[222]

Germany is, however, actively drawing on its extensive diplomatic network and development apparatus to engage with the Global South on digital issues. It has recently revived regular digital dialogue with key countries, such as Brazil, Japan, and India, to prepare joint research and development projects, discuss cyber issues, and coordinate work in multilateral

216 Tim Rühlig, "The Rise of Tech Standards Foreign Policy," DGAP Online Commentary, German Council on Foreign Relations (February 2022): https://dgap.org/en/research/publications/rise-tech-standards-foreign-policy (accessed June 22, 2022).

217 Sozialdemokratische Partei Deutschlands (SPD), BÜNDNIS 90/DIE GRÜNEN and Freie Demokratische Partei (FDP), "Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit" [Risking more progress. Alliance for freedom, justice and sustainability], (December 2021), pp. 114-115: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf (accessed June 22, 2022).

218 The Federal Government of the Federal Republic of Germany and the Government of the United Arab Emirates, "Recommendation 5A/B. Options for the Future of Global Digital Cooperation," (September 2020): https://www.global-cooperation.digital/GCD/Redaktion/EN/Downloads/options-for-the-future-of-global-digital-cooperation.pdf?__blob=publicationFile&v=2 (accessed June 22, 2022).

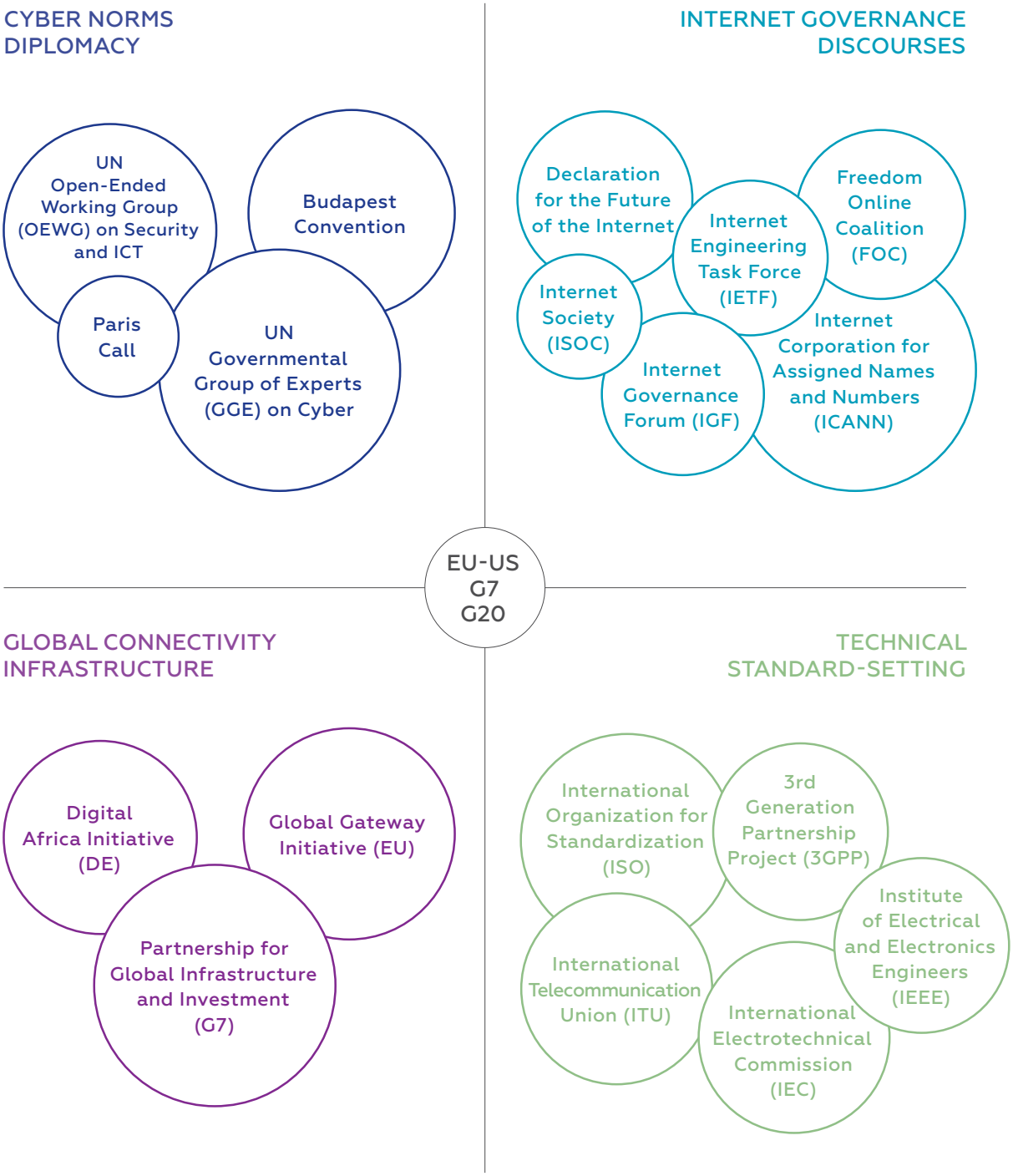
219 The Paris Call for Trust and Security in Cyberspace, "Home," (2021): https://pariscall.international/en (accessed June 22, 2022).

220 Federal Ministry for Economic Affairs and Climate Action (BMWK), "G20 – Shaping digitalization at global level," (2022): https://www.bmwi.de/Redaktion/EN/Artikel/Digital-World/g20-shaping-digitalisation-at-global-level.html (accessed June 22, 2022).

221 G7 Digital Ministers' meeting, "Ministerial Declaration," (May, 2022): https://www.bundesregierung.de/resource/blob/998440/2038510/e8ce1d2f3b08477eeb2933bf2f14424a/2022-05-11-g7-ministerial-declaration-digital-ministers-meeting-en-data.pdf?download=1 (accessed June 22, 2022).

222 In fact, the digitalization section comes last in the 28-page G7 leaders' summit communiqué. G7 Germany, "G7 Leaders' Communiqué," June 28, 2022: https://www.g7germany.de/resource/blob/974430/2062292/9c213e6b4b36ed1bd687e82480040399/2022-07-14-leaders-communique-data.pdf?download=1 (accessed June 28, 2022)

10 – KEY INSTITUTIONS AND INTIATIVES FOR GERMAN INTERNATIONAL TECHNOLOGY POLICY



Source: Authors' illustration

settings.[223] The bilateral format has proven useful, and Berlin is negotiating similar digital dialogues with South Korea, Indonesia, and Argentina. Germany has also recognized Africa's strategic importance in the digital sphere. Since 2015, it has channeled €164 million into digital projects through its "Digital Africa" initiative[224] and initiated more than 200 public-private partnerships in the African technology sector.[225] The digital and foreign ministries are scoping institutionalized digital dialogue with multistakeholder participation from the private sector, civil society, and subnational governments in the African Union, Kenya, South Africa, and Ghana. Intensified digital cooperation with Egypt is under consideration.

But as the strategic stakes rise, Germany's leverage to shape global digital governance increasingly depends on realizing synergies with EU efforts. Germany's technology diplomacy is, in fact, embedded in a larger turn toward a distinctly (geo-)strategic outlook on technology policy at the EU level. The bloc's Digital Compass for 2030 affirms that technology is a factor in "global influence,"[226] and Brussels emphasizes, more than the German policy discourse does, the link between digital sovereignty and European values.[227]

The EU has begun to translate this link into actionable foreign policy. This includes formats such as the EU-US Trade and Technology Council (TTC) (whose Paris meeting, for instance, launched new ICT security guidelines for trustworthy vendors in development initiatives, expanding the EU's 5G cybersecurity toolbox), the new TTC with India,[228] and the Global Gateway initiative.[229] Against the backdrop of Russia's aggression against Ukraine, the EU-US TTC, in particular, is developing into a vehicle for democratic coordination on issues ranging from investment screening and export controls to resilient semiconductor supply chains.[230] The EU is also opening an office in Silicon Valley to strengthen transatlantic engagement on digital agendas.[231]

Recommendations

Germany's success as a shaper of a global technology order that enables it as a leading high-tech industrial economy and bends towards democracy will depend on how successfully it nests its values and interests in a set of alliances, partnerships, and norms. To that end, German should:

Advance the notion of a democratic technology trust zone. This trust zone would regulate flows of skills, capital, and data to boost competitiveness and trustworthiness for strategically important ICT infrastructure such as network equipment, cloud/edge service providers, and smart city technology. It should be built on regulatory best practices and a strategic approach to technology-industrial policy that leverages mutual dependencies to lock in cooperation and safeguard access to critical technologies and materials. To that effect, the government should support a strong institutional nucleus in the form of an ambitious G7 digital ministerial meeting, an expanded OECD digital agenda, and intensified EU-US TTC meetings.

223 E.g., Auswärtiges Amt, "Deutsch-indische Cyberkonsultationen" [German-Indian Cyber Consultations], December 14, 2017: https://www.auswaertiges-amt.de/de/aussenpolitik/themen/cyber-aussenpolitik/indien-cyberkonsultationen/1890390 (accessed June 28, 2022).

224 Kooperation International, "Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung: Start der digitalen Lernplattform "Africa Cloud" angekündigt" [Federal Ministry for Economic Cooperation and Development: Launch of digital learning platform "Africa Cloud" announced], (November 2019): https://www.kooperation-international.de/aktuelles/nachrichten/detail/info/bundesministerium-fuer-wirtschaftliche-zusammenarbeit-und-entwicklung-start-der-digitalen-lernplattf (accessed June 22, 2022).

225 Federal Ministry for Economic Cooperation and Development, "Strategische Partnerschaft Technologie in Afrika" [Strategic Partnership Technology in Africa] (2022): https://www.bmz.de/de/mitmachen/wirtschaft/digitales-afrika-13718 (accessed June 22, 2022).

226 European Commission, "2030 Digital Compass: the European way for the Digital Decade," March 9, 2021, p. 18: https://ec.europa.eu/info/sites/default/files/communication-digital-compass-2030_en.pdf (accessed June 28, 2022).

227 Notably, European Commission President Ursula von der Leyen defined "tech sovereignty" as "the capability that Europe must have to make its own choices, based on its own values, respecting its own rules." European Commission, "Shaping Europe's digital future: op-ed by Ursula von der Leyen, President of the European Commission," February 19, 2020: https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260 (accessed June 22, 2022).

228 European Commission, "EU-India: Joint press release on launching the Trade and Technology Council," April 25, 2022: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2643 (accessed June 22, 2022).

229 European Commission, "Global Gateway," December 2021: https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/global-gateway_de (accessed June 22, 2022).

230 European Commission, "EU-US Trade and Technology Council Inaugural Joint Statement," September 29, 2021: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951 (accessed June 22, 2022).

231 Euractiv, "Neues EU-Büro im Silicon Valley für Big-Tech-Diplomatie" [New EU office in Silicon Valley for Big Tech diplomacy], (July 28, 2022): https://www.euractiv.de/section/innovation/news/neues-eu-buero-im-silicon-valley-fuer-big-tech-diplomatie (accessed August 15, 2022).

Establish a global connectivity doctrine with open internet access as a fundamental right. Germany should work with EU members and other like-minded democracies to devise jointly financed "connectivity packages" that bundle digital infrastructure assistance with cyber capacity-building and long-term support for local digital rights NGOs. But cooperation must extend beyond national governments. Germany should prod the EU and NATO, in addition to like-minded countries, to provide capabilities (e.g., satellites) that expand connectivity, narrow the global digital divide and serve UN Sustainable Development Goals on connectivity (9c) as well as maintain open information flows during authoritarian-driven Internet shutdowns and in conflict zones.

Create a German Open Tech Foundation. The *Ampel* coalition specifically refers to digital sovereignty in the Global South as a priority for ensuring freedom to choose vendors, platforms, and ICT infrastructure; avoiding lock-in effects; and guaranteeing an individual, not state-centric, notion of digital self-determination. The newly established Sovereign Tech Fund provides a means of financially supporting open source and open technology, principally in Germany. It should be complemented with a German Open Tech Foundation to provide international funding, particularly among communities in the Global South, for development of democracy-affirming and privacy-enhancing technologies in line with the coalition's global understanding of digital sovereignty.

Counter politicization of critical and emerging technologies standard-setting. As the weight of non-market economies in SSBs grows, Germany should initiate an international study group that identifies whether and what political instruments may be used to capture standard-setting for critical and emerging technologies. This should form the basis for coordinated engagement with SSBs on ensuring the primacy of technical criteria and preserving SSBs' reputation for impartiality. The German government should also encourage high-quality draft introductions, for example by allowing the participation of the academic and small- and medium-sized enterprise (SME) sectors in emerging technology standards work to be considered funding-eligible R&D.

Work to avoid the emergence of a digital "Non-Aligned Movement". A democratic technology order must reach beyond the transatlantic community. Worryingly, as technology becomes increasingly geopolitical, G77+ states are avoiding a clear affirmation of a common democratic technology agenda. India is a pivotal but complex partner in this regard. Germany already revived in 2022 its digital dialogue with India and included the country in this year's G7 guest list. Given India's 2023 G20 presidency, Germany should now build on this to emphasize India's democratic responsibility to champion an inclusive digital agenda centered on climate-friendly technology as well as open and free connectivity.[232]

Engage collaboratively in EU-US technology dialogue, especially in the TTC. Germany should create a bilateral digital dialogue with the United States that can align and amplify policy deliverables from the TTC.[233] But Germany should also increase its engagement elsewhere, particularly in a constructive conclusion to and implementation of the post-Privacy Shield Transatlantic Data Privacy Framework. The German-American Futures Forum, which was conceived as part of the July 2021 Washington Declaration[234] and whose initial meeting will occur in November 2022, could be another vehicle for deeper engagement, specifically on democracy-enabling technologies and norms.

Create asymmetric technology alliances with subnational governments. Cities and states are increasingly assuming digital governance responsibilities that national governments are unwilling or unable to undertake. In the United States, cities and states have led in data protection, in part by placing guardrails around AI-powered facial recognition technology and algorithmic bias in sensitive areas such as hiring. In China, Brazil, and India, subnational governments are driving technology-industrial and regulatory policy. Germany, in line with the European Council's new digital diplomacy conclusions, should work with subnational governments to build technology alliances that reflect German and EU regulatory values and support subnational adoption of cyber and internet governance norms.

232 David Hagebölling, Valentin Weber, Christoph Meinel and Tyson Barker, "Governing the internet for the global common good", Global Solutions Journal, 8 (2022), pp. 124-133: https://www.global-solutions-initiative.org/wp-content/uploads/2022/03/Global-Solutions-Journal-Issue-8.pdf (accessed, June 29, 2022).

233 Tyson Barker, "The Hidden G2 for Democratic Tech Governance is the EU-US Relationship," (June 2022): https://dgap.org/sites/default/files/article_pdfs/dgap_analysis_no._2_june_10_2021_18_pp_0.pdf (accessed August 15, 2022).

234 The Federal Government, "A German-American partnership for the future," (July 16, 2021): https://www.bundesregierung.de/breg-en/news/federal-chancellor-usa-trip-1942938 (accessed August 15, 2022).

CHAPTER 7

Ethical and Operational

Emerging and Disruptive Technologies, the German Military, and the *Zeitenwende*

CHAPTER OVERVIEW

Key Takeaways

1 Germany's future contribution to European and allied security depends on the Bundeswehr's ability to harness emerging and disruptive technologies (EDTs) such as artificial intelligence, 5G/6G cellular network technology, Low Earth Orbit (LEO) satellite connectivity, and quantum communications and computation.

2 Even amidst Russia's war of aggression against Ukraine, Germany continues to be mired in siloed conceptual, institutional, and ethical thinking that results in disconnections between the military and the technology sector, and even between Germany and its allies.

3 The *Zeitenwende* should catalyze not only a defense budgetary increase but a reconciliation between ethics and military requirements regarding EDTs if Germany is to look beyond immediate needs and ensure the Bundeswehr's future operational readiness.

Introduction

Russia's war of aggression against Ukraine has jolted Germany into drastically adjusting its defense posture. After decades of atrophy, the Bundeswehr is filling gaps in its basic military capabilities. There is also growing recognition among German policymakers that deeper integration of intelligent systems, organizational transformation around high-tech warfare, and fusing cyber and physical domains are critical to the Bundeswehr's future operational readiness.

And yet, Germany continues to be mired in siloed conceptual, institutional, and ethical thinking that results in little innovation and disconnections between the military and the technology sector, and even between Germany and its allies. Reconciling ethical concerns with battlefield realities is key to modernizing German armed forces, as is adjusting policies to account for the close linkage between military and civilian technology development and use.

The State of Play

Emerging and disruptive technologies (EDTs), such as artificial intelligence (AI), 5G/6G cellular network technology, Low Earth Orbit (LEO) satellite connectivity, and quantum communications and computation, are set to transform the Bundeswehr's operational environment. The German military considers the deeper integration of machine intelligence into military operations, especially through the massive deployment of unmanned systems, a key challenge for its operations this decade.[235] Indeed, highly automated unmanned aerial systems (UAS) were significant assets in recent conflicts such as that in Nagorno-Karabakh.[236] EDTs are also becoming indispensable to strategic planning and forecasting, with AI algorithms extracting insights from large data pools generated by a rapidly increasing number of sensors. The German Armed Forces Space Command, for example, is already deploying two machine learning applications to help produce situation pictures.[237]

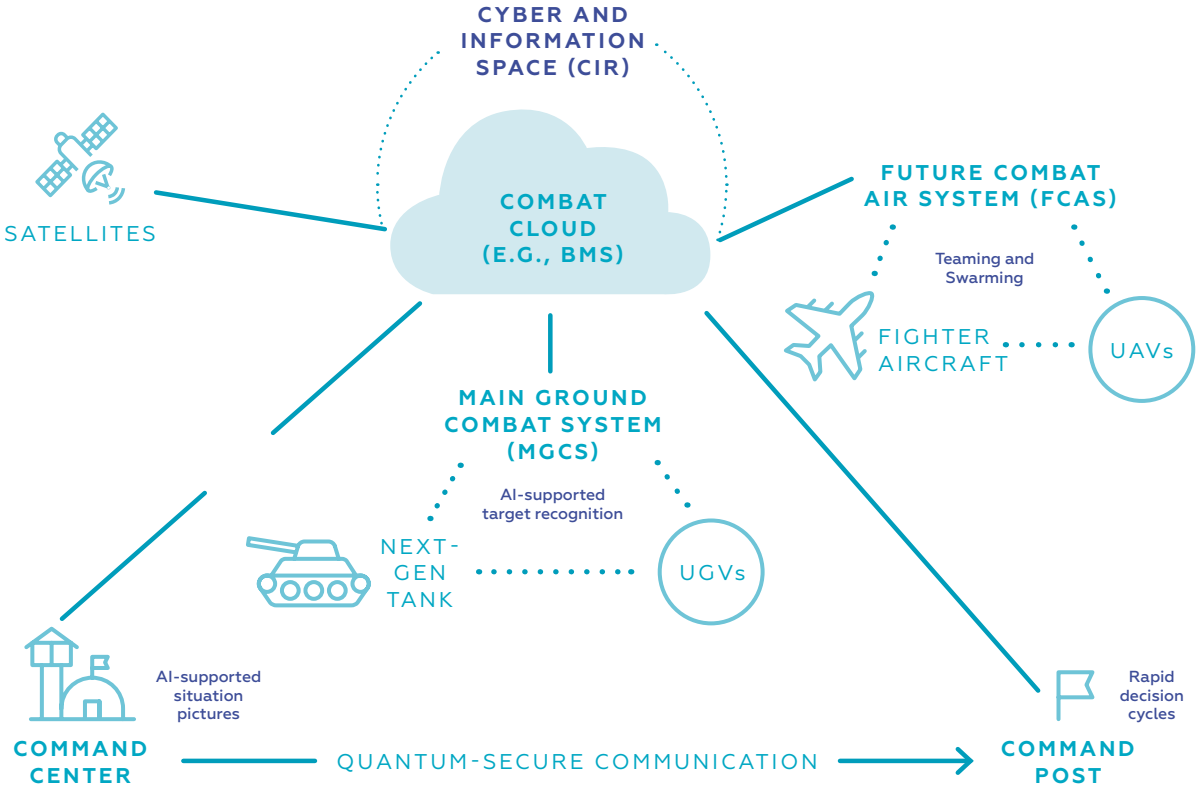
Crucially, in this changing environment, the *Bundeswehr*'s ability to harness EDTs for future operational effectiveness depends on close cooperation with EU and NATO allies and, therefore, sustained political capital spent on joint initiatives. Germany's current efforts to marshal EDTs are closely tied to joint

235 See Kommando Heer, "Thesenpapier I: Wie kämpfen Landstreitkräfte künftig?" [Thesis Paper I: How will land forces fight in the future?], Kommando Heer (2017): https://augengeradeaus.net/wp-content/uploads/2018/03/180327-Thesenpapier-I-Wie-ka%CC%88mpfen-LaSK-zuku%CC%88nftig.pdf (accessed July 18, 2022).

236 German Bundestag, *Zum Drohneneinsatz im Krieg um Bergkarabach im Jahre 2020* [On the use of drones in the war over Nagorno-Karabakh in 2020], WD2-3000-113/20, (January 2021): https://www.bundestag.de/resource/blob/825428/5b868defc837911f17628d716e7e1e1d/WD-2-113-20-pdf-data.pdf (accessed May 31, 2022).

237 BWI, "Künstliche Intelligenz: BWI entwickelt Lösungen für die Bundeswehr" [Artificial intelligence: BWI develops solutions for the Bundeswehr], January 24, 2022: https://www.bwi.de/news-blog/blog/artikel/kuenstliche-intelligenz-bwi-entwickelt-loesungen-fuer-die-bundeswehr (accessed May 31, 2022).

11 – HOW EMERGING AND DISPRUTIVE TECHNOLOGIES SHAPE THE BATTLEFIELD OF THE FUTURE



Source: Authors' illustration

European defense projects for forthcoming weapons platforms, including the Future Combat Air System (FCAS)[238] with France and Spain, and the Main Ground Combat System (MGCS)[239] with France. Neither is expected to be operational until the 2040s, but these systems will be able to provide the *Bundeswehr* with advanced capabilities such as deep integration into a joint combat cloud and intelligent human-machine teaming.[240]

German defense is also confronting a need to prepare *organizationally* for high-tech warfare. Conflicts are being fought at machine speed, necessitating quicker decision-making closer to the front. This requires more decentralized command structures with highly connected units. The *Bundeswehr* is consequently rolling out the Battle Management System (BMS) SitaWare Frontline, a new digital leadership solution that enables access to real-time information

238 Airbus, "Future Combat Air System (FCAS)": https://www.airbus.com/en/products-services/defence/multi-domain-superiority/future-combat-air-system-fcas (accessed May 31, 2022).

239 Hensoldt, "MGCS – The Smart Tank is Rolling in," (April 2021): https://www.hensoldt.net/stories/mgcs/ (accessed May 31, 2022).

240 "FCAS-Anforderungen festgelegt" [FCAS Requirements Set], *FlugRevue*, August 31, 2021: https://www.flugrevue.de/militaer/industrie-muss-sich-einigen-fcas-anforderungen-festgelegt/ (accessed May 31, 2022); André Uzulis, "MGCS – Ein neues Kampfsystem für das Heer" [MGCS – A new combat system for the army], *.loyal das Magazin*, (April 1, 2021): https://www.reservistenverband.de/magazin-loyal/mgcs-ein-neues-kampfsystem-fuer-das-heer/ (accessed May 31, 2022).

for digitally networked warfare.[241] The *Bundeswehr* aims to make the BMS operational by 2023, when it assumes leadership of NATO's Very High Readiness Joint Task Force.[242]

Germany has also taken important steps to prepare for the fusion of physical combat and cyber domains that accompanies defense-technological developments. The country has significantly expanded its cyber-institutional complex and earned a high national cyber power ranking.[243] As its use of digital technologies in systems and command structures has expanded, the *Bundeswehr* has pooled resources into a dedicated military branch, the Cyber and Information Space (CIR).[244] The German defense ministry is also enhancing its capabilities in secure quantum communication networks, in part through a dedicated lab at its CODE cybersecurity research institute.[245] The lab is developing MuQuaNet, a prototype of such a network.[246]

Precisely because the *Bundeswehr* must deal with potential military escalation in the cyber domain, ethical qualms are heightened. AI, for its part, can be used to automate cyber activities, thereby allowing an increase in the scale and frequency of cyberattacks.[247] AI also potentially incentivizes risk-taking since defensive techniques may be developed and scaled more slowly than offensive ones.[248] At the same time, attributing cyberattacks is complicated and time-consuming.[249] The German military may find itself obliged to act against a perceived malicious actor (state or non-state) on the basis of ambiguous information regarding responsibility or intent (e.g., espionage vs. sabotage).[250] As AI and other EDTs raise the stakes in cyberspace, Germany is still in the process of forging coherent and proportionate responses to these challenges.

Cooperation between the defense and technology sectors, and organizational adaptation, remain major challenges for the Bundeswehr. Notably, the situation is complicated by German society's deep ethical concerns about diminishing human agency and responsibility due to EDT usage. The Bundeswehr recognizes these concerns and is attempting to reconcile them with battlefield realities, command structures, and decision-making processes. An example of this is the explicit modelling of legal and ethical implications in its AI-based "GhostPlay" simulation environment.[251] At the same time, a German divergence from allies' generally more robust and pragmatic approach to dual-use EDTs can add further complexity to the joint planning of – and especially feature specification in – defense initiatives encompassing usage of advanced machine intelligence such as FCAS.

241 The BMS is based on the SitaWare software family that many NATO partners use. *Bundeswehr*, "Battle Management System - CIR digitalisiert" [Battle Management System - CIR digitalized]: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/auftrag/digitalisieren/gefechtsfuehrung-der-zukunft-das-battle-management-system (accessed May 31, 2022).

242 *Bundeswehr*, "Digitalisierung im Heer" [Digitalization in the army]: https://www.bundeswehr.de/de/organisation/heer/organisation/faehigkeiten/digitalisierung (accessed May 31, 2022).

243 See, e.g., Julia Voo et al., "National Cyber Power Index 2020. Methodology and Analytical Considerations," China Cyber Policy Initiative/Belfer Center for Science and International Affairs (September 2020): https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf (accessed May 31, 2022); International Telecommunication Union (ITU), "Global Cybersecurity Index 2020," (2022): https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (accessed May 31, 2022).

244 *Bundeswehr* Cyber- und Informationsraum [Bundeswehr Cyber and Information Space]: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum (accessed May 31, 2022).

245 Universität der Bundeswehr München, "CODE – Über Uns" [CODE – About us]: https://www.unibw.de/code/im-profil/ziele (accessed June 28, 2022).

246 Universität der Bundeswehr München, "Q-Lab,": https://www.unibw.de/code/forschung/zentrallabore/q-lab (accessed May 31, 2022).

247 James Johnson and Eleanor Krabill, "AI, Cyberspace, and Nuclear Weapons," *War on the Rocks*, January 31, 2020: https://warontherocks.com/2020/01/ai-cyberspace-and-nuclear-weapons/ (accessed May 31, 2022).

248 Ben Garfinkel and Allan Dafoe, "Artificial Intelligence, Foresight, and the Offense-Defense Balance," *War on the Rocks*, December 19, 2019: https://warontherocks.com/2019/12/artificial-intelligence-foresight-and-the-offense-defense-balance/ (accessed May 31, 2022).

249 German Bundestag, "Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare)" [Applicability of international humanitarian law to computer network operations and digital warfare (cyber warfare)], WD2-3000-038/15, (February 2015), pp. 12-13: https://www.bundestag.de/resource/blob/406028/de1946480e133cf38bbee41d8d3d6898/WD-2-038-15-pdf-data.pdf (accessed May 31, 2022).

250 James M. Action, "Cyber Warfare & Inadvertent Escalation," *Daedalus* Vol. 149, Issue 2 (April 2020), pp. 133-149: https://direct.mit.edu/daed/article/149/2/133/27317/Cyber-Warfare-amp-Inadvertent-Escalation (accessed May 31, 2022). Such ambiguity is particularly problematic when diverse military capabilities are entangled in cyber-physical systems. The detection of malware in missile defense early warning systems, for example, could be interpreted as preparation for a nuclear first strike even if it intends to weaken conventional ballistic missile defense. James M. Acton, "Why is Nuclear Entanglement So Dangerous?" Carnegie Endowment for International Peace (January 23, 2019): https://carnegieendowment.org/2019/01/23/why-is-nuclear-entanglement-so-dangerous-pub-78136 (accessed May 31, 2022).

251 Center for Digitalization and Technology Research of the Bundeswehr (dtec.bw), "GhostPlay – Simulation für KI-basierte Entscheidungsverfahren" [GhostPlay - Simulation for AI-based decision processes]: https://dtecbw.de/home/forschung/hsu/projekt-ghostplay (accessed May 31, 2022).

The Current Policy Approach

The February 2022 *Zeitenwende* announcement[252] is meant to reverse years of economizing Germany's military. But the new €100 billion special fund barely covers the Bundeswehr's basic needs. Germany needs a far more systemic budgetary – and ethical-cultural – transformation if it is to look beyond these needs and ready itself for future requirements. The first step is for the government to develop a cohesive vision for EDTs in the military.

In the 20th century, nuclear power and stealth technology, even the internet, were developed for military purposes. Civilian uses were subsequently found. Now the trend is reversed: Civilian technologies are becoming key to military prowess. Yet Germany's White Paper (2016) on security policy and the future of the Bundeswehr[253] and its recent position paper (2021) on the Bundeswehr's future[254] make little reference to the disruptive potential of technologies driven primarily by civilian innovation, including AI, quantum, and 5G/6G connectivity.[255]

Moreover, Germany's key technology policy documents illustrate that the government, even when dealing with EDTs with obvious dual-use potential, perpetuates an artificial civilian-military divide for development and regulation. Germany's High-Tech Strategy 2025 (2018)[256] and Industrial Strategy 2030 (2019)[257] deal with the commercial dimension, but defense considerations are entirely absent in the former and marginal in the latter. This also holds for Germany's AI strategy (2017, 2020)[258] and 5G strategy (2017).[259] Germany's cyber strategy (2021)[260] sees cybersecurity primarily through the civilian lens of law enforcement and the judiciary.[261]

The siloed treatment of EDTs in the military context reflects the dynamics of Germany's difficult ethical debates. Indeed, the country's political positions on military technologies have been primarily reactive, risk-averse, and driven by societal controversy. With the April 2022 decision to weaponize its Heron drones,[262] the German government put an end to an almost decade-long discussion[263] that frequently conflated notions of unmanned and autonomous systems.[264] Germany continues to rule out the use of fully autonomous drones and is one of the most vocal supporters of a ban on such systems in international law.[265]

252 The Federal Government, "Regierungserklärung von Bundeskanzler Olaf Scholz am 27. Februar 2022" [Government Statement by Chancellor Olaf Scholz on February 27, 2022]: https://www.bundesregierung.de/breg-de/suche/regierungserklaerung-von-bundeskanzler-olaf-scholz-am-27-februar-2022-2008356 (accessed May 31, 2022).

253 The Federal Government, "White Paper 2016 on German Security Policy and the Future of the Bundeswehr", (July 13, 2016): https://www.bundeswehr.de/resource/blob/4800140/fe103a80d8576b2cd7a135a5a8a86dde/download-white-paper-2016-data.pdf (accessed May 31, 2022).

254 Federal Ministry of Defence, "Positionspapier: Gedanken zur Bundeswehr der Zukunft" [Position Paper. Thoughts on the Bundeswehr of the future], (February 9, 2021): https://augengeradeaus.net/wp-content/uploads/2021/02/20210209_AKK_GI_Bundeswehr_der_Zukunft.pdf (accessed May 31, 2022).

255 This is heavily reflected in the almost complete absence of direct references to key dual-use EDTs (e.g., artificial intelligence: 1 reference; 5G or 6G: 0 references; quantum: 0 references) in the 143-page white paper.

256 References to security challenges are limited to civilian (IT) security. Federal Government, "Forschung und Innovation für die Menschen: Die High-Tech Strategie 2025" [Research and Innovation for the people: The high-tech strategy 2025], (September 2018): https://www.hightech-strategie.de/SharedDocs/Publikationen/de/hightech/pdf/forschung-und-innovation-fuer-die-menschen.pdf?__blob=publicationFile&v=4 (accessed June 19, 2022).

257 Federal Ministry for Economic Affairs and Energy (BMWi), "Made in Germany: Die Industriestrategie 2030" [Made in Germany: The industrial strategy 2030], (November 2019): https://www.bmwi.de/Redaktion/DE/Dossier/industriestrategie-2030.html (accessed May 31, 2022).

258 The Federal Government, "Nationale Strategie für Künstliche Intelligenz" [National strategy for artificial intelligence]: https://www.ki-strategie-deutschland.de/home.html (accessed May 31, 2022).

259 The Federal Government, "5G Strategie für Deutschland" [5G strategy for Germany], (July 2017): https://www.bmvi.de/blaetterkatalog/catalogs/350336/pdf/complete.pdf (accessed May 31, 2022).

260 Federal Ministry of the Interior, Building and Community, "Cybersicherheitsstrategie für Deutschland 2021" [Cybersecurity strategy for Germany 2021], (August 2021): https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=1ABEA4EB553C692E35A59577B182FCC4.2_cid287?__blob=publicationFile&v=1 (accessed May 31, 2022).

261 As such, it emphasizes issues that include disinformation campaigns and cybercrime.

262 Federal Ministry of Defence, "Weg frei zur Bewaffnung der Drohne Heron TP mit Präzisionsmunition" [Way cleared for arming the Heron TP drone with precision ammunition], (April 6, 2022): https://www.bmvg.de/de/aktuelles/bewaffnung-der-heron-tp-drohnen-mit-praezisionsmunition-5389376 (accessed May 31, 2022).

263 Nina Werkhäuser, "No armed drones for the German army — for now," Deutsche Welle, December 14, 2020: https://www.dw.com/en/no-armed-drones-for-the-german-army-for-now/a-55936615 (accessed May 31, 2022).

264 Whereas autonomous systems have the capability to act with some level of independence from human operators, the notion of unmanned systems merely refers to the lack of a physical presence of human operators (e.g., remote control).

265 See, e.g., The Federal Government, "Rede der Bundesministerin der Verteidigung, Dr. Ursula von der Leyen, in der Aktuellen Stunde zum Beschaffungsprogramm von Drohnen für die Bundeswehr vor dem Deutschen Bundestag am 2. Juli 2014 in Berlin" [July 2, 2014 question time parliamentary speech in Berlin by Federal Minister of Defence Dr. Ursula von der Leyen on the drone procurement program for the German armed forces], (July 2, 2014): https://www.bundesregierung.de/breg-de/service/bulletin/rede-der-bundesministerin-der-verteidigung-dr-ursula-von-der-leyen--793046 (accessed May 31, 2022).

12 – THE CIVILIAN-MILITARY DIVIDE IN GERMANY'S GROWING INNOVATION INSTITUTIONAL ECOSYSTEM

INSTITUTION	CREATION	FUNDING	DOMAIN	PRIORITIES
SECURITY/DEFENSE INNOVATION INSTITUTIONS				
Cyber Innovation Hub (CyberHub)	2017	€200M 2019-2023	Defense (BMVg)	Advance soldier-centered digital innovations, incl. AI and virtual reality applications; Function as interface between the Bundeswehr and the start-up ecosystem
Agency for Innovation in Cybersecurity (Cyber Agency)	2020	€350M 2020-2023	Security/Defense (BMVg & BMI)	Support ambitious and innovative R&D in the field of cybersecurity, incl. in relevant adjacent fields like human-technology interaction and AI
Digitalization and Technology Research Center of the Bundeswehr (dtec.bw)	2020	€500M 2020-2024	Defense (BMVg)	Bundle Bundeswehr research on critical and emerging technologies; Spur research cooperation with private sector, public administration, and society
CIVILIAN INNOVATION INSTITUTIONS				
Federal Agency for Disruptive Innovation (SPRIND)	2019	≈€1B 2019-2029	Civilian (BMBF & BMWK)	Support disruptive innovations, including in the fields of optical processors, micro-optics, and augemented reality
German Agency for Transfer and Innovation (DATI)	2022 (planned)	€15M initially	Civilian (BMBF)	Advance tech innovation, esp. at universities of applied sciences; Enhance cooperation with start-ups, SMEs as well as public institutions
Sovereign Tech Fund (STF)	2022 (planned)	€3.5M per annum	Civilian (BMWK, Open Knowledge Foundation)	Support open source software ecosystem; Improve security of internet base technologies; Bolster interoperability and digital sovereignty

Source: Authors' own illustration

Recent efforts to bolster competitiveness in defense technology do mark a break in the habit of creating artificial silos between military and civilian spheres. A 2020 strategy paper on the German defense industry[266] reflects increased awareness of civilian research and development (R&D) as the driver of military EDT applications.[267] Germany has also made notable investments over the past five years in new agencies tasked with catalyzing defense research and innovation (see figure 12).

Nevertheless, the divide between civilian and military R&D remains greater in Germany than in allies such as France, the United Kingdom, and the United States. The US Defense Advanced Research Projects Agency is frequently namechecked in German policy discourse, but the German government maintains a clear separation between its own emerging security and defense innovation institutions and the civilian innovation agency, SPRIND.[268] It is also telling that the federal defense ministry's support

266 The Federal Government, "Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie" [German government strategy paper on strengthening the security and defense industry], (February 2020): https://www.bmwk.de/Redaktion/DE/Downloads/S-T/strategiepapier-staerkung-sicherits-und-verteidigungsindustrie.pdf?__blob=publicationFile&v=4 (accessed May 31, 2022).

267 Notably, the paper emphasizes the strategic importance of security and defense in general technology and industrial policy, and identifies as a key challenge the transfer of (basic) R&D into procurable security and defense products.

268 SPRIND, "Get to Know SPRIND": https://www.sprind.org/en/we/ (accessed May 31, 2022).

for research at civilian universities is stagnating at around €50 million annually.[269]

Crucially, Germany's inability to harness its significant EDT R&D for defense undermines its efforts to contribute to a European defense sector prepared for the future. The debate about military EDTs at the EU level has certainly been forward-looking, but a persistent implementation gap exists. The bloc's Strategic Compass (2022),[270] initiated by the German 2020 EU Council presidency, highlights the critical importance of strengthening the joint European technology-industrial base. Still, industrial fragmentation along national lines continues to impede greater scaling of defense technology and its attendant benefits.

EU member states also fail to mobilize sufficient resources. The EU's Coordinated Annual Review on Defence (2020) warns that spending levels on defense technology are insufficient.[271] Initiatives, such as the European Defense Fund (EDF), that call for disruptive technologies are important steps to furthering high-impact defense-related research.[272] But an initial €13 billion EDF budget for 2021-2027 was slashed by almost half, to €8 billion.[273] Moreover, all but two EU member states fall short of an agreement to spend 2 percent of their defense budget on research and technology.[274]

In view of these limitations, EU coordination with NATO's multifaceted work on EDTs remains a critical component of German policy. NATO's Strategic Concept 2030 focuses on EDTs and resilience against cyber, space-based, and hybrid threats.[275] NATO defense ministers also approved last year a plan that will guide the alliance's EDT policy development in seven key areas, among them AI, autonomy, and quantum-enabled technologies.[276] And, as part of the NATO 2030 agenda, Germany and other member states are advancing a transatlantic defense technology and industrial ecosystem. They have agreed to establish a Defence Innovation Accelerator for the North Atlantic (DIANA)[277] and a NATO Innovation Fund (NIF)[278] that will invest a minimum of €1 billion over the next 15 years.[279]

Recommendations

The *Zeitenwende* must advance a reconciliation between ethical concerns and military requirements regarding EDTs if the *Bundeswehr* is to be a strong pillar of European security. This will require the German government to:

Commit 2 percent of the €100 billion *Sondervermögen* to fostering disruptive defense R&D. The German government should not forfeit the opportunity to leverage the *Sondervermögen* for shaping a future-proof defense-technological sector. Currently, even as forthcoming weapons platforms like FCAS account for a notable share of the €100 billion budget, a mere €422 million are budgeted di-

269 Funding was €42 million in 2017, €63 million in 2018, and €53 million in 2019. Armin Himmelrath, "Unis erhalten weniger Geld vom Verteidigungsministerium" [Universities receive less money from the Federal Ministry of Defence], *Spiegel Online*, June 15, 2021: https://www.spiegel.de/panorama/bildung/ruestungsforschung-unis-erhalten-weniger-geld-vom-verteidigungsministerium-a-0bec8b22-6269-4224-b620-a689b085fd43 (accessed May 31, 2022).

270 European Union External Action Service (EEAS), "A Strategic Compass for Security and Defence," (October 2021): https://eeas.europa.eu/headquarters/headquarters-homepage/106337/towards-strategic-compass_en (accessed May 31, 2022).

271 European Defense Agency, "2020 CARD Report Executive Summary," (2020), p. 7: https://eda.europa.eu/docs/default-source/reports/card-2020-executive-summary-report.pdf (accessed May 31, 2022).

272 European Defence Fund, "Research on disruptive technologies for defence," European Commission (2021): https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/edf-2021-open-rdis-open (accessed 18 July 2022).

273 European Commission, "The EU budget powering the recovery plan for Europe. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions," COM(2020) 44 final, (May 27, 2020): https://ec.europa.eu/info/sites/default/files/about_the_european_commission/eu_budget/1_en_act_part1_v9.pdf (accessed May 31, 2022).

274 European Defence Agency, "Defence Data 2019-2020. Key findings and analysis," (2021), pp. 12-13: https://eda.europa.eu/docs/default-source/brochures/eda---defence-data-report-2019-2020.pdf (accessed May 31, 2022).

275 NATO, "Strategic Concepts," (November 29, 2021): https://www.nato.int/cps/en/natohq/topics_56626.htm (accessed May 31, 2022).

276 NATO, "Emerging and disruptive technologies," (April 7, 2022): https://www.nato.int/cps/en/natohq/topics_184303.htm (accessed May 31, 2022).

277 DIANA aims to strengthen allies' cooperation on EDTs and ensure continued interoperability. It will host an accelerator program for startups, providing access to pre-qualified investors, and connect test centers in Europe and North America to co-design, validate, and test military EDT applications. NATO, "Emerging and disruptive technologies," (April 7, 2022): https://www.nato.int/cps/en/natohq/topics_184303.htm (accessed May 31, 2022).

278 NATO, "NATO Allies take the lead on the development of NATO's Innovation Fund," (October 22, 2021): https://www.nato.int/cps/en/natohq/news_187607.htm (accessed May 31, 2022).

279 Vivienne Machi, "NATO hopes to launch new defense tech accelerator by 2023," Defense News, June 22, 2021: https://www.defensenews.com/global/europe/2021/06/22/nato-hopes-to-launch-new-defense-tech-accelerator-by-2023/ (accessed May 31, 2022).

rectly for EDT R&D, specifically AI capabilities.[280] The government should commit at least 2 percent of the Sondervermögen to the fostering of disruptive defense technologies with the aim of incentivizing venture capital flows into new defense start-ups and increasing R&D spending of Germany's established defense companies.

Connect the ethical debate on military EDT applications to operational realities. High-level discussions on ethics in Germany are frequently disconnected from operational realities. Debate should focus on appropriate degrees of machine autonomy and the delimitation of justifiable purposes for the use of EDTs. Relevant efforts could include interactive workshops during which political decision-makers and/or citizens engage in high-probability scenarios that, for example, involve drone swarms. This could foster debate on possible responses, including methodologies for selecting targets when human reaction times would be too slow.

Link dual-use implications of EDTs with innovation industrial policy. Ministries leading innovation and industrial policy, especially the Federal Ministry for Digital and Transport, the Federal Ministry for Economic Affairs and Climate Action, and the Federal Ministry of Education and Research, should consult the Federal Ministry of Defence to integrate dual-use dimensions of EDTs such as AI and quantum into their strategies. The new National Security Strategy should include a section unifying technology and innovation industrial policies, including those relevant to defense, under a cross-governmental assessment of key threats to national security.

Augment knowledge transfer among military and civilian R&D. Civilian technology R&D increasingly determines military advantage. The German government should acknowledge this by expanding links between the Munich-based Digitalization and Technology Research Center of the Bundeswehr (dtec.bw) and Bavaria's high-tech startups. The government should support a separate Track II platform for innovators that facilitates discovering dual-use applications for EDTs developed with the support of innovation agencies, including SPRIND and the Cyber Innovation Hub. It should also create incentives, such as fund matching, for German and European venture capital investment in defense technology startups.

Align defense procurement with technological innovation cycles. Defense budget fluctuations stifle the ability to support lengthy EDT innovation cycles. The government should establish a dedicated fund for disruptive defense technology with annual minimum budget guarantees through 2030. The Bundestag Defence Committee should also appoint a member to report on project outcomes, foster debate on defense innovation spending, and identify opportunities for cooperation with other committees, including the Committee on Foreign Affairs and the Committee on Digital Affairs.[281]

Maintain allies' interoperability through joint principles and military formations. The German government must ensure that EDT-related transformations do not undermine interoperability with allied forces. It should promote development of common ethical principles and codes of conduct such as those defined in NATO's AI strategy. Germany should also promote binational rollouts (e.g., in the Franco-German brigade or German-Dutch corps) of experimental technologies and leverage its role as a participant in NATO's Framework Nations Concept to create test beds for military innovations in multinational formations.

280 Federal Ministry of Defence, "Ministerin: Wir sorgen für eine voll einsatzbereite Bundeswehr" [Minister: We provide for a fully operational Bundeswehr], (July 3, 2022): https://www.bmvg.de/de/aktuelles/ministerin-wir-sorgen-fuer-voll-einsatzbereite-bundeswehr-5438596 (accessed August 14, 2022).

281 For a related argument for a defense innovation and experimentation ambassador, see: Torben Schütz et al., "Beware of Potemkin: Germany's Defense Rethink Risks Reinforcing Old Habits," *War on the Rocks*, April 11, 2022: https://warontherocks.com/2022/04/beware-of-potemkin-germanys-defense-rethink-risks-reinforcing-old-habits/ (accessed May 31, 2022).

ABOUT THE PROJECT

This DGAP project proposes an integrated policy approach to German digital capacities and objectives. Such a strategy should link Germany's incumbent industrial strengths and digital governance objectives with its geopolitical aims.

This report outlines an integrated approach based on seven interdependent layers of a "technology policy stack". For this analysis, the DGAP invited 38 individuals to join a working group and participate, between July and October 2021, in seven off-the-record workshops on the crucial strategic dimensions of Germany's international digital identity. Participants included elected officials, candidates, and senior German government representatives; German political party staff responsible for platforms and coalition agreements; subject matter experts in technology and foreign policy; thought leaders and senior technology-company management; key academics, economists, and political theorists; and representatives of civil society and digital rights advocacy organizations. Additional experts were invited to take part in the workshops on an ad hoc basis. Each workshop focused on a layer in Germany's technology policy stack. Working group members were consulted intermittently during the drafting of this report.

We are grateful to the Open Society Initiative for Europe for their generous support, which made this project possible.

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 Lara Bührer, Luise Rombach

Design Concept WeDo

Cover Photo © iStock / NicoElNino

Author picture(s) © DGAP

Photos: Cover © iStock/NicoElNino;
© DGAP; p. 21 © Giu Vicente/Unsplash;
p. 33 © Michael Fousert/Unsplash;
p. 45 © IMAGO/aal.photo; p. 59 © IMAGO/
Kosecki; p. 71 © iStock/piranka;
p. 83 © IMAGO/photothek