Ethical and Operational
Emerging and Disruptive Technologies, the German Military, and the Zeitenwende
CHAPTER OVERVIEW

1. DIGITAL SOVEREIGNITY AS GERMANY’S LEITMOTIF IN A GLOBAL CONTEXT

2. ASSESSING STRENGTHS AND CHALLENGES OF GERMANY’S INNOVATION ECOSYSTEM

3. SAFEGUARDING GERMANY’S TECHNOLOGY STACK AND INNOVATION INDUSTRIAL BASE

4. SHAPING THE GLOBAL TECHNOLOGY RULE BOOK IN THE SERVICE OF EUROPE

5. OPTIMIZING EXPORT CONTROL, INVESTMENT SCREENING AND MARKET ACCESS INSTRUMENTS

6. STRENGTHENING INTERNATIONAL TECHNOLOGY ALLIANCES, PARTNERSHIPS, AND NORMS

7. EMERGING AND DISRUPTIVE TECHNOLOGIES, THE GERMAN MILITARY, AND THE ZEITENWENDE
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

---


European defense projects for forthcoming weapons platforms, including the Future Combat Air System (FCAS) with France and Spain, and the Main Ground Combat System (MGCS) 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.

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.
for digitally networked warfare.\textsuperscript{241} The Bundeswehr aims to make the BMS operational by 2023, when it assumes leadership of NATO’s Very High Readiness Joint Task Force.\textsuperscript{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.\textsuperscript{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).\textsuperscript{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.\textsuperscript{245} The lab is developing MuQuaNet, a prototype of such a network.\textsuperscript{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.\textsuperscript{247} AI also potentially incentivizes risk-taking since defensive techniques may be developed and scaled more slowly than offensive ones.\textsuperscript{248} At the same time, attributing cyberattacks is complicated and time-consuming.\textsuperscript{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).\textsuperscript{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.\textsuperscript{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.

\begin{itemize}
\item \textsuperscript{241} The BMS is based on the SiteWare software family that many NATO partners use. Bundeswehr, “Battle Management System – CIR digitalisiert” [Batttle Management System – CIR digitized], https://www.bundeswehr.de/de/organisation/zyber-und-informationsraum/suchraum/digitalisieren/ (accessed May 31, 2022).
\item \textsuperscript{242} Bundeswehr, “Digitalisierung im Heer” [Digitalization in the army], https://www.bundeswehr.de/de/organisation/heer/organisation/themen/ (accessed May 31, 2022).
\item \textsuperscript{244} Bundeswehr Cyber- und Informationsraum [Bundeswehr Cyber and Information Space], https://www.bundeswehr.de/de/organisation/zyber-und-informationsraum (accessed May 31, 2022).
\item \textsuperscript{246} University of the Bundeswehr Munich, “Q-Lab,” https://www.unibw.de/code/forschung/zentralabora/q-lab (accessed May 31, 2022).
\end{itemize}
The February 2022 Zeitenwende announcement\textsuperscript{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\textsuperscript{253} and its recent position paper (2021) on the Bundeswehr’s future\textsuperscript{254} make little reference to the disruptive potential of technologies driven primarily by civilian innovation, including AI, quantum, and 5G/6G connectivity.\textsuperscript{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)\textsuperscript{256} and Industrial Strategy 2030 (2019)\textsuperscript{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)\textsuperscript{258} and 5G strategy (2017).\textsuperscript{259} Germany’s cyber strategy (2021)\textsuperscript{260} sees cybersecurity primarily through the civilian lens of law enforcement and the judiciary.\textsuperscript{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,\textsuperscript{262} the German government put an end to an almost decade-long discussion\textsuperscript{263} that frequently conflated notions of unmanned and autonomous systems.\textsuperscript{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.\textsuperscript{265}


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.


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


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).

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 reflects increased awareness of civilian research and development (R&D) as the driver of military EDT applications. 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. In 2019, Germany announced the Federal Agency for Disruptive Innovation (SPRIND) with an initial budget of €1 billion, aiming to support disruptive innovations, including in the fields of optical processors, micro-optics, and augmented reality.

### Security/Defense Innovation Institutions

<table>
<thead>
<tr>
<th>INSTITUTION</th>
<th>CREATION</th>
<th>FUNDING</th>
<th>DOMAIN</th>
<th>PRIORITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Innovation Hub (CyberHub)</td>
<td>2017</td>
<td>€200M 2019-2023</td>
<td>Defense (BMVg)</td>
<td>Advance soldier-centered digital innovations, incl. AI and virtual reality applications; Function as interface between the Bundeswehr and the start-up ecosystem</td>
</tr>
<tr>
<td>Agency for Innovation in Cybersecurity (Cyber Agency)</td>
<td>2020</td>
<td>€350M 2020-2023</td>
<td>Security/Defense (BMVg &amp; BMI)</td>
<td>Support ambitious and innovative R&amp;D in the field of cybersecurity, incl. in relevant adjacent fields like human-technology interaction and AI</td>
</tr>
<tr>
<td>Digitalization and Technology Research Center of the Bundeswehr (dtec.bw)</td>
<td>2020</td>
<td>€500M 2020-2024</td>
<td>Defense (BMVg)</td>
<td>Bundle Bundeswehr research on critical and emerging technologies; Spur research cooperation with private sector, public administration, and society</td>
</tr>
</tbody>
</table>

### Civilian Innovation Institutions

<table>
<thead>
<tr>
<th>INSTITUTION</th>
<th>CREATION</th>
<th>FUNDING</th>
<th>DOMAIN</th>
<th>PRIORITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Agency for Disruptive Innovation (SPRIND)</td>
<td>2019</td>
<td>≈€1B 2019-2029</td>
<td>Civilian (BMBF &amp; BMWK)</td>
<td>Support disruptive innovations, including in the fields of optical processors, micro-optics, and augmented reality</td>
</tr>
<tr>
<td>German Agency for Transfer and Innovation (DATI)</td>
<td>2022 (planned)</td>
<td>€15M initially</td>
<td>Civilian (BMBF)</td>
<td>Advance tech innovation, esp. at universities of applied sciences; Enhance cooperation with start-ups, SMEs as well as public institutions</td>
</tr>
<tr>
<td>Sovereign Tech Fund (STF)</td>
<td>2022 (planned)</td>
<td>€3.5M per annum</td>
<td>Civilian (BMWK, Open Knowledge Foundation)</td>
<td>Support open source software ecosystem; Improve security of internet base technologies; Bolster interoperability and digital sovereignty</td>
</tr>
</tbody>
</table>

Source: Authors’ own illustration

---


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.

for research at civilian universities is stagnating at around €50 million annually.\footnote{Funding was €42 million in 2017, €63 million in 2018, and €53 million in 2019. Armin Himmelrath, “Unis erhalten weniger Geld vom Verteidigungsmministerium” [Universities receive less money from the Federal Ministry of Defence], Spiegel Online, June 15, 2021: https://www.spiegel.de/panorama/bildung/questungsforschung-unis-erhalten-weniger-geld-vom-verteidigungsmministerium-a-695620-669b856543 (accessed May 31, 2022).}

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),\footnote{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).} 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.


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.\footnote{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).} 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.\footnote{NA TO, “Emerging and disruptive technologies,” (April 7, 2022): https://www.nato.int/cps/en/natohq/news_187607.htm (accessed May 31, 2022).} 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)\footnote{NA TO, “Strategic Concepts,” (November 29, 2021): https://www.nato.int/cps/en/natohq/topics_56626.htm (accessed May 31, 2022).} and a NATO Innovation Fund (NIF)\footnote{NA TO, “Sondervermögen” [German Defense Innovation Accounts] (November 3, 2021): https://www.nato.int/cps/en/natohq/topics_184303.htm (accessed May 31, 2022).} that will invest a minimum of €1 billion over the next 15 years.\footnote{NA TO Allies take the lead on the development of NATO’s Innovation Fund,” (October 22, 2021): https://www.nato.int/cps/en/natohq/news_184303.htm (accessed May 31, 2022).}

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-
rectly for EDT R&D, specifically AI capabilities.\textsuperscript{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 (dtoc.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.\textsuperscript{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.

---


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

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

Publisher
Deutsche Gesellschaft für Auswärtige Politik e.V.

ISSN 2198-5936

Editing Andrew Cohen

Layout Luise Rombach

Design Concept WeDo

Author picture(s) © DGAP

Cover Photo © IMAGO / photothek

This work is licensed under a Creative Commons Attribution – NonCommercial – NoDerivatives 4.0 International License.