Paper
03

Leveraging the Defense Metaverse

Unlocking the Power of Artificial Intelligence for Force Development

Dr. Heiko Borchert
Co-Director,
Defense AI Observatory, Germany

Torben Schütz
Research Fellow,
Defense AI Observatory, Germany

Dr. Christian Brandlhuber
Co-Founder and CTO,
21Strategies, Germany

ABSTRACT

Leveraging the potential of artificial intelligence (AI) is a pressing imperative for militaries as operational scenarios evolve and the need for adaptable capabilities becomes paramount. This paper delves into AI's value proposition and introduces the innovative concept of the "defense metaverse." The defense metaverse concept constructs a dynamic digital twin of the battlespace, fusing AI and sophisticated models to test and refine tactical concepts. The integration of AI-driven tactics generated using the defense metaverse stands to bridge critical gaps between future concepts and technology, leading to superior force development and force readiness. Drawing attention to the success of the GhostPlay project, which pioneers AI-augmented tactics for air defense and aggressor swarms, this paper identifies three vital areas for militaries to prioritize in augmenting capability using AI: experimentation, training, and infrastructure. Establishing a culture of experimentation, coupled with immersive training using non-conventional tactics, will be pivotal in realizing the potential of AI in developing future military capability. To this end, pursuing an "open" defense metaverse approach harnessing multi-partner collaboration while safeguarding strategic interests will be essential.

INTRODUCTION

Amidst the evolving contours of complex operational environments, the integration of artificial intelligence (AI) presents an array of transformative prospects for militaries. This paper offers a nuanced exploration of these prospects and the introduction of an innovative concept—the "defense metaverse." The integration of AI-driven tactics generated using the defense metaverse stands to bridge critical gaps between future concepts and technology to support superior force development and force readiness. The paper begins laying the contextual groundwork by dissecting the challenges faced by militaries in delineating AI's intrinsic value. Considering the backdrop of challenges presented by anti-access strategies, Multi-Domain Operations, and force integration imperatives, the defense metaverse is explored as a construct envisioning a digital twin of the battlespace brought to life through a fusion of AI and advanced modeling. The paper discusses the strides achieved by the GhostPlay project in augmenting tactical paradigms assisted by AI and offers a prelude to future possibilities. Finally, pivoting the discussion to the importance of experimentation, training, and the essential infrastructure that underpins the defense metaverse, this paper advocates for an "open" approach to collaboration. Cultivating a multi-partner digital ecosystem that dynamically offers open interfaces for training and evaluating the tactical effects of AI systems may unleash the very powerful potential of the defense metaverse.

AUGMENTING CAPABILITY: DELINEATING A ROLE FOR AI

Why should militaries use artificial intelligence (AI), and what is AI expected to deliver for them? These questions might surprise given the current hype around AI. But they must not, because most armed forces struggle to properly define the value proposition meant to drive their journey into defense AI.[1] This is problematic because the lack of a clearly set purpose and adequate metrics makes it hard to define how AI can augment military capabilities, what has been achieved, where shortfalls endanger mission success, and what should be done nationally or in tandem with partners. There are different ways to look at defense AI. Militaries can consider using AI to improve existing technologies and use them more effectively and efficiently. This seems a safe bet. Indeed, many countries adopt this incremental help to

1 This is the finding of a series of case studies commissioned by the Defense AI Observatory (DAIO) on the current state of play regarding defense AI. Until today DAIO has published country studies on Australia, Canada, China, Finland, Israel, Italy, Russia, Sweden, Turkey, the UK, and the United States. Forthcoming studies will cover Denmark, Estonia, France, Greece, India, Japan, the Netherlands, Singapore, South Korea, Spain, Taiwan, and the UAE. All studies are available from https://defenseai.eu/english#publikationen.

mitigate the challenges of concepts and technology maturation – but it risks being out of tune with some fundamental strategic challenges.

First, the conflict picture is changing (Ministry of Defence, 2018; Allen et al., 2021; Barno and Bensahel 2021). Sensing and the delivery of precision effects are growing in reach and depth to constitute anti-access/area denial challenges (A2AD). As it becomes more difficult to ensure one's own freedom of maneuver and intervene in adversarial air space, "no-go areas" emerge that are too risky for anyone to operate in (Krepinevich, 2015). The risk of losing airmen and air assets is increasing, prompting a discussion about how to best distribute force and use uncrewed assets in response. With uncrewed assets, mass is back in business as it offers an option to sustainably overwhelm adversaries. At the same time, mass also raises tricky questions related to force coordination, personnel recruitment and training, the interplay with legacy systems, and industrial production capacities needed to deliver uncrewed assets commensurate with battlefield attrition rates. In parallel, decision-making becomes more complex, characterized by the demands of fast-paced hyper war (Allen and Husain, 2017) on the one hand and glacially evolving hybrid threats (Mazzarr, 2015; Hybrid CoE, 2019) on the other hand. This makes it ever more important to balance the need to swiftly adapt decision-making to the demands of the operating environment with growing requirements to augment predictive capacities to anticipate adversarial courses of action.

With uncrewed assets, mass is back in business as it offers an option to sustainably overwhelm adversaries.

Second, in response to this conflict picture, the Multi-Domain Operations (MDO) concept gains in prominence. It strives to seamlessly integrate force elements across all domains (land, sea, air, space, and cyberspace) to deliver superior effects (JAPCC, 2019). MDO leverages the idea of Mosaic Warfare (Graystead, 2019; Haystead, 2020), which argues in favor of radically "deconstructing" force elements to evade adversarial A2AD capabilities and flexibly reconfigure them to advance agility and improve lethality. Among many other aspects, this concept also requires a fundamental rethink of centralized and hierarchical command and control (C2) approaches to the benefit of decentralization and emergence.

Third, these developments reinforce the old wisdom that integration is essential for military effectiveness (Brooks and Stanley, 2007; Borchert et al., 2021). Integration is key for air power as many nations are interested in accessing fifth and sixth generation fighter capabilities parallel to expanding cooperation on uncrewed aerial vehicles with partners. However, absent adequate doctrinal paradigms and concepts of operations, formidable aerospace technology will not

provide the capability gains air forces hope for. In addition, the concepts-technology integration strand must be addressed hand in hand with national modernization and replacement agendas, as old and new assets must play together during the transition phase. This prompts the question about the roles old and new systems are expected to play and the mechanisms needed to ensure interoperability among all elements of the C4ISTAR[2] value chain. Key to delivering air power, this value chain is also vulnerable to adversarial progress in shaping and potentially dominating the electromagnetic spectrum, thus prompting new requirements for force coordination beyond traditional communication links.

Against this background, we contend that air forces should envision using AI to provide superior force development methods to advance tactical versatility by creating a defense metaverse.

DEFENSE METAVERSE AND AI TACTICS

Originally, Neal Stephenson (1992) conceived the metaverse as a three-dimensional virtual space for humans to interact with software agents. Decades later, so-called digital twins, or digitized copies of physical assets, provided the first tangible manifestation of this idea. Today, digital twins have become a popular technology underpinning the fourth industrial revolution.

The defense metaverse builds on this idea by establishing a digital twin of the battlefield composed, for example, of urban and rural infrastructure, terrain, vegetation, weather conditions, realistic sensor and effector models, and other features – complemented with a self-learning multi-agent AI red team. This combination aims to create a – proverbial – digital playground for air forces to test concepts, design ideas, and plans for future defense systems against its own analysis but also against a variety of AI-based non-conventional challengers.

Compared to traditional analytical simulation, the added value of the defense metaverse is threefold. First, the defense metaverse seamlessly integrates strategic, operational, and tactical levels of analysis in one digital environment to realistically illustrate effects and their impact on sensor-to-shooter webs. This is important as traditional simulation models focus only on one layer and model assumptions accordingly. As a result, simulation results depend on these pre-specified assumptions and thus only confirm what is already known. By contrast, the defense metaverse – thanks to its permeability – overcomes this lock-in effect and produces simulation results that are much more realistic.

2 Command, Control, Computers, Communications, Intelligence, Surveillance, Target Acquisition, and Reconnaissance.

Second, state-of-the-art simulation methods have limits. Monte Carlo simulations, for example, used to conduct tactical analyses, do not provide single-case transparency and are not able to systematically capture tactical benefits or flaws arising from specific defense systems or capabilities. In addition, scripted scenarios cannot offer large and representative sets of scenarios as efforts to do so quickly become disproportionate. Therefore, an optimal simulation environment needs to be able to perform both tasks. The defense metaverse fulfills this requirement as it presents the results of larger-scale runs as statistical aggregates of individual scenarios.

Third, AI-enabled intelligent red teams significantly enlarge the scenario envelope. Today, so-called "third wave AI," which is context and consequence-aware as *Table 3.1* illustrates, is not yet ready for the battlefield.[3] Nonetheless, it already offers force planners the opportunity to create a broad variety of scenarios – including high-intensity combat – featuring coordinated action of large groups of challengers across multiple domains. This creates a dynamic that entices learning by interacting with adversarial forces that do not behave as pre-scripted software agents. Instead, they consider the context in which they operate, factor in the consequences of their own actions, can anticipate adversarial action, and behave accordingly.

Handcrafted Knowledge	**Correlation Learning**	**Contextual Reasoning**
First Wave AI	Second Wave AI	Third Wave AI
Human experts construct expert systems that capture the specialized knowledge of experts in rules that the system can apply	Statistical and probabilistic methods are used to train neural networks to perform classification and prediction tasks	Computing systems have full situational awareness and reason in context, i.e., they understand the consequences of their action
Military Example • Inventory control	Military Example • Image recognition • Semantic analysis	Military Example • AI tactics • Full machine autonomy

Table 3.1: Three Waves of Artificial Intelligence (Source: DARPA, *n.d.;* NATO STO 2023).

3 Third wave AI techniques like (deep) reinforcement learning and multi-agent reinforcement learning, which enable cooperative team tactics, have been remarkably successful in idealized environments and perfect information games. Nonetheless they are yet in the early stages of adoption. For example, training these systems to learn policies that are stable remains challenging. In addition, several aspects relevant for the deployment – for example, the need to reduce vulnerabilities of team policies due to adversarial deception or malign behavior of team members – constitute important aspects of ongoing research activities.

Is this defense metaverse science fiction? No. The authors of this paper are engaged in developing it with GhostPlay, a defense capability and technology development project funded by the Digitalization and Technology Research Center of the Bundeswehr. Since its inception in September 2021, GhostPlay has demonstrated that the defense metaverse discussed here is feasible and delivers surprising results.

GhostPlay uses the defense metaverse to develop algorithms that trigger novel battlefield behavior at the tactical level. In so doing, GhostPlay "models novel AI-based solutions for air defense and aggressor swarms that learn how to outperform each other" (Borchert et al., 2022). To this purpose, GhostPlay explores how AI can augment a legacy ground-based air defense system (GBAD), like the German Gepard anti-aircraft artillery (AAA) platform. In so doing, GhostPlay goes beyond the state of the art. GhostPlay no longer only looks at improving individual processing steps in the observe-orient-decide-act cycle (OODA). Instead, it establishes a control regime that accelerates decision-making and reduces sensor-to-shooter latency. Unlike past solutions, GhostPlay's agents are also no longer centrally coordinated but operate in a decentralized mode using specific "rules-of-encounter" and reinforcement learning protocols to exchange information and achieve a common objective in cooperation with partners (multi-agent cooperation).

As a result, GhostPlay decision policies indicate which actions need to be taken, for example, to drastically improve the Gepard's performance. Currently, an aggressor would require around ten uncrewed aerial vehicles (UAV) to saturate an AAA system. But, simulation results suggest that attacking a GhostPlay-enhanced AAA requires the aggressor swarm to grow to sixty members to achieve the same result. In addition, the system also shows impressive collaborative behavior. In 9,864 out of 10,000 scenarios, a group of ten AAA platforms acting as a team could implement effective protection against a massive attack of a 105-member aggressor swarm without suffering more than three losses. This outcome was possible because the AAA team has learned how to compensate for the loss of single platforms by regrouping and reorganizing tasks among the remaining team members (Borchert et al., 2022).

At the time of writing, work on AI-augment swarm tactics to attack a GBAD constellation is still ongoing. Preliminary results suggest that tactical versatility can significantly improve mission success, i.e., GBAD destruction. For example, an aggressor swarm consisting of eight Switchblade 600 air-launched effectors deployed from a helicopter can overwhelm a Gepard-like defender when fully exploiting terrain features (e.g., hiding in ground clutter, flying at the height of treetops, attacking from the direction of the sunlight to escape passive electro-optical sensors), using flight trajectories that lead to simultaneous attacks from opposite directions to maximally exploit the GABD's physical latency, as well as varying the flight tempo and the flight path during the mission. While this might sound unsurprising to humans, the point is that these tactics have been self-learned

– not pre-scripted – and emerged from the fact that red aggressor swarms have perfectioned the art of exploiting GBAD shortcomings.[4]

CRITICAL LINES OF EFFORT

A defense metaverse like GhostPlay that offers sophisticated AI-enhanced non-conventional red teaming bridges today's critical gap between concepts and technologies by offering AI tactics as the missing link. In so doing, the defense metaverse becomes a critical trust-builder: Nobody has yet seen the true potential of sophisticated AI tactics on the battlefield. Therefore, experimentation, testing, and validation with the help of the defense metaverse can illustrate if AI tactics meet expectations. In addition, as an analytical simulation, the defense metaverse provides value to identifying design flaws of new defense systems as early as possible, thus mitigating the risk of false investments and erroneous product developments. It also helps avoid sunk costs by exploring how legacy systems can be augmented to meet new mission demands, as *Figure 3.1* illustrates below.

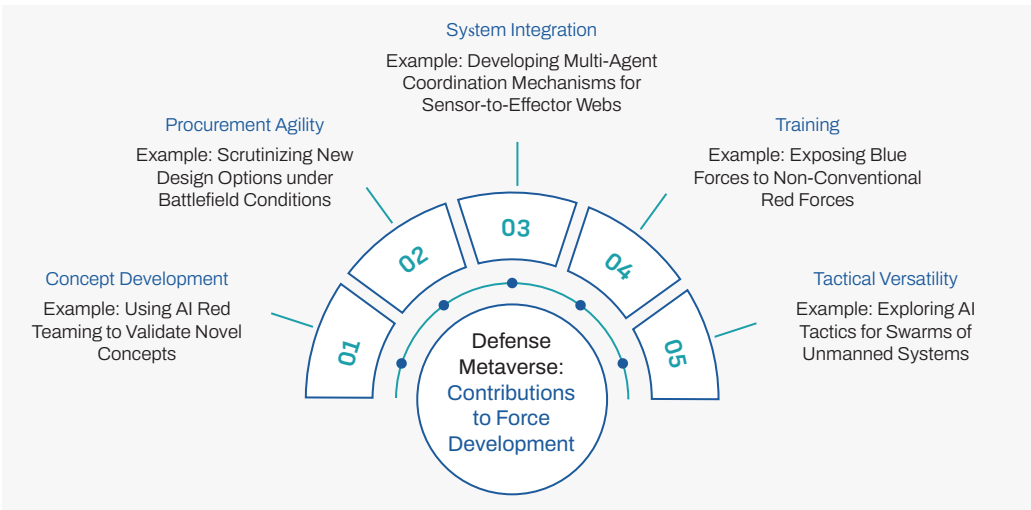

Figure 3.1: Supporting Force Development with the Defense Metaverse

4 The AI-augmented GBAD, in turn, has developed counter-tactics, but these need to mature before they can be discussed.

It goes without saying, however, that the defense metaverse as a playground for new AI tactics is but a digital twin of reality, albeit very powerful. Thus, results need to be transposed into reality. In this regard, we offer three observations on mindsets, training, and infrastructure that military forces should address when exploring the opportunities of the proposed defense metaverse.

First, Jensen et. al (2022) convincingly argue that military innovation related to information technology requires structures that ensure information flows and information interchange as well as "resonance," defined as "the degree to which prevailing ideas about how war is fought and problem-solving routines accommodate new information flows." Acknowledging the existence of these two innovation barriers is crucial when questioning long-held assumptions, such as the proposition to replace hierarchical C2 systems with decentralized AI-enhanced solutions, for example.

One prerequisite is an organizational culture in which experimentation constitutes the norm rather than a seldom-used instrument. Combining test labs of companies and research institutes with experimental units of the armed forces is as important as setting aside dedicated budgets. In addition, leadership formation must nurture daringness as an essential cultural trait. In this regard, experiments provide fertile ground to challenge users operating in familiar conceptual and technological comfort zones.

Moreover, experimentation needs to go hand in hand with training. The defense metaverse offers a unique opportunity to expose air forces to non-conventional red teams using tactics that have not yet been seen but may generally be feasible considering adversarial capabilities. As these red forces decipher how forces to be trained operate, they can constantly exploit their shortfalls and thus ignite a learning dynamic that depends less on pre-staged curricula but on adversarial surprise and initiative. Again, the success of this approach presupposes a level of intellectual curiosity that feels comfortable with non-conventional challenges that question the adequacy of existing training programs. The good thing about the proposed approach, however, is that an AI-enhanced red team coach will simultaneously identify human, conceptual, and technical shortfalls, thus offering different vectors of improvement.

> *The defense metaverse offers a unique opportunity to expose air forces to non-conventional red teams using tactics that have not yet been seen but may generally be feasible considering adversarial capabilities.*

Finally, the defense metaverse requires appropriate software and hardware infrastructure. Both need to play together in the simulation and decentralized coordination mechanisms to create a system that learns how to learn and develop new tactics. As discussed above, such systems represent "third wave AI," which is context and consequence-aware (See *Table 3.1*). Third wave AI opens an attractive future defense development path but also presents new challenges as it will be demanding to ask

international partners to engage in know-how and technology transfer in this domain. Therefore, air forces should think about an "open" defense metaverse approach, which would offer open interfaces for the suppliers of different nations to train and evaluate the tactical effects of AI systems. This "open" defense metaverse could be established as a government-controlled entity that would vet partners before granting access to create a multinational digital environment commensurate with national strategic ambitions.

REFERENCES

Allen, J. R., Hodges, F. B., and Lindley-French, J. (2021) Future War and the Defence of Europe. Oxford: Oxford University Press.

Allen, J. R., and Amir H. (2018) 'On Hyperwar,' Proceedings 2 January.
Available at: https://www.usni.org/magazines/proceedings/2017/july/hyperwar

Barno, D. and Bensahel, N. (2020) Adaptation Under Fire. How Militaries Change in Wartime. Oxford: Oxford University Press.

Borchert, H., Brandlhuber, C., Brandstetter, A., and Schaal G. S., (2022) Free Jazz on the Battlefield. How GhostPlay's AI Approach Enhances Air Defense. Hamburg: Defense AI Observatory.
Available at: https://defenseai.eu/daio_study2203

Borchert, H., Schütz, T., and Verbovszky J., (2021) Beware the Hype. What Military Conflicts in Ukraine, Syria, Libya, and Nagorno-Karabakh (Don't) Tell Us About the Future of War. Hamburg: DAIO.
Available at: https://defenseai.eu/daio_beware_the_hype

Brooks, R. and Stanley, E. A. eds. (2007) Creating Military Power. The Sources of Military Effectiveness. Stanford: Stanford University Press.
Available at: https://www.darpa.mil/work-with-us/ai-next-campaign

Gioannopoulos, G., Smith, H. and Theocharidou, M. (2021) The Landscape of Hybrid Threats. A Conceptual Model. Luxembourg: Publications Office of the European Union.
Available at: https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/

Grayson, T. (2019) 'Mosaic Warfare,' Presentation, The International Society for Optics and Photonics, 2 April.
Available from: https://spie.org/news/dcs-plenary---mosaic-warfare?SSO=1

Haystead, J. (2020) 'DARPA's Mosaic Warfare, Moving to Address the Ever-More-Rapidly-Paced Advances/ Changes in Fielded Threat Capabilities,' The Journal of Electronic Defense, 43:2, pp. 20-25.

JAPCC (2019) Shaping NATO for Multi-Domain Operations of the Future. Read Ahead. Kalkar: Joint Air Power Competence Center.
Available at: https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf.

Jensen, B., Whyte, C., and Cuomo, S. (2022) Information in War. Military Innovation, Battle Networks, and the Future of Artificial Intelligence. Washington, DC: Georgetown University Press.

Krepinevich, A. F. (2015) Maritime Competition in a Mature Precision-Strike Regime. Washington, DC: Center for Strategic and Budgetary Assessments.
Available at: https://csbaonline.org/research/publications/maritime-competition-in-a-mature-precision-strike-regime

Mazzarr, M. J. (2015) Mastering the Grey Zone. Understanding a Changing Era of Conflict. Carlisle Barracks: US Army War College.
Available at: https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1303

Ministry of Defence (2018) Global Strategic Trends. The Future Starts Today. London: Ministry of Defense. Available at: https://www.gov.uk/government/publications/global-strategic-trends

NATO STO (2023) Science & Technology Trends 2023-2043. Across the Physical, Biological, and Information Domains. Volume 2. Brussels: NATO Science & Technology Office. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf.

Stephenson, N. (1992). Snow Crash. New York: Bantam Books.