DAIO Defense AI Observatory

Master and Servant

Defense AI in Germany

Heiko Borchert, Torben Schütz, Joseph Verbovszky

DAIO Study 23|12

Ein Projekt im Rahmen von

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

About the Defense AI Observatory

The Defense AI Observatory (DAIO) at the Helmut Schmidt University in Hamburg monitors and analyzes the use of artificial intelligence by armed forces. DAIO comprises three interrelated work streams:

- Culture, concept development, and organizational transformation in the context of military innovation
- Current and future conflict pictures, conflict dynamics, and operational experience, especially related to the use of emerging technologies
- Defense industrial dynamics with a particular focus on the impact of emerging technologies on the nature and character of techno-industrial ecosystems

DAIO is an integral element of GhostPlay, a capability and technology development project for concept-driven and AI-enhanced defense decision-making in support of fast-paced defense operations. GhostPlay is funded by the Center for Digital and Technology Research of the German Bundeswehr (dtec.bw). dtec.bw is funded by the European Union – NextGenerationEU.

Ein Projekt im Rahmen von

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union NextGenerationEU

Master and Servant

Defense AI in Germany

Heiko Borchert, Torben Schütz, Joseph Verbovszky

DAIO Study 23|12

Ein Projekt im Rahmen von

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

About the Authors
Dr. Heiko Borchert is DAIO's co-director. He is Associate Fellow at the Center for Advanced Security, Strategic and Integration Studies (CASSIS, Bonn), subject matter expert at the Hague Center for Strategic Studies, and runs a strategic affairs consulting boutique. He studied international relations, business administration, economics, and law at the University of St. Gallen, where he also got his Ph.D. His Twitter account is @HeikoBorchert.

Torben Schütz is a PhD candidate at the Helmut-Schmidt-University and Associate Fellow at the German Council on Foreign Relations (DGAP). As a DAIO Research Fellow, he oversees the team's work on conflict pictures and conflict dynamics. Torben Schütz has worked for the German Council on Foreign Relations and the Stiftung Wissenschaft und Politik/German Institute for International and Security Affairs. He holds a master's degree in political science from Leibniz University Hannover. His Twitter account is @_schuetzt.

Joseph Verbovszky is DAIO's Research Fellow for defense technology-industrial affairs. Before joining DAIO, he worked in the areas of international coordination and strategic analysis at different defense companies. He holds a master's degree in international relations and economics from the Johns Hopkins School of Advanced International Studies (SAIS). He graduated with a PhD on German Structural Pacifism from the University of the Bundeswehr München. His Twitter account is @warkhorse.

Acknowledgments
For this study we have conducted interviews with more than a dozen high-ranking Bundeswehr and industry experts, who remain anonymous. We are immensely grateful for their insights and suggestions, but remain solely responsible for any errors in fact, analysis, or omission.

Design
Almasy Information Design Thinking

Imprint
Heiko Borchert, Torben Schütz, and Joseph Verbovszky, Master and Servant. Defense AI in Germany. DAIO Study 23/12 (Hamburg: Defense AI Observatory, 2023).

Defense AI Observatory | Chair of Political Theory | Helmut Schmidt University
Holstenhofweg 85 | 22043 Hamburg | T +49 40 6541 2776
www.defenseai.eu | contact@defenseai.eu | @Defense_AIO

ISSN (online): 2749–5337
ISSN (print): 2749–5345

Content

1 Summary

The German Ministry of Defense (MoD), the Bundeswehr, and the defense technology and industrial base understand the importance of artificial intelligence (AI) in shaping the contours of the future strategic environment and the use of military power. Since the late 1990s, this defense ecosystem has been in a continuous process of transformation that reflects changes in the geostrategic landscape, is influenced by technological advances, and shaped by socio-political requirements. However, arguing that the Bundeswehr must change is often easier than defining how it needs to change and what goal the change is meant to achieve.

This is the context that shapes Germany's approach to defense AI. Numerous projects have been launched, structures and processes are being reorganized, money has been earmarked, and training is underway or being readjusted. Overall, however, the path ahead remains murky – with the obvious risk that action remains without traction. Like other organizations that embark on a whole-scale transformation process, the German defense establishment struggles to link the envisioned future with the status quo and is thus caught in a "master and servant" logic that will be painful to overcome.

First, the metaphor describes the struggle to readjust Germany's strategic culture amid war in Europe. Germany's strategic culture is input-driven. Socio-political acceptance of military power trumps everything. This prevailing attitude is best illustrated by the idea that defense AI serves "humanitarian precision," as one interview partner put it: accelerating defense decision-making serves the purpose of a value-conscious "citizen in uniform" – otherwise the Bundeswehr would not be considered a legitimate instrument of power providing decision-makers political options.

Second, defense trumps offense with most of the current defense AI studies, concepts, and projects aiming at augmenting the survivability rather than the lethality of the Bundeswehr. In this regard, the use of force is repackaged as the "sharp end of digitalization" while the overall defense administration remains geared towards peace-time tasks rather than the return of the use of force in Europe. Therefore, the Bundeswehr operates in a bifurcated world: the armed forces need to envision the future defense environment while procrastinating future concepts and projects into today's procedures and processes – the master – to induce incremental change.

Third, three decades of political neglect have served as a particularly cruel master when it comes to innovation. German armed forces preoccupied with the need

to survive – politically, rather than militarily – simply did not have the strategic bandwidth to consider the added value of technology beyond the primary goal of ensuring basic military functions. The "tyranny of the status quo" has pinned socio-technological imaginaries to what matters here and now. Force planners could (and would) not request, what they did not know. This triggered a kind of technology blindness that has – unintentionally – been reinforced by a technology agnostic approach to capability development that describes capability requirements in generic terms. The extent to which synchronizing concepts and technology development can ignite leapfrogs in capability development thus remains underexploited.

Against this background defense AI is seen as a tool – the humble servant – subordinate to human will power and decision-making. The belief that humans must always remain in the loop dominates political discourse and structures the debate on ethics and defense AI. As a result, Germany adopts a "non-intrusive" onboarding process to incrementally add AI elements to large defense development and procurement projects. This makes it difficult to assess what defense AI is all about and whether it delivers what is expected.

Simultaneously, Germany's defense AI thinking is heavily influenced by US ideas. The need for AI to succeed in a "hyperwar environment," increasing reference to multi-domain operations, and the adoption of different combat cloud concepts can be traced back to US concepts that influence thinking in NATO. Germany's "administrative gold-plating," however, implies that the US emphasis on performance and lethality is being tamed and made palatable for a German defense audience that is risk averse. Consequently, defense AI is mainly understood as a capability multiplier that improves the efficiency and effectiveness of existing military processes.

This sets the framework for numerous projects that explore the benefits and risks of defense AI. Along Germany's capability value chain – consisting of Command, Control, Computers, Communications or C4 (Führung), Intelligence, Surveillance and Reconnaissance or ISR (Aufklärung), precision effects (Wirkung), and support (Unterstützung) – most of the current defense AI projects focus on C4 and ISR. Projects focusing on providing recognized operational pictures at joint and services levels are (politically) more palatable than exploring the benefits of defense AI for precision effects. Given the clear hierarchy between men and AI, the focus is on decision-making support and step-by-step improvement of existing technologies with the help of AI.

In this context, governance plays a major role. A great deal of attention is being devoted to adapting today's structures for a digital world with the MoD and the military services operating at different levels of ambition and diverging speed. This creates risks for Bundeswehr jointness as existing mechanisms for synchronization seem weak or are not yet fully used to implement proper strategic guidance. Whether the new defense AI implementation strategy, that is expected by then end of 2023, can alleviate the situation, remains to be seen.

Apart from providing basic funding to key defense research and technology (R&T) organizations, most of Germany's defense R&T projects are tied to ongoing procurement projects. Thus, it is very difficult to assess the level of defense AI-related funding. While the more than €400M that the new five-year Sondervermögen has earmarked for R&T and AI may seem substantial, this amount also includes investments in related digital infrastructure. Based on an analysis of the non-public budgets of various current development projects, we contend that Germany currently spends around €50M per year on AI-related software development.

The true status of the Bundeswehr's fielding and operating of defense AI is difficult to grasp. An open-source intelligence system for crisis early warning that uses AI for data analytics and predictive analysis is one of the most prominent current examples. Other examples include AI-based radar warning receivers to protect Bundeswehr helicopters, intelligent image processing for missiles, and enterprise applications in the fields of warehouse management or medical services.

Using AI in the defense environment also affects military education and training. The Bundeswehr's Command and Staff College (Führungsakademie der Bundeswehr) is about to review its curriculum with the goal to incorporate AI elements as of 2024. In addition, the University of the Bundeswehr/Hamburg is setting up a new AI bachelor's and master's degree course. Individual services also explore opportunities for AI-enhanced simulation-based training. Moreover, different initiatives have been launched to train defense AI algorithms.

In sum, Germany has embarked on a defense AI journey. Individual projects have been started, but substantial homework remains to be done. This includes, first, the need to be more precise about the contribution AI is expected to make in achieving future capability growth. Second, Germany's – currently non-existent – defense industrial policy needs to be updated with regard to defense AI. Third, the German MoD needs to be more outspoken about its international defense AI ambition. Finally, more thought needs to be given on how to create a framework to certify, qualify, and approve future defense AI solutions.

2 Thinking About Defense AI

The 2018 artificial intelligence (AI) strategy of the German government describes how Germany wants to use AI to advance national and European competitiveness. Technological advances and global changes, the need to understand AI as a "key enabling technology", as well as the "democratic desire to anchor such a far-reaching technology (…) in an ethical, legal, cultural and institutional context" are the pillars driving the federal governments AI policy.[1] The strategy differentiates between "strong" and "weak" AI and interprets the latter as "solution(s) of specific problems using methods from mathematics and computer science, whereby the systems developed are capable of self-optimisation" with a focus on the use of this type of AI in deduction systems, knowledge-based systems, pattern analysis and pattern recognition, robotics and autonomous systems as well as smart multimodal human-machine interaction.[2] The 2020 update of the German AI strategy extends previous lines of effort on building human capacities, establishing research structures, advancing research and transfer structures, creating an appropriate regulatory framework, and supporting networking.[3]

The German AI strategy and its update remain silent on the use of AI for defense and security. The same is true for the 2018 Concept of the Bundeswehr,[4] the 2021 strategic guidance of then Minister of Defense Kramp-Karrenbauer, and the 2021 coalition treaty. Only the 2019 concept paper on "AI for use in the area of responsibility of the Ministry of Defense" fills the void. This fact is disenchanting, but it is not surprising.

The country's strategic culture tames the Bundeswehr's technology appetite. This creates tensions. The Bundeswehr recognizes that technology is changing the future battlefield. It also embraces allied concept ideas to signal its willingness to cooperate with partners. However, culture, the current organizational set up, and the lack of robust technology leadership pin the Bundeswehr down to the status quo. In this context defense AI has a hard time blossoming. Rather the focus is on incremental evolution most often tied to large procurement projects that apply defense AI as part of broader functionalities. This makes it difficult to understand Germany's overall defense AI ambition and the added value AI is expected to deliver for the German Bundeswehr.

1 Artificial Intelligence Strategy, p. 4.
2 Ibid., pp. 4–5
3 Artificial Intelligence Strategy of the German Federal Government. 2020 Update.
4 This document only refers to AI in relation to data mining and data analytics. See: Konzeption der Bundeswehr, footnote 48.

2.1 Structural Pacifism Shapes Defense Technological Imaginaries

Germany's security policy is characterized by a structural pacifism[5] in which the need to reconcile competing elements of Germany's post-war security identity with a byzantine policy process leads to the prioritization of security policy conformity over effectiveness (performance).

Resulting from the trauma of WWII, the nascent Federal Republic of West Germany "reinvented itself" in opposition to its authoritarian past.[6] The formation of Germany's post-war identity relied heavily on fantasy[7] – a narrative scenario that promises the impossible fulfillment of a complete identity – and, more importantly, on negative contingency – the projection of catastrophe into the future, which is meant to be avoided. In his seminal work on the history of the Federal Republic, Frank Biess demonstrates how negative contingency in the form of German Angst served to stabilize German democracy by emphasizing its fragility.[8]

While conducive to internal stability, negative contingency retards German security policy. It appears primarily in the form of "The Lessons of History," such as "Never Again War," "Never Again Alone" and "Never Again Auschwitz," which prescribe modes of behavior that prevent a return of German authoritarianism and preserve post-war Germany's non-belligerent identity. Unfortunately, the "Lessons of History" are often contradictory and open to interpretation, leading to uncertainty over the best way forward. Reconciling them therefore presents itself as the "right way" to do security policy, i.e., most conform with Germany's identity.[9]

Reconciling competing interpretations of German post-war identity is made more difficult by the byzantine logic of German security policy decision-making. Myriad actors are involved in the decision-making process, all of whom come with their own domestic political interests. The most relevant interests include those of the Chancellery, the Foreign Office, the Defense Ministry, the Ministry of Economics, the Ministry of Finance, and the Ministry of Development; the interests of the coalition parties and, finally, the interests of small parliamentary groups within parties or individuals who can gather enough support to form blocking minorities on a given issue.[10] Decisions over the use of force, specifically deployment and

5 Verbovszky, German Structural Pacifism.
6 Stengel, The Politics of Military Force, p. 102.
7 Eberle, Discourse and Affect in Foreign Policy, p. 46.
8 Biess, Frank, Republik der Angst, p. 31.
9 Verbovszky, Structural Pacifism, p. 29.
10 Ibid., p. 35.

the annual defense budget, are managed by completely separate decision processes, with deployment lead primarily by the foreign office and the budget by the finance ministry and finance committee.[11] Furthermore, the defense budget is constitutionally allocated out of the annual budget, subjecting it to further domestic political interests.[12] As a result, force planning (budget) at the political level lags behind operations and their requirements.[13]

The need to resolve myriad domestic political interests in a way that conforms with Germany's post-war non-belligerent identity leads to a security policy dominated by inputs. Security policy decision are done via "reverse consensus," i.e., even before going into respective committees for deliberation they are designed to be consensus-capable in the final vote.[14] The prioritization of this "right way" to do security policy leads to a highly conformist policy, which is, at best, inconsistently effective.

Beyond the scope of security policy, elements similar to structural pacifism are also observable in other aspects of German society, in particular, Germany's skepticism toward technological change. One powerful tool for measuring the impact of cultural and political factors is the use of socio-technological imaginaries, i.e., "collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology."[15] They "play an important role in the development, assessment and regulation of cutting-edge technologies."[16] This approach has already been applied to demonstrate Germany's attitudes toward developments in the fields of nanotechnology[17] and space technology.[18]

Common themes emerge across these diverse fields and the afore-presented national AI strategy: both nanotechnology and AI are seen as crucial technologies to retain a competitive economic advantage and preserve Germany's wealth,[19] while both nanotechnology and space technology are viewed as advantageous to analyze and improve the environment.[20] In none of the three technology fields do military applications receive any particular attention. Additionally, risks within the respective technology fields are prominently covered and preemptive regulation is

11 Ibid., p. 30.
12 Art. 87a, para. 1 Grundgesetz.
13 Verbovszky, Structural Pacifism, p. 204.
14 Ibid., p. 38.
15 Jasanoff, "Future Imperfect," p. 4.
16 Burri, "Imaginaries of Science and Society," p. 233.
17 Ibid.
18 Kober/Schütz, Den Weltraum ordnen – Zukunftsvorstellungen und (New) Space Governance."
19 Burri, "Imaginaries of Science and Society," p. 237; Artificial Intelligence Strategy, p. 8
20 Burri, "Imaginaries of Science and Society," p. 237, Kober/Schütz, "Den Weltraum ordnen."

at the forefront of political action: from space debris[21] to risks of nanotechnology in food or cosmetics[22] to ever-present warnings about defense AI in the German discourse.[23] Lastly, at least in the cases of nanotechnology and AI, the government wants to establish a discourse with the wider public. However, the fact that this discourse needs to be framed from the outset in terms of negative contingencies significantly limits opportunities to step out of the existing narrative or to break new ground.

2.2 Future Conflict Picture

Strategic culture shapes how the Bundeswehr thinks about the future. Its capstone document Future Operating Environment 2035 discusses the likely future battlefield.[24] Fast-paced adversarial action and the amalgamation of different forms of conflicts that evolve in complex and chaotic environments are considered a key characteristic. Advances in technology, international power shifts, new forms of decentralized organization, and the long-term consequences of climate change on the battlefield are key drivers shaping the future battlefield.

Considering these developments, future military action needs to put more emphasis on accelerating data gathering, analysis, and application, requires a comprehensive recognized operational picture, depends on shorter sensor to shooter cycles, and demands more flexible and partially automated measures of response. Strategic depth and delivering effects at greater distance become more important and should go hand in hand with developing counter-Anti Access/Area Denial (A2AD) capabilities and capacities.

Technologies play a major role in shaping these trends and implementing effective battlefield solutions.[25] Digitalization and automation are important, the paper argues. AI and unmanned systems are getting more critical in view of automating processes and operating in risk-prone areas. More emphasis is needed on superior sensing capabilities, new weapon systems as well as directed energy weapons primarily for defensive purposes. New concepts of deterrence will be needed to counter adversarial hypersonic weapons.

21 Kober/Schütz, "Den Weltraum ordnen."
22 Burri, "Imaginaries of Science and Society," p. 239.
23 See for example: Mehr Fortschritt wagen, p. 145.
24 Future Operating Environment 2023, pp. 7–11.
25 See also: Krieg der Zukunft.

The 2022 Operational Guidance for the Armed Forces by the Chief of Defense (CHOD) underpins these reflections.[26] This capstone document highlights the need for new innovative solutions to be "battle ready" and emphasizes the pressing need to assess sensor data "on the edge" to counter adversarial jamming.[27] In particular, this guideline posits:

> In addition to modern sensors as well as C2 and precision effects, the network infrastructure – i.e., the ability to transmit data, store it and make it available and usable for planning and decision-making processes of all kinds – will be decisive in the future. The interoperability of data clouds is a prerequisite for future systems. AI will play an increasingly important role, linking all fields of technology and thus also having military relevance. AI applications that support data correlation and data processing on behalf of the Commander and his command aides will become increasingly relevant. Since it is likely that adversaries will exploit these technological capabilities, it is imperative to participate in these developments.[28]

In this context, the Operational Guidance also fully embraces the idea of Multi-Domain Operations (MDO) and adopts the current working definition of NATO.[29] Furthermore the capstone document contends that the core idea driving MDO is not new. But today's focus provides opportunities to link capabilities across domains, advance operational tempo, and impose dilemmas on the adversary by precise direct and indirect effects.[30] Therefore the MoD's Directorate-General for Planning has tasked the Planning Office of the Bundeswehr at the end of 2022 to start national MDO implementation with the goal of submitting a respective document to the CHOD by mid-2024.[31]

26 Operative Leitlinien für die Streitkräfte (OpLLSK).
27 Ibid. Para. 297–298.
28 "Neben modernen Sensoren sowie Führungs- und Wirkmitteln wird künftig die Netzwerkinfrastruktur, d.h. die Befähigung, Daten zu übertragen, sie zu speichern und für Planungs- und Entscheidungsprozesse aller Art verfüg- und nutzbar zu machen, entscheidend sein. Die Interoperabilität solcher Datenclouds ist Voraussetzung für künftige Systeme. KI wird dabei zunehmend eine, alle Technologiefelder verbindende Rolle spielen und damit auch militärisch relevant. KI-Anwendungen, die den (Truppenführer) und seine Führungsgehilfen bei der Korrelation und Verarbeitung der Massendaten unterstützen, werden zunehmend relevanter. Da anzunehmen ist, dass gegnerische Akteure ihre technologischen Möglichkeiten ausschöpfen werden, kommt es zwingend darauf an, an diesen Entwicklungen teilzuhaben." See: Ibid, para. 295.
29 "Orchestration of military activities across all domain and environments, synchronized with non-military, to enable the Alliance to deliver converging effects at the speed of relevance." See: Ibid, para. 286.
30 Ibid., para. 290.
31 Interview, 28 February 2023.

2.3 Digitalization and Software-Defined Defense

The need to digitize armed forces put forward by the CHOD's Strategic Guidance is not new. In fact, Network-Centric Warfare or Network-Enabled Operations, the state-of-the art military concepts in the early 2000s, strived on the idea of transferring private industry success in digitizing enterprise processes into the military domain. As Antoine Bousque argues, the focus on international crisis management and counter insurgency put this approach to a hard reality test, which ended badly and led its temporary demise.[32] The resurgence of military peer-to-peer conflicts, the growing emphasis on MDO, and attempts to distribute military capabilities among manned and unmanned platforms and binding them together via a digital lifeline has rejuvenated defense digitalization.

The German MoD's current Strategic Guideline on Digitalization is right in arguing that the Bundeswehr's unique selling proposition lies in preparing and using armed forces. In doing so, Network-Enabled Operations and the ability to contribute to MDO are key. That's why a seamless and powerful ICT federation is indispensable.[33] Therefore, defense digitalization makes the armed force more assertive, increases the Bundeswehr's operational capability as a whole and on the digitized battlefield, and supports administrative action.[34]

As of recently, the emphasis on digitalization has boosted software-defined defense as a new concept. This concept rests on detaching the hardware aspects of military capabilities from the software aspects with the goal to connect the latter in "data-centric, multi-modal, multi-domain, adaptative battle networks."[35] Gen Michael Vetter, the MoD's Chief Information Officer, backs software-defined defense as a new way of ensuring future capability growth by "digitally upgrading" legacy systems. For example, he refers to Ukraine's use of a self-developed app to enhance the target assignation process of the Panzerhaubitze 2000 as a representative use case that illustrates how digital solutions enable Ukrainians to quickly engage the adversary and change position after firing without being targeted by the adversary.[36]

32 Bousquet, The Scientific Way of Warfare, pp. 199–219.
33 Strategische Leitlinie Digitalisierung, p. 7.
34 Färber, "Digitalisierung der Bundeswehr," p. 225.
35 Soare/Singh/Nouwens, Software-defined Defence, p. 2.
36 Audio statement by Gen Michael Vetter, published via Welchering, "Von der Bundeswehr zur digitalen Verteidigungsarmee?"

This understanding also underpins the MoD's 2021 data strategy.[37] The Bundeswehr joins the chorus of many other armed forces in EU/NATO nations[38] and calls data "an asset of significant value" that enables information and effects superiority.[39] That's why the data strategy is geared towards providing data of high quality and accessibility to strengthen the mission-readiness and resilience of IT and weapon systems, reduce life-cycle costs of IT and weapon systems, boost the use of data across the Bundeswehr, increase the use of data, and enable data analytics.[40]

The challenge, however, rests in synchronizing reality with the Bundeswehr's digital ambition. Today, the Bundeswehr effectively operates in two worlds – old and new – requiring soldiers to envision the future while procrastinating future concepts and projects into legacy procedures and processes as the only means available to induce incremental change. This creates obvious tensions between "feelgood" digitalization, operated to convey the image of a techno-savvy and thus also attractive employer, and defense digitalization meant to meet the Bundeswehr's operational performance requirements.[41]

2.4 Defense AI

Joint Thinking

Defense digitalization provides the umbrella for defense AI. The 2019 concept paper on "AI for use in the area of responsibility of the Ministry of Defense" discussed above is Germany's current defense AI capstone document. Although other concept papers refer to defense AI, this paper discusses in detail the general goals of using defense AI, the operationalization for the Bundeswehr as well as the requirements (e.g., organization, human resources, legal aspects, IT hard/software aspects) to be met. In doing so the paper follows the data-centric approach outlined above, for example, when arguing right at the start that "the successful use of AI by the Bundeswehr depends on the quantity and quality of the data used to enhance learning."[42] The document applies a very generic definition of

37 Datenstrategie GB BMVg.
38 Layton, Evolution not Revolution, p. 10; Payne, Bright Prospects – Big Challenges, pp. 10–11; Kahn, Risky Incrementalism, pp. 13–15; Engen, When the Teeth Eat the Tail, pp. 14, 16.
39 Datenstrategie GB BMVg, para. 106, 102.
40 Ibid., para. 206.
41 Interviews, 25 March 2022 and 6 February 2023.
42 "Der Erfolg des Einsatzes von KI in der Bundeswehr steht dabei im direkten Zusammenhang mit der Quantität und Qualität der Daten, mit denen diese lernt bzw. umgeht." See: Künstliche Intelligenz. Nutzung im Geschäftsbereich es Bundesministeriums der Verteidigung, p. 2.

> AI as a technology that uses machines with sophisticated algorithms taking on tasks that require – some sort of – intelligence to accomplish tasks that have previously required primarily or exclusively human decision-making or action.[43]

The concept document builds on the national AI strategy's differentiation between weak and strong AI and argues that strong AI "could lead to the development of autonomous weapon systems that individually set their respective goals of action and thus operate with maximum freedom of maneuver."[44] Germany, however, rejects the use of lethal autonomous weapon systems (see section 2.5).

Picking up the weak vs strong AI distinction might serve to align defense AI thinking with the national AI strategy, but doubts remain that it will add value in the defense context. First, this understanding focuses more on the socio-political acceptability rather than the performance and the impact of defense AI. Second, this dichotomy builds on commercial practices that strive on abundant, largely unrestricted, and readily available data. Such a data-centric approach, although prevalent in the German MoD and across the international defense establishment, is problematic given the lack of defense-relevant data. It also reinforces an IT-centric understanding of defense AI with a prime focus on the hardware infrastructure needed to process data. By contrast, the US Defense Advanced Research Projects Agency (DARPA) advocates a more nuanced approach based on three waves of AI (Box 1), a differentiation that could be used to describe in detail what type of defense AI is needed to achieve what type of capability growth.[45]

Box 1: Three Waves of AI According to DARPA

"Early work in AI emphasized handcrafted knowledge, and computer scientists constructed so-called expert systems that captured the specialized knowledge of experts in rules that the system could then apply to situations of interest. Such **"first wave" AI technologies** were quite successful – tax preparation software is a good example of an expert system – but the need to handcraft rules is costly and time-consuming and therefore limits the applicability of rules-based AI.

43 "Technologie (...) bei der Maschinen mit hochentwickelten Algorithmen Aufgaben übernehmen, für deren Bewältigung eine - wie auch immer geartete - Intelligenz notwendig ist und die bisher vor allem oder ausschliesslich menschlicher Entscheidungsfindung oder Handlung bedurfte." Ibid., p. 6.

44 Ibid., pp. 8–9.

45 This notion is also gaining prominence in NATO with the most recent science and technology trends report making explicit reference to it. See: Science & Technology Trends 2023–2043. Volume 2, pp. 27–28.

The past few years have seen an explosion of interest in a sub-field of AI dubbed machine learning that applies statistical and probabilistic methods to large data sets to create generalized representations that can be applied to future samples. Foremost among these approaches are deep learning (artificial) neural networks that can be trained to perform a variety of classification and prediction tasks when adequate historical data is available. Therein lies the rub, however, as the task of collecting, labelling, and vetting data on which to train such **"second wave" AI techniques** is prohibitively costly and time-consuming.

DARPA envisions a future in which machines are more than just tools that execute human-programmed rules or generalize from human-curated data sets. Rather, the machines DARPA envisions will function more as colleagues than as tools. Towards this end, DARPA research and development in human-machine symbiosis sets a goal to partner with machines. Enabling computing systems in this manner is of critical importance because sensor, information, and communication systems generate data at rates beyond which humans can assimilate, understand, and act. Incorporating these technologies in military systems that collaborate with warfighters will facilitate better decisions in complex, time-critical, battlefield environments; enable a shared understanding of massive, incomplete, and contradictory information; and empower unmanned systems to perform critical missions safely and with high degrees of autonomy. DARPA is focusing its investments on a **third wave of AI** that brings forth machines that understand and reason in context."

Source: https://www.darpa.mil/work-with-us/ai-next-campaign (emphasis added, last accessed 27 March 2023).

Furthermore the document portrays a holistic defense AI approach that takes into account societal discourse and political preferences, defense capability needs and process improvements, multinational capability needs and interoperability, advances in defense digitalization, the capacities of the defense research and technology networks as well as civil and commercial progress in further developing the technology.[46] The last aspect is of particular relevance as it pushes the MoD to the backseat of AI development:

> AI is not an explicit military capability, and the Bundeswehr is not the driver of AI-related innovation. Given its economic relevance, private companies shape technology developments. As a consequence, the future use of AI by the Bundeswehr is shaped largely by adapting civil and commercial developments and applications.[47]

46 Künstliche Intelligenz. Nutzung im Geschäftsbereich des Bundesministeriums der Verteidigung, pp. 10–11.

47 "KI ist keine explizite militärische Fähigkeit und die Bundeswehr ist im Bereich KI nicht der Treiber der Innovation. Der wirtschaftlichen Bedeutung von KI entsprechend sind hier Privatunternehmen Treiber der Technologieentwicklung. Der künftige Einsatz von KI in der Bundeswehr leitet sich damit zu einem grossen Anteil aus der Adaption von zivilen/kommerziellen Entwicklungen und Anwendungen ab." See: Künstliche Intelligenz. Nutzung im Geschäftsbereich des Bundesministeriums der Verteidigung, p. 13.

Against this background the concept document mainly refers to gains in efficiency, effectiveness, and process improvements as the key imaginaries when describing the goals of using defense AI:

> AI will enable a new degree of network-enabled capabilities. In extreme cases, AI could revolutionize core aspects of the future use of force by improving the precision and accelerating the speed of the sensor to shooter chain. This could also provide additional options to reorganize the chain in more flexible ways, enhance new degrees of automation and data transmission and data management. Finally, AI could also offer new ways of delivering precision effects in hybrid teams consisting of human operators and AI support. Thus, AI could become decisive in ensuring a military actor's battlefield survivability.[48]

While the document also discusses potential areas of applications of defense AI, it refrains from describing how exactly defense AI is expected to enhance the Bundeswehr's key capabilities and how AI-enhanced initial and full operational capabilities (IOC, FOC) would look like in practice. Rather the document argues that AI should be introduced with the help of broadly defined pilot projects that can quickly expose the Bundeswehr to defense AI,[49] without specifying which capability areas should be used to achieve what kind of capability gain with the help of defense AI.

Despite numerous initiatives, the big picture for German defense AI remains blurry. The strategic rationale underpinning defense AI is fuzzy, and it is unclear how defense AI will augment capability growth over the next decades. Consequently, current efforts seem to be "lost in detail" as there is a gap between high-level guidance and ongoing projects. This gap is meant to be closed by a new defense AI implementation strategy that the Armed Forces Digitalization Center is expected to submit by the end of 2023.[50]

Service Thinking

In this context Germany's military services express different levels of ambition when it comes to using defense AI. Already back in 2017–18, the Germany Army published a series of concept notes outlining the future digital battlefield and the role of AI.[51] In 2019, the Germany Army Concepts and Capability Develop-

48 "Mit KI kann in der Zukunft ein euer Grad vernetzter Operationsführung erreicht werden. Im Extremfall könnte KI sogar wesentliche Aspekte künftiger Kriegsführung revolutionieren, indem bspw. Die Funktionskette vom Sensor zum Effektor bzw. das Gefecht noch weitaus präzisere und schneller, aber auch weiträumiger und variabler gestaltet werden kann, neue Grade der Automatisierung und Datenübertragung sowie Verarbeitung erreicht oder völlig neue Wirkkonzepte in Mischformen (hybride Teams aus Mensch und KI-Unterstützung) ermöglicht werden. Damit könnte KI entscheidend für die Überlebensfähigkeit jedes Akteurs auf dem Gefechtsfeld der Zukunft werden." See: Ibid., p. 17.
49 Ibid., p. 15.
50 Interview, 6 February 2023.
51 Wie kämpfen Landstreitkräfte künftig?; Digitalisierung von Landoperationen.

ment Office published a fully-fledged defense AI position paper. It argued that that defense AI would help render basic services more efficient, improve combat-ready capabilities, and overcome existing capability gaps.[52] In so doing the paper reflects US and NATO discourse on the digital and accelerated battlefield (hyperwar), talks about operating at machine speed, taking decisions on the edge, and using AI to coordinate and synchronize a growing number of sensors and effectors.[53] Moreover, the paper outlines four lines of efforts to use defense AI to further improve defense AI for human resources and material management, and enhance training and education.[54]

The German Luftwaffe seems convinced that without AI today's means of command and control will be insufficient to operate air power within the next 15 years. The Luftwaffe expects defense AI to synchronize information for Recognized Air Pictures (RAP), optimize flight routes, mission planning and mission management, will coordinate target acquisition, and submit proposals on how to design and implement plans of attack. The German Luftwaffe is taking baby steps in using defense AI, but its thinking is highly aligned with the US Air Force vision of using AI to set up Advanced Battle Management Systems (ABMS) to enable to conduct of Joint All Domain Operations (JADO).[55]

The German Navy, by contrast, lags behind. So far, defense AI has played only a subordinate role. The service considers itself as technology driven as the Luftwaffe, but dire savings plans have limited the Navy's capability development priorities to what is absolutely needed to ensure its survival. In the past, this even led the Navy to divest leading technology applications from aboard its ships to save costs. The current Navy leadership attempts to lead a conceptual turnaround to provide more leeway to innovation and change also by establishing a respective innovation cell with the Navy leadership team (see section 4.2). In this context the Navy warms up to defense AI, which has gained traction as of last year. As more defense AI use cases become known, sailors seem to become more aware how defense AI could offer added value aboard their ships.[56]

The Cyber and Information Domain Service has an instrumental understanding of defense AI that is directly related to its core tasks (see section 4.2). As this service plays a key role in providing common operational pictures (see section 3.1) it emphasizes the role of AI in providing analytical support and rendering digital processes more efficient and effective. As such AI is part of the so-called "Analytics

52 Künstliche Intelligenz in den Landstreitkräften, p. 10.
53 Ibid., pp. 5–7. See also: Brendecke/Doll/Kallfass, "Der Führungsprozess von morgen," p. 71.
54 Künstliche Intelligenz in den Landstreitkräften, p. 12.
55 Autorenteam Luftwaffe, "Der Einfluss künstlicher Intelligenz bei Führung von Luftoperationen der Zukunft", pp. 65–68.
56 Interviews, 23 February 2023 and 14 March 2023.

and Simulation" cluster which combines different methods such as pattern recognition, decision support, machine learning, and simulation.[57]

2.5 Ethics and Defense AI

The German emphasis on applying military power only in a well-established, normatively underpinned, and rules-based framework is a direct consequence of its strategic culture discussed in section 2.1. It implies that ethics plays a formative role for developing and using defense AI and puts a focus on arms control to shape the use of AI and other emerging technologies, as the 2021 coalition treaty underlines.[58] In addition, the MoD's 2019 defense AI concept paper is unmistakable when it posits that the MoD "can – on its own – neither lead nor shape the societal debate on AI as well as its risks and benefits, because the military use of AI constitutes only a small portion of a much broader topic."[59] Rather the MoD needs to engage in a multi-stakeholder process to shape the boarder public discourse on AI.

In this regard, leading officers make it amply clear that – in their view – defense AI should always play a subordinate role to human decision-makers. This position, however, is almost always tied to the role of lethal autonomous weapon systems, leading to a somewhat precarious focus of defense AI on this very specific application.[60] For example, Gen Dr. Ansgar Rieks, Deputy Chief of the Luftwaffe, states that "we don't want automated command of warfare. (…) We don't want autonomous weapon systems we can no longer control."[61] RADM Christian Bock, Director Education (Ausbildung), at the German Command and Staff College, contends in a co-authored paper that "humans must remain in control of decision making as AI cannot replace human innovation, surprise, human values, personal experience, trust and emotions, and camaraderie."[62] Such statements serve to show that the Bundeswehr leadership holds a collective vision, stabilize institutional thinking[63] about defense AI, and publicly communicate the socio-technical imaginary that shapes Germany's dealing with defense AI.

57 "Von Big Data zu KI: Zweite Ausbaustufe des Gemeinsamen Lagezentrums CIR," Färber, "Digitalisierung der Bundeswehr," p. 231.
58 Mehr Fortschritt wagen, p. 146.
59 "Der gesellschaftliche Diskurs zum Gesamtthema KI und die mit deren Anwendung verbundenen Chancen und Risiken kann nicht alleine durch das BMVg gesteuert oder gestaltet werden, da die militärischen Anwendungsbereiche nur einen kleinen Teil des Gesamtthemas darstellen." See: Künstliche Intelligenz. Nutzung im Geschäftsbereich des Bundesministeriums der Verteidigung, p. 10.
60 "The debate on responsible AI in a military context should not have a predominant focus on ethical issues regarding (lethal autonomous weapon systems." See: Meerveld/Lindelauf/Postma/Postma, "The irresponsibility of not using AI in the military," p. 4.
61 Ehlke, "Interview mit Generalleutnant Dr. Ansgar Rieks," S. 18
62 "Der Mensch muss allein deshalb Teil der Entscheidungen bleiben, weil KI in keiner Phase den Menschen mit dessen Innovation, Überraschungsfähigkeit, Werten, persönlichen Erfahrungen, Vertrauen und Emotionalität, insbesondere der Kameradschaft ersetzen kann." See: Bock/Schmarsow, "Gedanken zum Einsatz von KI beim militärischen Führen und Entscheiden", p. 154.
63 For more on the role of institutional thinking and tacit knowledge in facilitating or preventing military innovation, see: Jensen/Whyte/Cuomo, Information in War, pp. 35–36, 40–46.

Germany's strong focus on ethics in relation to technology also influences the narrative used to justify the use of defense AI. In response to our question about the strategic purpose of using defense AI, one interview partner argued that it's all about "humanitarian precision." Humanitarian precision, in turn, combines the reality of a post-heroic and risk-averse society with the need for speed on the battlefield. Humanitarian precision thus is a political currency as it provides the Bundeswehr legitimation in the eye of political decision-makers and thus makes the armed forces an accepted political instrument.[64] "The sharp end of digitalization" is a similar rhetorical figure used by members of the Bundeswehr[65] to describe the added value of digitalization in advancing precision effects.

However, demanding respect for ethical principles and normative guidelines in technology development is one thing, implementing adequate approaches to do so is a different thing. So far, the MoD's guidance on implementing ethical guidelines has remained vague, while in practice different initiatives emerge:

- At the international level the new ISO/IEC/IEEE 24787–7000:2022 standard defines a process for value-based engineering also applicable for defense.[66] Members of the NATO Data and Artificial Intelligence Review Board (DARB) sympathize with using this standard, which is also currently explored by the GhostPlay consortium (see section 3.1).[67]
- At the national level the German Association for Electrical, Electronic, and Information Technologies (VDE) has submitted a standard to ensure AI trustworthiness that shall lead to an AI Trust Label. The standard can be used across all industry sectors and is based on specifying values, measurable criteria, indicators, and observables.[68]
- At the corporate level companies work on project-specific solutions. One German example is the independent panel of experts on the responsible use of new technologies in the context of the Future Combat Air Systems (FCAS).[69] Among other things, this approach shall lead to creating a so-called FCAS Ethical AI Demonstrator envisaged to provide a scenario-based simulation environment which can illustrate ethical dilemmas and possible options in solving them.[70]

64 Interview, 22 February 2023.
65 Interview, 22 February 2023. See also: Rieks, "Digitalisierung der Streitkräfte," p. 104.
66 For more on the standard, see: https://www.iso.org/standard/84893.html (last accessed 27 March 2023).
67 Interview, 7 February 2023. See also: Hofstetter/Verbovszky, How AI Learns the Bundeswehr's "Innere Führung."
68 "Kann Künstliche Intelligenz wertekonform sein?"
69 https://www.fcas-forum.eu/en (last accessed 27 March 2023).
70 Koch, "Elements of an Ethical AI Demonstrator for Responsibly Designing Defence Systems."

3 Developing Defense AI

The German MoD and the Bundeswehr have embarked on exploring the opportunities of defense AI. Numerous projects have been kicked off, but it remains difficult to understand how individual projects will contribute to future capability growth. In addition, structural pacifism has led to a bifurcated national ecosystem favoring knowledge stovepipes rather than an integrated approach.

3.1 Development Priorities and Projects

At the time of writing this study, a national defense AI capability roadmap has not been publicly released. The MoD's leading Directorates-General (see section 4.1) might have a clear understanding what ongoing defense AI development activities are meant to achieve but such a perspective has not been publicly communicated. Therefore, Bundeswehr's defense AI development priorities remain opaque. Consequently, this section provides our assessment of more than a dozen ongoing projects that have been selected to illustrate the diversity of current activities.[71] We structure these projects along the Bundeswehr's capability value chain – with some projects crossing several capability areas – and highlight the primary domain on which the respective projects focus (Table 1).

Command, Control, Computers, Communications, and Cyber (C4/C5)

Generating new and supporting existing Common Operational Pictures (COP) with the help of AI is a major focus area. This priority extends previous activities started in the early 2000s when the strive for Network-Enabled Operations shaped Bundeswehr transformation.[72] As in the past, COPs are considered central to acting swiftly and precisely.[73] AI is expected to deliver new functionalities with regard to assessing mass data, pattern recognition, and computing suggestions for courses of action.[74] Defense AI in support of COPs is important because this area of application is considered inconspicuous and in line with the dominant socio-technical imaginary thus giving the Bundeswehr freedom to explore AI's strengths and shortfalls.[75] COPs also constitute an ongoing capability gap,[76] which will become even more important to close given the Bundeswehr's growing emphasis on the need of being MDO capable.

71 We respect information classification levels and thus remain generic in describing the relevant projects. Whenever possible, we provide references to public source for additional information.
72 Borchert, "The Rocky Road to Networked and Effects-Based Expeditionary Forces," pp. 83–107.
73 Operative Leitllinien für die Streitkräfte, para. 271.
74 Künstliche Intelligenz. Nutzung im Geschäftsbereich des Bundesministeriums der Verteidigung, pp. 17–18.
75 Interview, 28 February 2023.
76 Interview, 23 February 2023.

Table 1: Selected German Defense AI Development Projects

Command, Control, Computers, Communications, Cyber (C4/5)	Intelligence, Surveillance, Reconnaissance	Precision Effects	Support
(Führung)	(Aufklärung)	(Wirkung)	(Unterstützung)
Common operational pictures	Military internet of things for tactical reconnaissance (MITA)	Wild Hornets: AI-enhanced capability development for air-launched effects	FCAS focus on navigation, cyber security, training, and life cycle costs
Subsea situational picture	Automated assessment of sensor data		Electromagnetic resistance of unmanned systems (ESAS)
Space situational awareness	AI classifier for hydroacoustic signatures		MissionLab
AirC2			
Air Combat Management System (ACMS)			
FCAS situational awareness			
AI for Next Generation Weapon System (NGWS)			
ErzUntGlas: Glass battlefield			
AuGe: Automated terrain evaluation to support operational planning			
Ostflanke: Wide Area ISR			
FCAS "kill chain" and Future Combat Mission System (FCMS)			
Main Ground Combat System (MGCS)			
GhostPlay: Digital twin of the future AI-driven battlefield			

Land Domain **Naval Domain** **Air Domain** **Cyber Domain** **Others**

Source: Authors' compilation.

Although useful, the COP focus is also problematic. For one it is challenging to fuse management and military relevant data into overall pictures as the underlying data sets fall into different levels of classification. In addition, current operational picture applications are not yet seamlessly linked to the emerging crisis early warning system that the Bundeswehr is already using (see section 6).[77] Finally, the focus on COP tends to reinforce a centralized and hierarchical understanding of command and data management which can render military decision-making brittle in view of adversarial attempts to own the electromagnetic domain.

The Bundeswehr's military services have specific COP needs. The Navy, for example, wants to create a subsea situational picture by fusing data from various military sensors with geoinformation and information about key offshore and subsurface infrastructure. AI is meant to be used for object recognition, modelling, and new modes of data visualization.[78] Space Situational Awareness satisfies a similar need for a different domain with BWI and the Cyber Innovation Hub of the Bundeswehr (CIHBw) exploring the use of defense AI to forecast space weather and project orbital movements of objects to avoid space collisions.[79]

The Luftwaffe launched a study to assess the role of AI in its command and control process. Project AirC2 evaluates the contribution of AI in increasing C2 efficiency and tempo and looks at the added value of AI in enhancing air C2 education and training. In addition, the Air Combat Management System (ACMS) project evaluates the use of AI to anticipate adversarial action, produce recognized air pictures, and recommend future courses of action.[80]

Defense AI is also a major issue for the Future Combat Air System (FCAS) and the Next Generation Weapon System (NGWS). FCAS has identified a total of eight use cases for defense AI. Situational awareness strives to establish a common relevant operational picture with AI to "support orientation, decision making, and planning; either for a human operator using tactical displays or for automated functions directly assessing (…) digital data."[81]

Intelligence, Surveillance, and Reconnaissance (ISR)

Using defense AI for tactical-level reconnaissance constitutes the core of project MITA.[82] It focuses on wide area surveillance with the help of an AI-augmented sensor grid and automated data fusion. The goal is to produce a COP that illus-

77 Interview, 18 March 2022.
78 Interview, 23 February 2023.
79 "Wie KI bei der Vorhersage des Weltraumwetters hilft."
80 Interview, 25 March 2022.
81 Azzano et al., "The responsible use of AI in FCAS."
82 MITA stands for "Military Internet of Things für taktische Aufklärung" or military internet of things for tactical reconnaissance.

trates adversarial troop movements in 3D and identifies adversarial intruders in real-time. BWI and Helsing have been working on this project, which was demonstrated in a live experiment at the end of 2022.[83]

Defense AI for ISR is also of interest for the Germany Navy. In cooperation with the University of the Bundeswehr/Hamburg, the Navy is developing AI-augmented solutions to assess sensor data and classify hydroacoustic signatures.[84]

Precision Effects

Wild Hornets uses and develops AI tactics for aggressors and defenders to evaluate existing concept ideas. To this purpose the project will develop tactics for air-launched effector swarms that target an adversarial high-value asset and test the feasibility of using air-launched effectors against next generation ground-based air defense solutions. Wild Hornets is a cooperation project that involves the Germany Army Concepts and Capability Development office and team GhostPlay (see below).

Support

Several FCAS use cases look into the use of defense AI for supportive functions. AI shall enable complex guidance and flight control behavior to navigate unmanned platforms. Improving the detection of anomalies and adversarial activities shall improve cyber security and resilience. System operator training shall become AI augmented, and AI-based big data analytics could improve production, maintenance, and logistics thus reducing life cycle costs.[85]

Within dtec.bw (see section 3.2), ESAS at the University of the Bundeswehr/Hamburg uses AI, simulation, and numerical modelling to advance existing test and validation methods to improve the electromagnetic resistance of unmanned systems.[86] The MissionLab at the University of the Bundeswehr/Munich creates a center of competence to test mission technologies such as mission planning/management systems, intelligent sensor systems or adaptive assistance systems with experimental simulation and flight trials thereby also using AI.[87]

83 BWI, "Generalinspekteur lässt sich KI-gestützte Aufklärung vorführen."
84 Presentation at the University of the Bundeswehr/Hamburg, 15 March 2022; written communication, 22 July 2022.
85 Azzano et al., "The responsible use of AI in FCAS."
86 ESAS stands for "elektromagnetische Störfestigkeit autonomer Systeme." For more, see: https://dtecbw.de/home/forschung/hsu/projekt-esas/projekt-esas (last accessed 27 March 2023).
87 For more, see: https://dtecbw.de/home/forschung/unibw-m/projekt-missionlab/projekt-missionlab (last accessed 27 March 2023).

Cross-Functional Projects

Defense AI can improve situational awareness and situational understanding by improving the C2-ISR link. This, for example, is a key national R&T priority for NGWS with a focus on sensor data fusion, sensor resource management, and the integration of both elements. This project also explores options for a so-called AI Backbone that would provide a "single set of algorithms" to support different tasks and establish an open and unitary framework to facilitate the comprehensive use of defense AI. Different companies are involved with Helsing, Schönhofer Sales and Engineering, and IBM leading the AI Backbone workstream.[88]

In addition, ErzUntGlas[89] explored options how to improve and accelerate interactions between existing land systems with unmanned aerial systems (UAS) and AI. Several UAS were used as sensor carriers to produce a recognized operational picture that was integrated into the Army's C2 system via SitaWare Frontline. The project ran from 2019 to 2021 and was meant to support the German-Franco Main Ground Combat System (MGCS). The procurement office BAAINBw worked in tandem with Atos, Krauss-Maffei Wegmann, RAFAEL and Aeronautics.[90] With a similar goal AuGe[91] looks at the role of AI in automatically assessing and incorporating terrain specifics into operational planning with the aim of using terrain features for tactical advantages.[92]

Different initiatives focus on the role of defense AI in the so-called "kill chain."[93] Eastern Flank, for example, is a follow-on project to MITA funded by the new Sondervermögen. It combines the use of defense AI for modular effector systems with a UAS-based surveillance system. Automating the handover of targeting data to different effectors is one of the capabilities to be developed.[94] Developing a more effective "kill chain" also constitutes a core element of FCAS and the Future Combat Mission System (FCMS). AI is expected to support the detection and identification of potential targets, improve threat analysis and weapon aiming and facilitate a platform-agnostic sensor-to-shooter management.[95] The same is true for MGCS, which is to build a federated multi-asset approach to deliver future land power. AI is expected to contribute to situational awareness, manned-unmanned teaming, multi-sensor data fusion, and sensor-effector resource management.[96]

88 Interview, 2 March 2023.
89 ErzUntGlas stands for "Erzeugung eines gläsernen Gefechtsfelds zur Unterstützung dynamischer Operationen" or producing a "glass battlefield" to support dynamic operations.
90 Wiegold, "Studie fürs 'gläserne Gefechtsfeld' Drohnen und KI"; "Live-Demonstration Aufklärung im 'Gläsernen Gefechtsfeld'."
91 AuGe stands for "Automatisierte Geländebeurteilung im militärischen Führungsprozess zur Beschleunigung der Entscheidungsfindung" or automated terrain evaluation as part of the military command process to accelerate decision-making.
92 Interview, 14 November 2022.
93 The "kill chain" is a popular military term to describe the link between C4/C5, ISR and precision effects.
94 Interview, 14 November 2022.
95 Azzano et al., "The responsible use of AI in FCAS;" https://fcms-germany.net/ (last accessed 27 March 2023).
96 Dean, "Main Ground Combat System (MGCS): A Status Report."

GhostPlay is also cross-functional but has a different focus. This project leverages defense AI to develop tactics. It develops defense decision algorithms (Play) for defender and aggressor tactics thereby using a powerful simulation environment (Ghost). GhostPlay's original focus envisions a Suppression of Enemy Air Defense (SEAD) scenario with swarms of unmanned aerial systems targeting a high value asset protected by ground-based air defense. Both sides use AI developed tactics to outsmart each other. The "ability to learn tactical behavior in cooperation with other machines and/or humans" constitutes the projects' AI research focus.[97] GhostPlay is part of dtec.bw with the University of the Bundeswehr/Hamburg as the lead and a consortium including Hensoldt, 21strategies, and Borchert Consulting & Research.

3.2 Germany's Defense AI Ecosystem

The 2020 capstone document of the German government on supporting the security and defense industry has identified AI as a national key technology.[98] The problem, however, is that the implications of this categorization are unclear. In addition, Germany's techno-industrial ecosystem is bifurcated, with defense-relevant actors being mostly segregated from the remaining ecosystem. Germany's key policy documents reflect this spilt and maintain an artificial separation between the civilian and military domain even in areas of application with obvious dual use potential.[99] Therefore the German Bundeswehr has access to only a limited spectrum of the country's techno-economic power. Overall, the defense AI ecosystem, as a sub element of the national ecosystem, rests on four building blocks (see Table 2 on next page).

Bundeswehr

The Bundeswehr constitutes the ultimate end user, whose requirements shape defense products. Seamless exchange with the remaining partners of the defense AI ecosystem would be needed to optimally synchronize each partner's activities. This, however, is undercut by civil-military dichotomy that maintains knowledge and technology stovepipes that are challenging to penetrate.

As we discuss in more detail in section 4, the Bundeswehr has established new entities to advance defense digitalization, such as the so-called Systems Centers

97 Borchert/Brandlhuber/Brandstetter/Schaal, Free Jazz on the Battlefield, p. 11.
98 Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie, p. 3.
99 Borchert/Schütz/Verboszky, "Unchain My Heart," pp. 433, 437–438, 447; Hagebölling/Barker, Ethik und einsatzfähig, p. 6;

Table 2: Selected Actors in Germany's Defense AI Ecosystem

Bundeswehr	Research and Technology Organizations	Defense Industrial Players	IT and Consulting Companies
Army • Test and experimentation units • Systems Center for Digitalization Land Domain **Navy** **Luftwaffe** **Cyber and Information Service (CIR)** • Center for Digitalization **Joint Support Service (Streitkräftebasis)** **Medical Command (Sanitätsdienst der Bundeswehr)** **BWI** • Cyber and Innovation Hub (CIHBw)	**Fraunhofer Segment for Defense and Security (VVS)** **German Aerospace Center** **Bundeswehr Universities in Hamburg and Munich** **dtec.bw**	**Established Players** • Airbus • Atlas Elektronik • Diehl • ESG • Hensoldt • IABG • KMW • MBDA • Plath • Rheinmetall Defense • Rhode & Schwarz • Schönhofer Sales and Engineering • tkMS **New Players** • 21strategies • Aleph Alpha • Data Machine Intelligence Solutions • HAT.tec • Helsing • Traversals	• Accenture • Atos • CapGemini • Conet • IBM • MSG Plaut • PwC • SAP

Source: Authors' compilation.

(Systemzentren) for single services. Some service-specific institutions also have a cross-functional task, such as the Center for Digitalization of the Bundeswehr. This center is key to develop Germany's CIR capabilities, provides software development and IT integration capabilities for the Bundeswehr, and is in charge of developing the Bundeswehr's capabilities for military intelligence, electronic warfare, and geoinformation.[100]

Moreover, the Cyber Innovation Hub of the Bundeswehr serves as a transmission mechanism to accelerate digital solutions that originate from within the Bundeswehr and to spin-in outside digital innovation.[101] BWI is the Bundeswehr's own system house that supports digitalization in the fields of infrastructure provision, application development, and strategic advice.[102] Finally, the German Army also uses its test and experimentation unit as a testbed for rapid technology insertion and experimentation as well as synchronized concept and technology development.[103]

Research and Technology Organizations (RTO)

RTO constitute the second pillar of the defense AI ecosystem. Here bifurcation becomes most obvious. More than 70 universities and universities of applied sciences adhere the voluntary civil clause that prevents them "from engaging in defense research and cooperating with the defense industry."[104] This also means that the Bundeswehr will not directly benefit from the German government's decision to set up six centers of competence on AI[105] and "providing funding for the establishment of 100 new professorships in AI at German universities."[106] Furthermore, the German Research Center for AI (DFKI), which has been pioneering AI research since the late 1980s, does not engage in defense either.[107]

To some extent the Bundeswehr can close the gap by relying on research and technology conducted at its universities in Hamburg and Munich. Activities at these two locations have received a boost thanks to a €500M budget to set up the Digitalization and Technology Research Center (dtec.bw) that is meant to advance defense digitalization.[108] Beyond dtec.bw, the lion's share of Germany's defense

100 For more, see: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/zentrum-digitalisierung-der-bundeswehr (last accessed 27 March 2023).
101 For more, see: https://www.cyberinnovationhub.de/en/ (last accessed 27 March 2023).
102 For more, see: https://www.bwi.de/ (last accessed 27 March 2023).
103 "Test- und Versuchskräfte in Munster aufgestellt."
104 Borchert/Schütz/Verbovszky, "Unchain My Heart", p. 437.
105 For more, see: https://www.bmbf.de/bmbf/de/forschung/digitale-wirtschaft-und-gesellschaft/kuenstliche-intelligenz/kuenstliche-intelligenz_node.html (last accessed 27 March 2023).
106 Artificial Intelligence Strategy of the German Federal Government. 2020 Update, p. 10.
107 For more, see: https://www.dfki.de/web (last accessed 27 March 2023).
108 For more, see: https://dtecbw.de/home (last accessed 27 March 2023).

research falls on the Fraunhofer Society and the German Aerospace Center.[109] The so-called Fraunhofer Segment for Defense and Security combines the dedicated know how of twelve RTO with expertise in radar techniques, communication and information processing, high-speed dynamics, optronics, and applied optics to name but a few areas of core expertise.[110] The German Aerospace Center mirrors some of these areas of expertise and contributes additional capacities in the fields of AI safety and security as well as well as in-depth aerospace research activities.[111]

Defense Industrial Players: Old and New

The defense industry forms the third pillar of the defense AI ecosystem. Most of Germany's key defense companies are involved in developing or adopting AI for defense purposes in one way or another. More recently, several new players with a dedicated focus on AI and defense AI have entered the market. Some of them originate from the commercial world and join forces with incumbent defense players:

- 21strategies specializes in developing large scale multi-agent reinforcement learning to compute optimal decision-making strategies under uncertainty in the context of national security, capital markets, and supply chains. The company originates from the finance industry and has been deploying its technology in trading and risk hedging. 21strategies works on GhostPlay, Wild Hornets, FCAS, and NGWS. Hensoldt cooperates with 21strategies.[112]
- Aleph Alpha is working on large language models and develops generative AI solutions to support public and private sector applications. Among others, Aleph Alpha is working on defense AI solutions for FCAS.[113]
- Data Machine Intelligence Solutions develops data modeling and visualization solutions, inter alia, with a focus on solutions for mission planning and management as well as simulation technologies. Data Machine Intelligence Solutions also contributes to FCAS's defense AI work stream.[114]
- HAT.tec focuses on developing technologies in support of human-autonomy teaming, with a focus on automated reasoning, planning and decision-making. HAT.tec also works on defense AI solutions for FCAS.[115]
- Helsing develops AI for real-time information processing and turning unstructured sensor data into common operational pictures. The company is head-

109 Together with France, Germany also maintains the German-Franco Research Institute Saint-Louis with a focus on energetic and advanced protective materials, flight techniques for projectiles, laser technologies as well as protection technologies, security, and situational awareness. For more on this institute, see: https://www.isl.eu/en/research (last accessed: 27 March 2023).
110 For more, see: https://www.vvs.fraunhofer.de/en/members.html (last accessed: 27 March 2023).
111 For more, see: https://www.dlr.de/EN/research/research.html (last accessed: 27 March 2023).
112 For more, see: https://www.21strategies.com/ (last accessed 27 March 2023).
113 For more, see: https://www.aleph-alpha.com/ (last accessed: 27 March 2023).
114 For more, see: https://www.datamachineintelligence.eu/ (last accessed: 27 March 2023).
115 For more, see: https://www.hattec.de/ (last accessed: 27 March 2023).

quartered in Germany with subsidiaries in France and the United Kingdom. Helsing works on defense AI for FCAS, NGWS and MITA. Helsing cooperates with Rheinmetall Defense Electronics, Saab, and MBDA.[116]

- Traversals uses AI for open-source intelligence to analyze and assess global events, identify potential threats, and assessing multilingual information. Traversals AI Dynamic Frontline Monitoring, for example, uses AI-enhanced technologies to provide a 24/7 near-real time operational picture of the Ukrainian-Russian front line.[117]

Overall, a recent market survey by the Ministry for Economic Affairs and Climate Action suggests that more than 6,600 AI startups employing 149,000 people have been established in Germany since 1995.[118] As of this total around 400 AI companies are members of the German AI Association. So far, however, this association also adheres to the civil clause restricting cooperation with the MoD and the Bundeswehr. But rumors have it that compliance with the voluntary self-binding rule is about to expire soon.[119]

IT and Consulting Companies

IT and consulting companies form the final fourth pillar of the German defense AI ecosystems. These companies are instrumental in supporting concept development, providing hardware infrastructure and computer processing capacities as well as assisting the synchronization of digitalization and organizational change.

116 For more, see: https://helsing.ai/ (last accessed: 27 March 2023).
117 For more, see: https://traversals.com/ (last accessed: 27 March 2023).
118 According to the survey around 58% of all startups work on software and IT services followed by consulting, advertising and financial services (approximately 19%) and engineering and research and development services (around 7%). See: KI-Startups in Deutschland, pp. 6, 12.
119 Interview, 14 February 2023.

4 Organizing Defense AI

The Bundeswehr is in its early days to adjust its organizational fitness to future defense AI requirements. The 2019 capstone document acknowledges that a strong Bundeswehr-common approach with joint responsibility for capability development is needed to counter the risks of duplication, parallel structures, crowding-out effects, and fragmentation.[120] So far, however, tensions exist between top down-driven and decentralized service-specific approaches.

4.1 Joint Approaches

At the ministerial level there are two sources of power advancing defense AI. On the one hand, defense AI is part of the Bundeswehr's digitalization approach with the Directorate-General for Cyber/IT shaping the respective agenda. CIT I 2, in particular, is responsible for research and technology as well as innovation management related to Cyber/IT, while CIT II 8 is responsible for the Bundeswehr's IT systems as well as analysis and simulation. In 2019 the German MoD has also established a Digital Council (Digitalrat), which advises the Minister of Defense and provides impulses to advance defense digitalization.[121] On the other hand, the Directorate-General for Planning implements the Bundeswehr's integrated planning. In this regard defense AI is part of the toolbox needed for the Bundeswehr's future development. Therefore, Plg I 2 plays a key role with the leading desk officer for defense AI who also chairs the Bundeswehr's defense AI community, a semi-formalized network set up to advance information sharing related to defense AI activities.

Tensions arise from the fact the Bundeswehr's military services follow different digital levels of ambition and enjoy great leeway in implementing their respective digital agendas while the Directorate-General for Cyber/IT shapes the broad guidelines and the idea of a Bundeswehr-common AI backbone (see section 3.1). This creates a "wait and see" atmosphere as the services need to strike a balance between following through on their own agendas and supporting a joint agenda, which might come at the cost of sacrificing service-specific resources for joint tasks. A cluster approach that respects joint and service-specific interests could work, observers say, but very much depends on the willingness of the actors involved and the availability of extra resources. This situation creates a vacuum, which nurtures the rise of "local kingdoms," that strive to advance activities within their own areas of responsibility with insufficient levels of information exchange and coordination across the services.[122]

120 Künstliche Intelligenz. Nutzung im Geschäftsbereich des Bundesministeriums der Verteidigung, p. 20.
121 Erster Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung, p. 16.
122 Interviews, 25 March 2022 and 14 March 2023.

In this context tensions are likely to be reinforced by the ambition to set up a Bundeswehr Multi Domain Combat Cloud (MDCC) as a key digital instrument to enable Bundeswehr MDO (see section 2.2).[123] In essence, cloud-based approaches are considered key to synchronize service specific operational pictures.[124] As such the MDCC will emerge in parallel with domain specific cloud concepts for future airpower (FCAS) and land power (MGCS) solutions. In addition, the FCAS combat cloud is likely to compete with the F-35 cloud concept that will be relevant for the Bundeswehr given its recent decision to procure the US fighter jet. So far, it is unclear how all these cloud concepts will be aligned and how the duality of national and multinational cloud approaches will affect cloud-based defense AI services.

4.2 Single Service Approaches

Against this background, the Bundeswehr services operate at different levels to bring organizations in line with defense AI requirements.

Army

The Army's program on digitalizing land-based operations (D-LBO) is the service's capstone program to create a whole-of-service digital federation for future operations.[125] Within this context, the Army's 2019 AI concept paper offers a vision to set up an AI steering group with the Army Command that would oversee the work of the so-called Army AI Work Bench at the Army Concepts and Capabilities Development Office. This work bench is meant to serve as the overall coordination mechanism for all Army AI activities and liaise with industry and academia. In addition, the Army would create a development center mainly focusing on training defense algorithms and developing key data models as well as an AI data center that would take care of Army data, provide data expertise and data scientists.[126]

Elements of this vision will be realized with the Army's forthcoming Systems Center for Digitalization (Systemzentrum Digitalisierung Dimension Land). It combines elements of a data center with software development, tests as well as validation and verification. The center is going to be the powerhouse for all things digital of the Army and is thus also likely to play an important defense industrial role by strengthening digital sovereignty with defense software developed in Germany.[127]

123 Färber/Bibow, "Die Multi Domain Combat Cloud für die vernetzte Operationsführung," pp. 55–58.
124 Interview, 22 February 2023.
125 For a general overview, see: https://www.bundeswehr.de/de/organisation/heer/organisation/faehigkeiten/digitalisierung (last accessed 27 March 2023).
126 Künstliche Intelligenz in den Landstreitkräften, p. 14–15, 19–20.
127 Interview, 22 February 2023. For more on the center, see: Systemzentrum Digitalisierung Dimenson Land, para. 301–315.

Luftwaffe

The German Luftwaffe is exploring the impact of defense AI on future air power. So far, the service has taken organizational baby steps with one desk officer in the Luftwaffe Command being in charge of the subject matter. The Luftwaffe also considers defense AI as part of its broader digitalization agenda and as an important enabler to advance air power innovation. Tensions exist here as well as the service has two responsible officers for digitalization (Deputy Air Chief) and innovation (desk officer, LTC level). Both have pledged to inform each other but given "split" responsibilities true leadership on defense AI remains yet to be developed.[128]

Navy

The new Chief of the Navy puts great emphasis on naval innovation. He has created the position of a Commissioner for Innovation, Digitalization, Empowerment, and Agility (ID:EA)[129] at the Naval Command. This new position is to bridge the digitalization/innovation divide and push both agendas. Defense AI is part of the ID:EA tasks and will benefit from a vast network of naval reservists that is to be expanded. Overall, the current focus is on breaking up existing structures by creating opportunities for new digital naval projects outside existing planning processes that are considered too cumbersome to deal with.[130]

Cyber and Information Domain Service

The Cyber and Information Domain Service, established in 2017, operates and protects the Bundeswehr's IT infrastructure, is engaged in electronic warfare, provides satellite-based imagery reconnaissance data, and operates the Bundeswehr Geoinformation Center.[131] Its Center for Bundeswehr Digitalization and Cyber and Information Service Capability Development (Zentrum Digitalisierung Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum) pools software analysis and software development expertise.[132] With regard to defense AI, the Electronic Warfare Battalion 912, for example, plays an important role as its own AI laboratory is exploring the use of AI to calculate flight paths or analyze radio communications.[133]

128 Interview, 25 March 2022.
129 The Navy Chief announced his intention to create this position in April 2022. For more, see: Inspekteur der Marine – Absicht 2022, p. 5.
130 Interviews, 23 February 2023 and 14 March 2023.
131 For more, see: https://www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service (last accessed 27 March 2023).
132 Fleischmann, "Das Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum," p. 36.
133 For more, see: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/aktuelles/das-ki-labor-eine-explorative-lern-und-entwicklungsumgebung-5514392 (last accessed 27 March 2023).

5 Funding Defense AI

Most recently, the 2020 decision to spend €500M on setting up the dtec.bw and the 2022 decision on the new €100bn special fund (Sondervermögen)[134] have increased the Bundeswehr's financial leeway to some extent. But how much the Bundeswehr[135] spends on defense AI is difficult to gauge, as defense R&T projects are integrated into ongoing and future procurement programs with overall program costs not disclosing individual R&T amounts. Thus, we suggest three levels of analysis to get a basic understanding of current funding priorities:

- **Digital infrastructure**
  Investments in the Bundeswehr's digital infrastructure are essential to implement the digitalization ambition discussed above. Consequently, roughly 20% of the special fund are about to be spent on this focus area.[136] The 2023 Sondervermögen budget plan further specifies that €8.5bn have been earmarked for D-LBO, almost €4.5 for satellite-based communications, €3.5bn for equipment, and €2.6bn for the German Mission Network.[137]

- **Defense research and technology**
  Germany's 2023 budget law has earmarked around €330M on defense research and technology. The fact that this budget line has been cut by almost €200M compared to 2022 has created controversies and push back from leading RTO and defense industrial associations. In addition, the budget foresees approximately €515M on defense development and experimentation, which includes key weapons developments projects. Furthermore, the MoD can spend around €40M on methods such as Concept Development & Experimentation, modeling and simulation and innovation competitions, and around €25M on disruptive innovation in cybersecurity and key technologies. In addition, the defense budget also supports key research and technology organizations like the German-Franco Research Institute St. Louis (€24M), the German Aerospace Center (€50M), and the Fraunhofer Society (€90M).[138]

- **Defense AI**
  Specific figures for defense AI spending are even harder to come by. Two sources provide rough indications. The Sondervermögen law earmarks a total of €422M for research, development and AI, with AI focusing on surveying and

134 The five-year duration has been defined by the special law on the Sondervermögen. See: §1 Gesetz zur Finanzierung der Bundeswehr und zur Errichtung eines "Sondervermögens Bundeswehr" und zur Änderung der Bundeshaushaltsordnung.
135 By contrast, the German government has pledged to spend €5bn until 2025 to implement the national AI strategy. See: https://www.bmbf.de/bmbf/de/forschung/digitale-wirtschaft-und-gesellschaft/kuenstliche-intelligenz/kuenstliche-intelligenz_node.html (last accessed 27 March 2023).
136 Gesetz zur Finanzierung der Bundeswehr und zur Errichtung eines "Sondervermögens Bundeswehr" und zur Änderung der Bundeshaushaltsordnung, p. 1034.
137 Gesetz über die Feststellung des Bundeshaushaltsplans für das Haushaltsjahr 2023, Einzelplan 14, pp. 69–70.
138 Ibid., pp. 45, 48–49.

safeguarding wide areas (Eastern Flank).[139] The 2023 Sondervermögen budget law breaks this focus area down to a €16M increment without further specifying the AI amount.[140] We speculate that the respective amount is in the lower single-digit range. In addition, several dtec.bw projects focus on developing defense AI. Taken together, the total four-year budget of three AI projects[141] at the University of the Bundeswehr/Hamburg is about €20–30M, or €5–7.5M per year. The MissionLab at the University of the Bundeswehr/Munich operates on a total budget worth around €20M, or around €5M per year. In addition, we speculate that the German MoD spends a lower two-digit million amount per year on developing AI for NGWS. Considering these figures and adding a calculated reserve for projects unknown at the time of writing, we assume that the MoD currently spends around €50M per year on defense AI software development.[142]

139 Gesetz zur Finanzierung der Bundeswehr und zur Errichtung eines "Sondervermögens Bundeswehr" und zur Änderung der Bundeshaushaltsordnung, p. 1033.
140 The respective budget line includes spending on defense AI as well as land and sea-based navigation and mobile navigation in a Navigation Warfare (NAVWAR) environment.
141 This includes projects GhostPlay and ESAS discussed in section 3.1 and the (K)ISS project that develops AI-based diagnosis solutions for the International Space Station.
142 This is a rough estimate as most figures are not publicly available.

6 Fielding and Operating Defense AI

Explicit defense AI features and requirements have been defined for major future defense systems, but they remain to be developed. In-service defense systems use AI applications but a clear delineation between software-enabled analytics and automation and proper AI is difficult to draw. Consequently, the true status of the Bundeswehr's fielding and operating of defense AI is difficult to grasp. Overall, the following overview of selected projects is in line with the development priorities discussed in section 3.1.

Command, Control, Computers, Communications, and Cyber (C4/C5)

The German MoD's crisis early warning system is one of the most prominent defense AI use cases. The application currently in use with the Directorate-General for Strategy and Operations constitutes the MoD's contribution to the federal government's activities on crisis early warning. The Metis institute for strategy and foresight[143] at the University of the Bundeswehr/Munich supports the respective activities with analyses and research on AI for early warning.

The so-called Preview system analyses open-source intelligence (OSINT) for early warning. AI is providing data analytics and predictive analysis. Preview currently uses more than 60 indicators for early warning. The system is transparent, i.e., users can zoom in on each indicator's quantitative assessment, track assessment changes over time, and provides access to the sources that underpin assessment results. Preview is a multi-language solution that also offers back casts to validate the feasibility of current assessments with a database reaching back to 2015. As Preview is an OSINT solution, classified and open date are not yet fused. In addition, a link between crisis early warning and the Bundeswehr's activities on establishing common operational pictures has yet to be established.[144]

Intelligence, Surveillance, and Reconnaissance (ISR)

In early 2022, the Bundeswehr decided to equip all NH90 helicopters with a new protection suite that also includes AI-based components. The Hensoldt solution is using the company's Kalaetron Radar Warning Receiver, which uses AI for big data analysis to quickly detect new threat patterns and with a very low false alarm rate.[145]

Since 2018, BWI has been experimenting with the use of AI in combination with radar technology already in use on construction sites to see through walls. An intelligent algorithm shall detect humans as individuals or groups and identify the

143 https://metis.unibw.de/en/ (last accessed 27 March 2023).
144 Interviews, 18 and 21 March 2022. For more, see: Schurad, "Mit künstlicher Intelligenz der Zukunft auf der Spur," pp. 10–12.
145 "Hensoldt präsentiert Radarwarner auf KI-Basis;" "Hensoldt equips Bundeswehr NH90 helicopter with state-of-the-art protection systems."

current state of motion (walking, standing, or sitting). The feasibility of this application has been demonstrated, but a decision about the final use by the Bundeswehr is pending.[146]

Precision Effects

The IRIS-T air-to-air missiles developed by Diehl and in use with the Luftwaffe is using intelligent image processing to detect and defeat adversarial infrared decoys when engaging a target.[147] We assume that the same technology would be used for the Interactive Defence and Attack system for Submarines (IDAS), a technology project with thyssenkrupp Marine Systems, that was withdrawn from the Sondervermögen funding list after the Federal Audit Office criticized spending priorities.[148] Its funding now depends on the availability of money from the regular defense budget.

Similar technologies are also likely to underpin the Rolling Airframe Missile (RAM), that the German Navy is using to protect frigates and class K130 corvettes.[149] Originally developed by Raytheon in cooperation with Diehl and MBDA Germany, the missile uses "a new image-scanning seeker with autonomous (infrared) all-the-way guidance" and "requires no shipboard support after launch."[150]

Support

Different defense AI use cases fall into the support category. The Bundeswehr's Joint Support Service, for example, has been experimenting with the use of AI for an early warning system to support national crisis management. It has also been using AI applications to support warehouse functions.[151] The Medical Command uses civilian AI applications for decision support of doctors in the fields of analytics, diagnostics, and individual therapies.[152] In addition, BWI has been developing BundesWEAR, an app with AI features that offers individual measurements, suggests the best fitting clothing size, and offers online orders for home or barracks deliveries. The Bundeswehr is evaluating the app for future use.[153]

---

146 Ilg, "Militär-Projekt: Mit künstlicher Intelligenz durch Wände schauen."
147 Penney, "Short-range square off."
148 In particular, the Federal Audit Office warned of overspending and argued that development and procurement tasks should not be mixed. For more, see: Wiegold, "Nach Rechnungshof-Kritik: Weniger Projekte im Bundeswehr-Sondervermögen;" https://www.bundeswehr.de/de/organisation/ausruestung-baainbw/ruestungsprojekte/lfk-sys-see-luft-u212a-idas- (last accessed 27 March 2023).
149 "Deutsche Marine: Vertrag für 600 RAM Block 2B unterzeichnet;" https://www.bundeswehr.de/de/ausruestung-technik-bundeswehr/seesysteme-bundeswehr/korvette-k130 (last accessed 27 March 2023).
150 "SeaRAM Anti-Ship Missile Defence System;" https://www.diehl.com/defence/de/produkte/lenkflugkoerper/#ram (last accessed 27 March 2023).
151 "Heimatschutz durch künstliche Intelligenz;" "BWI entwickelt innovative KI-Lösungen für die Bundeswehr."
152 Künstliche Intelligenz im Geschäftsbereich der Bundesregierung, p. 11.
153 "BWI entwickelt innovative KI-Lösungen für die Bundeswehr."

7 Training for Defense AI

"Train as you fight" is a well-established mantra among armed forces. But if you don't know how AI will fight, it is hard to train for it. Furthermore, reconciling yet unknown AI tactics with Germany's Cold War legacy negative contingency "Train to fight so you don't have to" will be an additional challenge specific to the Bundeswehr.

The consequences of defense AI for training are manifold. Armed forces need to address the dynamics that AI-enhanced training systems can generate. They also need to understand to what extent defense AI is improving existing technologies and capabilities that can expand adversarial and allied leeway. In addition, defense AI can produce new – also non-conventional – battlefield behavior that needs to be incorporated by way of training. Defense AI also adds an additional layer of complexity in terms of trust and confidence to underpin successful cooperation. This is not only relevant for so-called manned-unmanned teaming in a traditional "master and servant" context with the unmanned partner following human guidance. It becomes even more important in a future environment in which context and consequence aware reasoning systems operate autonomously (see Box 1).

Right now, the Bundeswehr is in the very early stage of exploring these opportunities and addressing the respective consequences. The MoD's 2019 capstone document on defense AI leaves no doubt that the Bundeswehr needs to put more emphasis on teaching MINT[154] courses and apply the respective skills as qualification criteria for recruiting. The document is also cognizant of the fact that the use of defense AI will lead to greater differentiation among individual career paths and reinforce the need to offer specialist career tracks to attract talent. Among other areas of expertise, future members of the Bundeswehr will need broad and specialized AI expertise, software development know-how, improved MINT knowledge, and interdisciplinary know-how to develop solutions for human-machine interaction, the document contends.[155]

At the joint level the Bundeswehr Command and Staff College (Führungsakademie) is in the process of adapting its curriculum. In view of updating and adapting the curriculum in autumn 2024, stocktaking is currently underway to define the future role defense AI is going to play – both as an instrument for training and education and as a subject that future officers need to understand. As of April 2023, the College will establish and launch a digital open space learning environment. The modular set up could also be used to create interfaces for integrating wargaming, serious gaming, and AI-enhanced training solutions.[156]

154 MINT stands for mathematics, informatics, natural science, and technology.
155 Künstliche Intelligenz. Nutzung im Geschäftsbereich des Bundesministeriums der Verteidigung, p. 21–22.
156 Interviews, 22 February 2023.

In parallel, the University of the Bundeswehr/Hamburg is working on a new AI bachelor's and master's degree course. The program aims at teaching technical basics in the fields of mathematics and informatics as well as adjacent technology areas such as sensors, acoustics, or information technology. In addition, the new program would also embed defense-relevant AI in the broader societal context with building blocks focusing on law, ethics, sociology, and political science.[157]

Against this background, different service-level activities are under way, too:

- The Army's 2019 concept paper put a focus on the role of defense AI in live and constructive training simulations and AI-augmented learning analytics.[158] Consequently, the Army is exploring options to develop an AI-based learning management system that uses data analytics to track individual learning progress and adjusting teaching plans commensurate with individual achievements.[159]
- AI is explored to be used for new tactics, techniques, and procedures related to air defense and dogfight scenarios also with a view on playing computer generated blue and red forces.[160] In addition, the Luftwaffe's AirC2 project (see section 3.1) also has a training component that looks at using AI to train Luftwaffe operators in advancing and improving planning cycles.[161]
- So far, the Navy is not using defense AI for training. The service is, however, mulling the idea of using AI-based training for sea-based signals intelligence. This project would build on the insights gained from the Army's aforementioned learning management system and adapt it to the needs of automated processes on fleet service ships.[162]

In addition to joint and service-level activities different initiatives have been launched to train defense AI algorithms:

- The Luftwaffe, for example, has procured an off-the-shelf software product to teach air power gaming. While the primary purpose was to improve the respective planning and operating procedures, data generated by using the software is also used as a basis to train future defense AI algorithms.[163]
- The Army is working on using simulation-based training with reinforcement learning to train neural networks with the goal of enhancing the autonomous behavior of unmanned systems in battlefield scenarios. Furthermore, the Army also looks at reinforcement learning to train neural networks to command

157 Interview, 25 February 2023.
158 Künstliche Intelligenz in den Streitkräften, p. 12.
159 Interview, 7 March 2023.
160 Interview, 7 March 2023.
161 Interview, 25 March 2022.
162 Interviews, 22 February 2023 and 14 March 2023.
163 Interview, 25 March 2022.

battlefield units. Another focus area of the Army emerges from the need to generate training data for AI-enhanced image recognition.[164] Satisfying the need for high-quality data is also a task that new organizations such as the Army's Systems Center for Digitalization will need to accomplish.[165]

164 Interview, 7 March 2023.
165 Systemzentrum Digitalisierung Dimension Land, para. 335.

8 Conclusion

Currently, German defense AI is a grassroot movement. Motivated people push projects to bring defense AI into the Bundeswehr. Structural and procedural provisions are in place to bring about change. Right now, however, change is first and foremost about closing fundamental capability gaps that emerged during the past three decades. The Bundeswehr may want to operate at the technological edge, but existing shortfalls inhibit Germany's armed forces from doing so. New concepts that leverage emerging technologies are bound back by the resistance of a Bundeswehr bureaucracy solidly grounded in the status quo.

This is no surprise. As we have argued, Germany's handling of defense relevant technologies in general and defense AI in particular is locked-in a "master and servant" logic that is deeply rooted in the country's strategic culture and organizational set up (structural pacifism). Consequently, Germany prioritizes security and technology policy options, which comply with its non-belligerent post-war identity. Domestic socio-political legitimization of the use of force is consistently more important than the impact that can be achieved by using it. This preference will undoubtedly continue to determine political visions on future roles of defense AI and the panorama of technologies deemed acceptable for military use. This narrows future development options and limits the impact of defense AI to an evolutionary trajectory from the start. Since innovation in a tightly regulated defense market relies heavily on capability-pull by the Bundeswehr, its muted technology appetite does not bode well for the defense industry, too.

Consequently, broadening the footprint and strengthening the influence of the defense AI grassroot movement will require the MoD to do some heavy lifting. We see the need to work along four major lines of efforts: sharpen expectations regarding the added value defense AI is expected to deliver; define the role of defense AI in Germany's defense industrial policy; flesh out Germany's international defense AI ambition; and adjust the current system of certifying, qualifying, and approving defense AI solutions.

The Bundeswehr needs to be more precise on how defense AI will boost Bundeswehr capabilities. So far, this link is vague at best, also because today's capability definition must be technology agnostic. This, however, cements preferences for existing technologies and technology concepts. Remedying this shortfall requires the Bundeswehr to be more explicit about what level of maturity defense AI is expected to reach when and to the benefit of which capabilities and missions.

One way of delivering this roadmap is for capability developers to link first, second, and third wave AI to the Bundeswehr's four capability domains. This guidance could be used to delineate Bundeswehr-common and service-specific defense AI capability goals. Based on this overview the Bundeswehr could identify current defense AI shortfalls. Prioritizing mitigation measures can lead to creating a roadmap to address these shortfalls via national or multinational R&T projects and procurement programs.

In so doing, the Bundeswehr should put a premium on fully leveraging ongoing projects using AI for computer generated forces and high-performance simulation environments. This would combine past efforts on modelling and simulation with defense AI to create a new instrument in support of capability development as well as R&T and procurement management. These environments should be linked to existing test and verification units of the Bundeswehr to accelerate concept development and technology insertion. To this purpose, the Army's existing test units should be turned into a permanent Bundeswehr-common test lab to advance defense AI and defense digitalization.

Defense AI has yet to find its proper role in Germany's – non-existent – defense industrial policy. As discussed, the government's capstone document on supporting the security and defense industry calls AI a national key technology but the defense AI concept of the MoD argues that "the Bundeswehr is not the driver of AI-related innovation." These statements are conflicting and detrimental to the overall goal of using AI to improve Germany's competitiveness.

First, few commercial operators match the needs of the Bundeswehr for defense AI that is context and consequence aware while being almost "data abstinent" to deny adversaries the opportunity to dominate the electromagnetic spectrum. By voluntarily ripping itself off the role as a major force to spearhead technology development, the Bundeswehr effectively drops out as a demanding launch customer for cutting-edge defense AI solutions made in Germany.

Second, delegating the capacity to produce innovative defense AI solutions to private industry creates a perfect catch 22 if the majority of Germany's startup AI community considers itself bound by the voluntary civil clause. In addition, there is a mismatch between the interest of commercial companies in seizing current defense business opportunities and private investor's reluctance to fund defense companies given the current ambivalences of the European social taxonomy.[166]

Third, commercial companies working on defense AI thereby using a tech stack also fit for commercial applications might face undue international business development risks as it remains fuzzy how Germany's existing export and dual-use regulation schemes will consider defense AI algorithm exports.

Finally, the Bundeswehr and industry need to specify the "terms and conditions" on which the future defense data ecosystem will operate. This requires striking a balance between the Bundeswehr's interest in unrestricted data access, industrial preferences for data monetization, and the general need to incentivize a data

166 Borchert/Schütz/Verbovzsky, "'Unchain My Heart'," p. 433, 434, 445, 446.

sharing dynamic that also involves stakeholders that have not been involved in generating original data.[167]

The German MoD needs to define its international defense AI ambition. So far, Germany's international defense AI ambition is embryonic at best. This may reflect the fact that the Bundeswehr is only about to explore how to best use defense AI. But the lack of a specific international vision contrasts with the defense leadership role Chancellor Scholz has emphasized since delivering his 2022 Zeitenwende speech and the fact that NATO and the EU are stepping up defense AI activities.

So how could a defense AI framework nation look like? Three points of departure are feasible. First, the Bundeswehr could concentrate on hardware-focused activities to advance multinational defense AI by offering international partners access to its new digitalization centers and high-performance infrastructure that are being established. These infrastructure components could be valuable multinational assets if Germany manages to provide the respective hardware-enabled services on the battlefield. Second, a software-defined framework nation would focus on specific applications. For example, the Bundeswehr could think about red force training with AI-augmented opponents or AI-enhanced red teaming to support multinational capability development. AI-based decision policies that support decentralized multi-agent systems such as FCAS and MGCS could be another option. Third, the Bundeswehr could turn its strong focus on ethics into an asset by combining value-based engineering with simulation to offer partners a new digital test lab for the responsible use of defense AI.

The Bundeswehr needs to reflect upon how to certify, qualify, and approve future defense AI solutions. This is nothing but a daunting task because today's system benefits the so-called original equipment manufacturers (OEM) in their role as effective gatekeepers that can resist modifications of existing defense products.[168] Their powerful role, however, is likely to undermine software-defined defense if software-induced modifications change the overall characteristics of a defense solution for which the OEM – not the software developer – bears ultimate responsibility. Although there is no easy way out of this dilemma an AI-enhanced simulation environment could provide an option to test the characteristics and the performance of future defense AI solutions. The resulting digital twin could be augmented, for example, with mission-critical data gathered during international Bundeswehr operations as well as AI-enhanced red force elements.

167 For more on this aspect, see: Gutachten der Datenethikkommission der Bundesregierung, pp. 145–148.
168 Interview, 14 March 2022.

Literature

"Antwort des Parlamentarischen Staatssekretärs Thomas Silberhorn vom 8. Dezember 2020", Schriftliche Fragen mit den in der Woche vom 7. Dezember 2020 eingegangenen Antworten der Bundesregierung, Drucksache des Deutschen Bundestags 19/25159, 11. Dezember 2020, S. 83, https://dserver.bundestag.de/btd/19/028/1902816.pdf (last accessed 27 March 2023).

"Big Data" und Software zur Vorhersage von "Krisen" bei der Bundeswehr. Antwort der Bundesregierung, Drucksache des Deutschen Bundestags 19/3459, 19 July 2018 https://dserver.bundestag.de/btd/19/034/1903459.pdf (last accessed 27 March 2023).

"BWI entwickelt Lösungen mit künstlicher Intelligenz für die Bundeswehr", Europäische Sicherheit und Technik, 27 January 2022, https://esut.de/2022/01/meldungen/32112/bwi-entwickelt-loesungen-mit-kuenstlicher-intelligenz-fuer-die-bundeswehr/ (last accessed 27 March 2023).

"Deutsche Marine: Vertrag für 600 RAM Block 2B unterzeichnet," Europäische Sicherheit und Technik, 11 November 2022, https://esut.de/2022/11/meldungen/37952/deutsche-marine-vertrag-fuer-600-ram-block-2b-unterzeichnet/ (last accessed 27 March 2023).

"Heimatschutz durch künstliche Intelligenz. Die Bundeswehr auf dem Weg in die Zukunft," Bundeswehr, 14 April 2021, https://www.bundeswehr.de/de/aktuelles/meldungen/heimatschutz-durch-kuenstliche-intelligenz-bundeswehr-zukunft-5054820 (last accessed 27 March 2023).

"Hensoldt equips Bundeswehr NH90 helicopter with state-of-the-art protection systems," European Defence Review, 21 January 2022, https://www.edrmagazine.eu/hensoldt-equips-bundeswehr-nh90-helicopter-with-state-of-the-art-protection-systems (last accessed 27 March 2023).

"Hensoldt präsentiert Radarwarner auf KI-Basis," hartpunkt.de, 14 May 2019, https://www.hartpunkt.de/hensoldt-praesentiert-radarwarner-auf-ki-basis/ (last accessed 27 March 2023).

"Kann Künstliche Intelligenz wertekonform sein? VDE SPEC als Grundlage künftiger Entwicklungen," VDE Press Release, 25 April 2022, https://www.vde.com/de/presse/pressemitteilungen/ai-trust-label (last accessed 27 March 2023).

"Live-Demonstration Aufklärung im 'Gläsernen Gefechtsfeld'," Europäische Sicherheit und Technik, 22 December 2021, https://esut.de/2021/12/meldungen/31593/live-demonstration-aufklaerung-im-glaesernen-gefechtsfeld/ (last accessed 27 March 2023).

"SeaRAM Anti-Ship Missile Defence System," Naval Technology, 30 June 2014, https://www.naval-technology.com/projects/searam-anti-ship-missile-defence-system/ (last accessed 27 March 2023).

"Test- und Versuchskräfte in Munster aufgestellt," Press Release, Bundeswehr, 17 December 2020, https://www.bundeswehr.de/de/organisation/heer/aktuelles/test-und-versuchskraefte-in-munster-aufgestellt-4960224 (last accessed 27 March 2023).

"Truppe setzt auf Zukunftstechnologie 'Künstliche Intelligenz'", Bundeswehr-Journal, 3 January 2021, https://www.bundeswehr-journal.de/2021/truppe-setzt-auf-zukunftstechnologie-kuenstliche-intelligenz/ (last accessed 27 March 2023).

"Von Big Data bis KI. Zweite Ausbaustufe des Gemeinsamen Lagezentrums CIR", Bundesministerium der Verteidigung, 2. September 2020, https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/aktuelles/von-big-data-bis-ki-zweite-ausbaustufe-des-glz-cir-1826878 (last accessed 27 March 2023).

"Wie KI bei der Vorhersage des Weltraumwetters hilft," Gloem.de, 7 December 2021, https://www.golem.de/news/anzeige-wie-ki-bei-der-vorhersage-des-weltraumwetters-hilft-2112–161343.html (last accessed 27 March 2023)

Artificial Intelligence Strategy (Berlin: The Federal Government, 2018), https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie_engl.pdf&cid=729 (last accessed 27 March 2023).

Artificial Intelligence Strategy of the German Federal Government. 2020 Update (Berlin: The Federal Government, 2020), https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Fortschreibung_KI-Strategie_engl.pdf&cid=955 (last accessed 27 March 2023).

Autorenteam Luftwaffe, "Der Einfluss künstlicher Intelligenz bei er Führung von Luftoperationen der Zukunft", Wehrtechnik, II/2021, pp. 65–68.

Azzano, Massimo et al., "The responsible use of artificial intelligence in FCAS. An initial assessment", FCAS Forum, February 2020, https://www.fcas-forum.eu/articles/responsible-use-of-artificial-intelligence-in-fcas (last accessed 27 March 2023).

Biess, Frank, Republik der Angst. Eine andere Geschichte der Bundesrepublik (München: Rowohlt, 2019).

Bock, Christian und Matthias Schmarsow, "Gedanken zum Einsatz von Künstlicher Intelligenz beim militärischen Frühen und Entscheiden", in Norbert Lammert und Wolfgang Koch (Hrsg.), Bundeswehr der Zukunft. Verantwortung und Künstliche Intelligenz (Berlin: Konrad-Adenauer-Stiftung, 2023), pp. 138–158.

Borchert, Heiko, "The Rocky Road to Networked and Effects-Based Expeditionary Forces: Military Transformation in the Bundeswehr", in Terry Terriff, Frans Osing, and Theo Farrell (eds.), A Transformation Gap? American Innovations and European Military Change (Stanford: Stanford University Press, 2010), pp. 83–107.

Borchert, Heiko, Christian Brandlhuber, Armin Brandstetter, and Gary S. Schaal, Free Jazz on the Battlefield. How GhostPlay's AI Approach Enhances Air Defense. DAIO Study 22/03 (Hamburg: Defense AI Observatory, 2022), https://defenseai.eu/daio_study2203 (last accessed 27 March 2023).

Bousquet, Antoine, The Scientific Way of Warfare. Order and Chaos on the Battlefields of Modernity (London: Hurst & Company, 2022).

Brendecke, Jan-Wilhelm, Thomas Doll, Daniel Kallfass, "Der Führungsprozess von morgen. Wie Künstliche Intelligenz en Führungsprozess beschleunigen kann", Europäische Sicherheit und Technik, 69:10 (October 2020), pp. 68–71.

Burri, Regula Valérie, "Imaginaries of Science and Society: Framing Nanotechnology Governance in Germany and the United States," in Sheila Jasanoff and Sang-Hyun Kim (eds.) Dreamscapes of Modernity – Sociotechnical Imaginaries and the Fabrication of Power (Chicago/London: The University of Chicago Press, 2015), pp. 233–253.

BWI, "Generalinspekteur lässt sich KI-gestützte Aufklärung vorführen," press release, 7 December 2022, https://www.bwi.de/magazin/artikel/generalinspekteur-laesst-sich-ki-gestuetzte-aufklaerung-vorfuehren (last accessed 27 March 2023).

Dani, Enrico, "Digitalisierung landbasierter Operationen. Sachstand und Weiterentwicklung", Europäische Sicherheit und Technik, 71:2 (February 2022), pp. 40–43.

Datenstrategie GB BMVg (Berlin: Bundesministerium der Verteidigung, 2021).

Dean, Sindey E., "Main Ground Combat System (MGCS): A Status Report," European Security & Defence, 23 January 2023, https://euro-sd.com/2023/01/articles/29122/main-ground-combat-system-mgcs-a-status-report/ (last accessed 27 March 2023.

Digitalisierung von Landoperationen (Stausberg: Kommando Heer, 2017).

Eberle, Jakub, Discourse and Affect in Foreign Policy: Germany and the Iraq War (New York: Routledge, 2019).

Ehlke, Tobias, "Interview mit Generalleutnant Dr. Ansgar Rieks, Stellvertreter des Inspekteurs der Luftwaffe", cpm Forum für Rüstung, Streitkräfte und Sicherheit, 3/2021, pp. 16–19.

Engen, Robert C., When the Teeth Eat the Tail, A Review of Canada's Defence Artificial Intelligence. DAIO Study 23/09 (Hamburg: Defense AI Observatory, 2023), https://defenseai.eu/daio_study2309 (last accessed 27 March 2023)

Erster Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung (Berlin: Bundesministerium der Verteidigung, 2019), https://www.bmvg.de/de/aktuelles/bericht-digitale-transformation-geschaeftsbereich-bmvg-143246 (last accessed 27 March 2023).

Färber, Michael und Lars Bibow, "Die Multi Domain Combat Cloud für die vernetzte Operationsführung", Europäische Sicherheit und Technik, 71:11 (November 2022), pp. 55–58.

Färber, Michael, "Digitalisierung der Bundeswehr," in Norbert Lammert und Wolfgang Koch (Hrsg.), Bundeswehr der Zukunft. Verantwortung und Künstliche

Intelligenz (Berlin: Konrad Adenauer Stiftung, 2023), pp. 224–235, https://www.kas.de/de/bundeswehr-der-zukunft (last accessed 27 March 2023).

Fleischmann, Armin, "Das Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum: 'Unser Beitrag als Treiber der Digitalisierung der Bundeswehr'," in CIR 2.0: Von der Idee zur Dimension (Bonn: cpm Communication PresseMarketing, 2022), pp. 34–38, https://www.bundeswehr.de/resource/blob/5519316/29945909e7ed8cc36f2c9ff4ecd53186/download-sonderheft-cir-2–0-data.pdf (last accessed 27 March 2023).

Förderung von Künstlicher Intelligenz für die Bundeswehr. Antwort der Bundesregierung. Drucksache des Deutschen Bundestags 19/10803, 11 June 2019, https://dserver.bundestag.de/btd/19/108/1910803.pdf (last accessed 27 March 2023).

Future Operating Environment 2035 (Berlin: Bundesministerium der Verteidigung, 2019).

Gäbelein, Wolfgang, "Die Bundeswehr und das Gefechtsfeld der Zukunft: Entwicklungsperspektiven in Verbindung mit Künstlicher Intelligenz aus der Sicht des Verteidigungsplaners", in Norbert Lammert and Wolfgang Koch (eds.), Bundeswehr der Zukunft. Verantwortung und Künstliche Intelligenz (Berlin: Konrad-Adenauer-Stiftung, 2023), pp. 120–137.

Gesetz über die Feststellung des Bundeshaushaltsplans für das Haushaltsjahr 2023, Einzelplan 14, Bundesgesetzblatt Teil I, Nr. 54, 19 December 2022, pp. 2485, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl122s2485.pdf (last accessed 27 March 2023).

Gesetz zur Finanzierung der Bundeswehr und zur Errichtung eines "Sondervermögens Bundeswehr" und zur Änderung der Bundeshaushaltsordnung, Bundesgesetzblatt 2022, Teil 1, Nr. 23, 6 July 2022, p. 1030, https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%271034878%27%5D&skin=pdf&tlevel=-2&nohist=1&sinst=0E04B990 (last accessed 27 March 2023).

Grundgesetz für die Bundesrepublik Deutschland vom 19. Dezember 2022, Bundesgesetzblatt I S. 2478, https://www.bundestag.de/gg (last accessed 27 March 2023).

Gutachten der Datenethikkommission der Bundesregierung (Berlin: Datenethikkommission der Bundesregierung 2019), https://www.bundesregierung.de/breg-de/service/publikationen/gutachten-der-datenethikkommission-langfassung-1685238 (last accessed 27 March 2023).

Heiming, Gerhard, "Ausschüsse segnen Wirtschaftsplan zum Sondervermögen ab," Europäische Sicherheit und Technik, 2 June 2022, https://esut.de/2022/06/meldungen/34634/ausschuesse-segnen-wirtschaftsplan-zum-sondervermoegen-ab/ (last accessed 27 March 2023).

Hofstetter, Yvonne and Joseph Verbovszky, How AI Learns the Bundeswehr's "Innere Führung." Value-Based Engineering with IEEE7000TM-2021. DAIO Study 23/10 (Hamburg: Defense AI Observatory, 2023), https://defenseai.eu/daio_study2310 (last accesed 27 March 2023)

Ilg, Peter, "Militär-Projekt: Mit künstlicher Intelligenz durch Wände schauen," heise online, 18 July 2022, https://www.heise.de/news/Militaer-Projekt-Mit-kuenstlicher-Intelligenz-durch-Waende-schauen-7182283.html (last accessed 27 March 2023).

Inspekteur der Marine – Absicht 2022 (Rostock: Marinekommando, 2022), https://www.bundeswehr.de/de/organisation/marine/aktuelles/inspekteur-marine-absicht-2022–5400502 (last accessed 27 March 2023).

Jasanoff, Sheila, "Future Imperfect: Science, Technology, and the Imaginations of Modernity," in Sheila Jasanoff and Sang-Hyun Kim (eds.), Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power (Chicago/London: The University of Chicago Press, 2015), pp. 1–33.

Jensen, Benjamin M., Christopher Whyte, and Scott Cuomo, Information in War. Military Innovation, Battle Networks, and the Future of Artificial Intelligence (Washington, DC: Georgetown University Press, 2022).

Kahn, Lauren A., Risky Incrementalism Defense AI in the United States. DAIO Study 23/07 (Hamburg: Defense AI Observatory, 2023), https://defenseai.eu/daio_study2307 (last accessed 15 March 2023).

KI-Startups in Deutschland. Eine Untersuchung zu Unternehmensgründungen im Bereich Künstliche Intelligenz (Berlin: Bundesministerium für Wirtschaft und Klimaschutz, 2022), https://www.de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-download-ki-startups.html (last accessed 27 March 2023).

Kober, Klemens and Torben Schütz, "Den Weltraum ordnen. Zukunftsvorstellungen und (New) Space Governance, in Moritz Brake, Enrico Fels, Antje Nötzold,

and Andrea Rotter (eds.), Strategischer Wettbewerb im Weltraum. Politik, Sicherheit und Wirtschaft im All (Wiesbaden: Springer VS, forthcoming).

Koch, Wolfgang, "Elements of an Ethical AI Demonstrator for Responsibly Designing Defence Systems," 25th International Conference on Information Fusion, 4–7 July 2022, https://ieeexplore.ieee.org/document/9841387 (last accessed 27 March 2023).

Krieg der Zukunft?! Operative Herausforderungen des Multi-Domain Battlefield für die Bundeswehr. Lehrgang Generalstabs-/Admiralstabsdienst (LGAN) 2020 – Studienphase. Hintergrundinformation Presse (Hamburg: Führungsakademie der Bundeswehr, 2022), https://www.bundeswehr.de/de/organisation/weitere-bmvg-dienststellen/fuehrungsakademie-der-bundeswehr/mediathek/ueber-krieg-der-zukunft-5462696 (last accessed 27 March 2023

Künstliche Intelligenz im Geschäftsbereich der Bundesregierung. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Anke Domscheit-Berg, Dr. Petra Stitte, Nicole Gohlke, weiterer Abgeordneter und er Fraktion DIE LINKE, Bundestag Drucksache 20/430, 14 January 2022, https://dserver.bundestag.de/btd/20/004/2000430.pdf (last accessed 27 March 2023)

Künstliche Intelligenz in den Landstreitkräften. Ein Positionspapier des Amts für Heeresentwicklung (Köln: Amt für Heeresentwicklung, 2019).

Künstliche Intelligenz. Nutzung im Geschäftsbereich des Bundesministeriums der Verteidigung (Berlin: BMVg, 2019).

Layton, Peter, Evolution not Revolution. Australia's Defence AI Pathway. DAIO Study 22/02 (Hamburg: Defense AI Observatory, 2022), https://defenseai.eu/daio_study2202 (last accessed 27 March 2023).

Meerveld, H.W., R.H.A. Lindelauf, E.O. Postma, and M. Postma, "The irresponsibility of not using AI in the military", Ethics and Information Technology, 25:1 (January 2023), article 14, https://link.springer.com/article/10.1007/s10676–023–09683–0 (last accessed 27 March 2023)

Mehr Fortschritt wagen. Koalitionsvertrag 2021–2025 (Berlin: SPD/Bündnis90/Die Grünen/FDP, 2021), https://www.bundesregierung.de/breg-de/aktuelles/koalitionsvertrag-2021–1990800 (last accessed 27 March 2023).

Müller, Björn, "Künstliche Intelligenz in der Bundeswehr," Loyal, 8. November 2021, https://www.reservistenverband.de/magazin-loyal/kuenstliche-intelligenz-in-der-bundeswehr/ (last accessed 27 March 2023).

Operative Leitlinien für die Streitkräfte (Berlin: Generalinspekteur, 2022).

Payne, Kenneth, Bright Prospects – Big Challenges. Defence AI in the United Kindgom. DAIO Study 22/04 (Hamburg: Defense AI Observatory, 2022), https://defenseai.eu/daio_study2204 (last accessed 27 March 2023).

Penney, Stewart, "Short-range square-off," FlightGlobal, 27 June 2000, https://www.flightglobal.com/short-range-square-off/32654.article (last accessed 27 March 2023).

Rieks, Ansgar, "Digitalisierung der Streitkräfte: Ein (nicht nur) technischer Blick," in Norbert Lammert and Wolfgang Koch (eds.), Bundeswehr der Zukunft. Verantwortung und Künstliche Intelligenz (Berlin: Konrad-Adenauer-Stiftung, 2023), pp. 102–119.

Science and Technology Trends 2023–2043. Across the Physical, Biological, and Information Domains. Volume 2 (Brussels: NATO Science and Technology Organization, 2023), https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf (last accessed 27 March 2023).

Schurad, Dirk, "Mit künstlicher Intelligenz der Zukunft auf der Spur", Hardthöhen-Kurier, 38:4 (August 2018), S. 10–12, https://www.hardthoehenkurier.de/hhkemags/fullhhkemags/2018–04/index_20.html#page=11 (last accessed 27 March 2023).

Soare, Somina, Pavneet Singh and Meia Nouwens, Software-defined Defence: Algorithms at War (London: IISS, 2023), https://www.iiss.org/blogs/research-paper/2023/02/software-defined-defence (last accessed 27 March 2023).

Stengel, Frank A., The Politics of Military Force: Antimilitarism, Ideational Change and Post-Cold War German Security Discourse (Ann Arbor: University of Michigan Press, 2020).

Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie (Berlin: Bundesregierung, 2019), https://www.bmwk.de/Redaktion/DE/Downloads/S-T/strategiepapier-staerkung-sicherits-und-verteidigungsindustrie.html (last accessed 15 March 2023).

Strategische Leitlinie Digitalisierung (Berlin: Bundesministerium der Verteidigung, 2017).

Systemzentrum Digitalisierung Dimension Land (Berlin: Bundesministerium der Verteidigung, 2022):

Verbovszky, Joseph, German Structural Pacifism. PhD Dissertation (Munich: University of the Bundeswehr, 2022).

Wehrwissenschaftliche Forschung Jahresbericht 2020. Wehrwissenschaftliche Forschung für deutsche Streitkräfte (Bonn: Bundesministerium der Verteidigung, 2021).

Welchering, Peter, "Von der Bundeswehr zur digitalen Verteidigungsarmee?", Deutschlandfunk, 11 February 2023, https://www.deutschlandfunk.de/it-soldaten-das-software-defined-defence-konzept-soll-die-bundeswehr-umkrempeln-dlf-68c615bf-100.html (last accessed 27 March 2023).

Welchering, Peter, "Wie KI-Systeme die militärische Ausbildung verändern", Deutschlandfunk, 2. Februar 2022, https://www.deutschlandfunk.de/kuenstliche-intelligenz-wie-ki-systeme-die-militaerische-100.html (last accessed 27 March 2023).

Wie kämpfen Landstreitkräfte künftig? Thesenpapier (Strausberg: Kommando Heer, 2017).

Wiegold, Thomas, "Nach Rechnungshof-Kritik: Weniger Projekte im Bundeswehr-Sondervermögen," Augen geradaus!, 28 October 2022, https://augengeradeaus.net/2022/10/nach-rechnungshof-kritik-weniger-projekte-im-bundeswehr-sondervermoegen/ (last accessed 27 March 2023).

Wiegold, Thomas, "Studie fürs 'gläserne Gefechtsfeld': Drohnen und KI", Augen geradeaus?, 14 April 2019, https://augengeradeaus.net/2019/04/studie-fuers-glaeserne-gefechtsfeld-drohnen-ki/ (last accessed 27 March 2023).

Defense AI Observatory Studies

23|12 Heiko Borchert, Torben Schütz, and Joseph Verbovszky, Master and Servant. Defense AI in Germany

23|11 Katarzyna Zysk, High Hopes Amid Hard Realities. Defense AI in Russia

23|10 Yvonne Hofstetter and Joseph Verbovzsky, How AI Learns the Bundeswehr's "Innere Führung." Value-Based Engineering with IEEE7000™-2021

23|09 Robert C Engen, When the Teeth Eat the Tail: A Review of Canada's Defence Artificial Intelligence

23|08 Çağlar Kurç, Enabling Technology of Future Warfare. Defense AI in Turkey

23|07 Lauren A. Kahn, Risky Incrementalism. Defense AI in the United States

22|06 Yvonne Hofstetter, Wie KI Innere Führung lernt. Wertbasierte Technik mit IEEE7000™-2021

22|05 Andrea Gilli, Mauro Gilli, and Ivan Zaccagnini, Exploring the Benefits of a New Force Enabler: Defense AI in Italy

22|04 Kenneth Payne, Bright Prospects – Big Challenges. Defense AI in the United Kingdom

22|03 Heiko Borchert, Christian Brandlhuber, Armin Brandstetter, and Gary S. Schaal, Free Jazz on the Battlefield. How GhostPlay's AI Approach Enhances Air Defense

22|02 Peter Layton, Evolution not Revolution. Australia's Defence AI Pathway

21|01 Heiko Borchert, Torben Schütz, Joseph Verbovszky, Beware the Hype. What Military Conflicts in Ukraine, Syria, Libya, and Nagorno-Karabakh (Don't) Tell Us About the Future of War

Defense AI Observatory

www.defenseai.eu