October 2022

DGAP REPORT

Ethical and Operational

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

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

Tyson Barker
Head, Technology and
Global Affairs Program

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.[1] Indeed, highly automated unmanned aerial systems (UAS) were significant assets in recent conflicts such as that in Nagorno-Karabakh.[2] 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.[3]

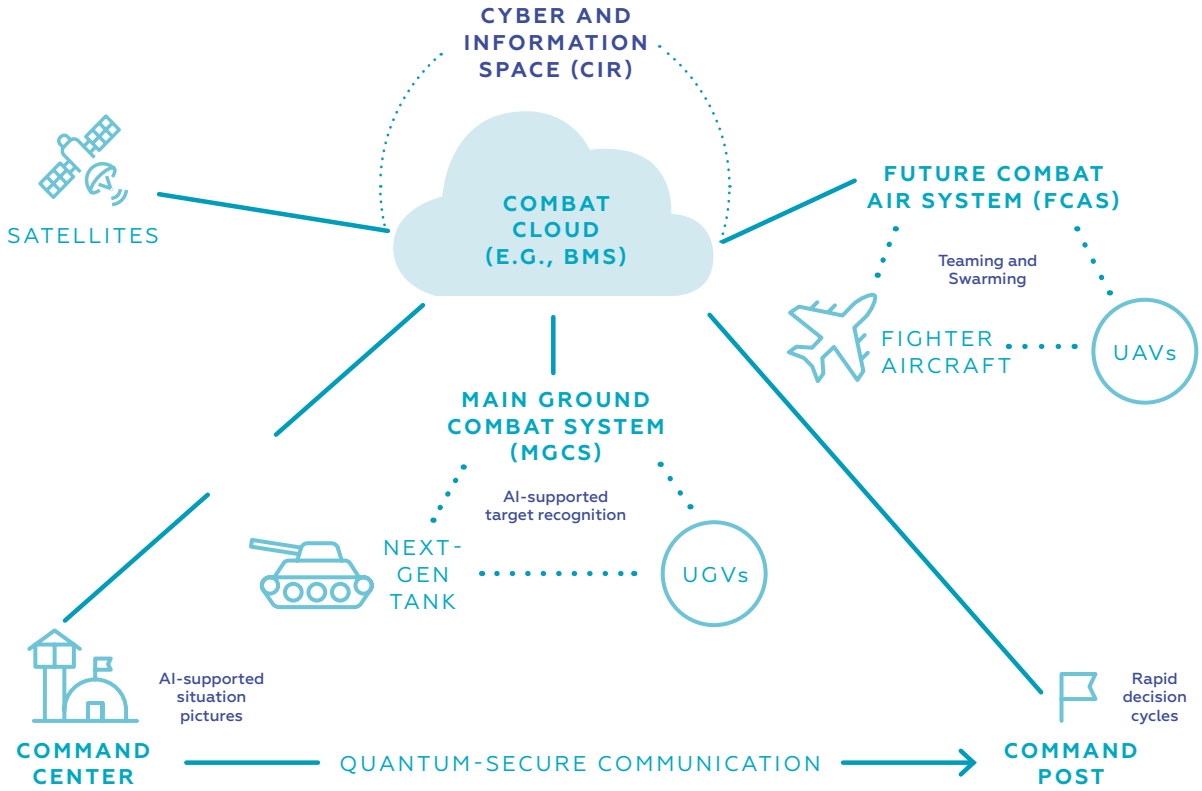
Crucially, in this changing environment, the *Bundeswehr*'s ability to harness EDTs for future operational effectiveness depends on close cooperation with EU and NATO allies and, therefore, sustained political capital spent on joint initiatives. Germany's current efforts to marshal EDTs are closely tied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

1 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).

2 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).

3 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).

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



Source: Authors' illustration

ropean defense projects for forthcoming weapons platforms, including the Future Combat Air System (FCAS)[4] with France and Spain, and the Main Ground Combat System (MGCS)[5] 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.[6]

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.[7] The *Bundeswehr* aims to make the BMS operational by 2023, when it assumes leadership of NATO's Very High Readiness Joint Task Force.[8]

4 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).

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

6 "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).

7 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).

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

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.[9] 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).[10] 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.[11] The lab is developing MuQuaNet, a prototype of such a network.[12]

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.[13] AI also potentially incentivizes risk-taking since defensive techniques may be developed and scaled more slowly than offensive ones.[14] At the same time, attributing cyberattacks is complicated and time-consuming.[15] 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).[16] 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.[17] 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.

The Current Policy Approach

The February 2022 *Zeitenwende* announcement[18] 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

9 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).

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

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

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

13 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).

14 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).

15 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).

16 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).

17 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).

18 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).

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[19] and its recent position paper (2021) on the Bundeswehr's future[20] make little reference to the disruptive potential of technologies driven primarily by civilian innovation, including AI, quantum, and 5G/6G connectivity.[21]

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)[22] and Industrial Strategy 2030 (2019)[23] 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)[24] and 5G strategy (2017).[25] Germany's cyber strategy (2021)[26] sees cybersecurity primarily through the civilian lens of law enforcement and the judiciary.[27]

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,[28] the German government put an end to an almost decade-long discussion[29] that frequently conflated notions of unmanned and autonomous systems.[30] 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.[31]

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[32] reflects increased awareness of civilian research and development (R&D) as the driver of military EDT applications.[33] Germany has also made notable investments over the past five years in new agencies tasked with catalyzing defense research and innovation (see figure 2).

19 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).

20 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).

21 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.

22 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).

23 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).

24 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).

25 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).

26 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).

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

28 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).

29 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).

30 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).

31 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).

32 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).

33 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.

2 – 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

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.[34] It is also telling that the federal defense ministry's support for research at civilian universities is stagnating at around €50 million annually.[35]

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),[36] initiated by the German 2020 EU

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

35 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).

36 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).

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.[37] Initiatives, such as the European Defense Fund (EDF), that call for disruptive technologies are important steps to furthering high-impact defense-related research.[38] But an initial €13 billion EDF budget for 2021-2027 was slashed by almost half, to €8 billion.[39] Moreover, all but two EU member states fall short of an agreement to spend 2 percent of their defense budget on research and technology.[40]

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.[41] 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.[42] 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)[43] and a NATO Innovation Fund (NIF)[44] that will invest a minimum of €1 billion over the next 15 years.[45]

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 directly for EDT R&D, specifically AI capabilities.[46] 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

37 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).

38 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).

39 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).

40 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).

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

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

43 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).

44 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).

45 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).

46 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).

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.[47]

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.

47 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).

DGAP

Advancing foreign policy. Since 1955.

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

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

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

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Editing Andrew Cohen

Layout Luise Rombach

Design Concept WeDo

Author picture(s) © DGAP

Cover Photo © IMAGO / photothek