Australian Government
Department of Defence

Fighting Artificial Intelligence Battles

Operational Concepts for Future AI-Enabled Wars

Joint Studies Paper Series No. 4

Peter Layton

Defending Australia and its National Interests
www.defence.gov.au

FIGHTING ARTIFICIAL INTELLIGENCE BATTLES

OPERATIONAL CONCEPTS FOR FUTURE AI-ENABLED WARS

Peter Layton

ADC Publications are produced by the Centre for Defence Research

Australian Defence College
PO Box 7917
CANBERRA BC ACT 2610

Contact via email: cdr.publications@defence.gov.au

Available to download at www.defence.gov.au/ADC/Publications/Joint_Studies.asp

Managing editor: Fiona Mackrell

Designer: Directorate of Information and Systems: Corporate Graphics

Printed by: Elect Printing

First published in Australia 2021

You may attribute this work as follows: Peter Layton, 'Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled Wars', *Joint Studies Paper Series*, No. 4 (Canberra: Department of Defence, 2021). https://doi.org/10.51174/JPS.004.

The views expressed in this publication are the author's own and do not necessarily reflect the views or policies of the Australian Government or the Department of Defence, or any part thereof. While reasonable care has been taken in preparing this publication, to the extent permitted by law, the Commonwealth of Australia and the authors disclaim all liability howsoever caused (including as a result of negligence) arising from the use of, or reliance on, this publication. By accessing this publication, users are deemed to have consented to this condition and agree that this publication is used entirely at their own risk.

National Library of Australia – Cataloguing-in-Publication entry

Author:	Peter Layton
Title:	Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled Wars
Series:	Joint Studies Paper Series No. 4
ISSN:	2208-6013 (printed version)
	2208-6021 (online version)
DOI:	https://doi.org/10.51174/JPS.004
Subjects:	Australian Defence Force
	artificial intelligence
	AI-enabled wars
	force structure
	defence and offence concepts
	operational and tactical concepts

Contents

Foreword

It is a time of rapid disruptive technological change, especially in the field of artificial intelligence (AI). While this technology has been developed by and for the commercial sector, the apparent potential for AI in military applications is now leading armed forces worldwide to experiment with embryonic, AI-enabled defence systems to determine how these could best be used for combat and peacetime tasks.

Australia is no different, with funding allocated in the *2020 Defence Strategic Update* to begin introducing AI capabilities into Defence. This process will involve developing AI applications that address defined tactical-level and strategic-level military problems, building a skilled AI workforce, engaging with partners and allies, integrating ethics into AI applications and conducting AI experiments. A tangible demonstration of this plan in action is the opening this year of the Defence Technology Acceleration ColLab at Fairbairn, Australian Capital Territory.

Peter Layton's paper contributes to this broadly based movement by considering the role AI might play in future sea, land and air combat operations at the tactical and operational levels of war. This is a little examined area, as much of the discussion so far has focused on the key technological issues and concerns. These deliberations have indicated that AI might be a significant technology in future wars, but there remain numerous uncertainties. This paper provides a starting point from which to begin a debate that will help to resolve some of these uncertainties.

The paper argues that AI will infuse most military machines; however, its general-purpose nature means that it is likely to be employed initially within existing operational level constructs. Given this, AI's principal warfighting usefulness for the short-to-medium term is in 'find and fool'. AI, with its machine learning, is excellent at finding items hidden within a high-clutter background; in this function, it is better than humans and much faster. However, AI can be fooled through various means; its great finding capabilities lack robustness. These two key characteristics could have a dramatic effect when applied to current sea, land and air operational level thinking.

The operational concepts tentatively devised in this paper are noticeably different to those without AI technology.

The concepts discussed are intended to stimulate thinking about human–machine teams operating on the envisaged AI-enabled battlefield of the future. Such a battlefield may seem somewhat speculative at the moment, almost science fiction. Even so, many nations are already well advanced in their planning, research and development. Given the long lead times needed to reorient military forces in new directions, this journey needs to start now.

Jerome Reid
Group Captain
Director, Defence AI
Director, Defence Technology Acceleration ColLab
Information Warfare Division
January 2021

Author biography

Dr Peter Layton is a Visiting Fellow at the Griffith Asia Institute, Griffith University, a Royal United Services Institute Associate Fellow and a Royal Australian Air Force Reserve Group Captain. He has extensive aviation and defence experience and, for his work at the Pentagon on force structure matters, he was awarded the United States Secretary of Defense's Exceptional Public Service Medal. He has a doctorate from the University of New South Wales on grand strategy and has taught on the topic at the Eisenhower School for National Security and Resource Strategy, United States National Defense University. For his academic studies, he was awarded a Fellowship to the European University Institute, Fiesole, Italy. His research interests include grand strategy, national security policies particularly relating to middle powers, defence force structure concepts and the effects of emerging technology. He contributes regularly to the public policy debate on defence and foreign affairs issues and is the author of the book Grand Strategy. His articles and papers may be read at https://peterlayton.academia.edu/research.

Abbreviations

4IR	fourth industrial revolution
AAA	anti-aircraft artillery
ADF	Australian Defence Force
AI	artificial intelligence
CAP	combat air patrol
C-ISRT	Counter Intelligence Surveillance Reconnaissance and Targeting
DARPA	Defense Advanced Research Project Agency
GAI	ground-alert interceptors
GAN	Generative Adversarial Networks
GOFAI	Good Old-Fashioned Artificial Intelligence
IADS	integrated air defence system
IoT	Internet of Things
IPW	initial period of war
MUSV	medium unmanned surface vessel
MUTT	Multi-Utility Tactical Transport
NOMARS	No Manning Required Ship
OODA	Observe–Orient–Decide–Action
OoT	Ocean of Things
PLA	People’s Liberation Army
RCV	Robotic Combat Vehicle

SAM	surface-to-air missiles
UAV	uncrewed aerial vehicle
UGV	uncrewed ground vehicle
US	United States
USAF	United States Air Force
US DoD	United States Department of Defense
USMC	United State Marine Corps
USN	United States Navy
USV	uncrewed surface vessels
UV	uncrewed vehicles

Introduction

Artificial intelligence (AI) technology has suddenly become important to military forces. The United States Department of Defense (US DoD) has increased investments in AI from some $600 million in 2016–17 to $2.5 billion in 2021–22, sprawling across over 600 projects.[1] China has adopted a 'Next Generation Artificial Intelligence Development Plan' that aims to make the country the pre-eminent nation in AI by 2030 and to shift the People's Liberation Army (PLA) from an 'informatized' way of war to 'intelligentized warfare'.[2] Even more dramatically, Russia's President has declared that 'artificial intelligence is the future … whoever becomes the leader in this sphere wil become the ruler of the world'.[3] These high-level initiatives and splendid statements are starting to produce outcomes.

In the United States (US), the United States Navy's (USN) Sea Hunter uncrewed surface vessel (USV) has sailed without a crew from California to Hawaii and back again, navigating by AI using data from the vessel's onboard sensors, radars and cameras.[4] Meanwhile, under the aegis of the US Defense Advanced Research Projects Agency (DARPA), an AI-powered simulated F-16 fighter aircraft recently comprehensively defeated a comparable simulation controlled by a very experienced human pilot in multiple simulated, close-in air combat events.[5] In a similar evaluation examining

[1] Daniel S. Hoadley and Kelley M. Sayler, *Artificial Intelligence and National Security: Updated November 10, 2020* (Washington DC: Congressional Research Service, 2020), 2. https://crsreports.congress.gov/product/pdf/R/R45178/10

[2] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington DC: Office of the Secretary of Defense, 2020), 16. https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF

[3] President Putin quoted in Alina Polyakova, 'Weapons of the Weak: Russia and AI-driven Asymmetric Warfare', [Report], Artificial Intelligence and Emerging Technology Initiative, Brookings, published online 15 November 2018. https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/

[4] Jurica Dujmovic, 'Drone Warship Sea Hunter of the U.S. Navy is Powered by Artificial Intelligence', *MarketWatch*, 3 July 2019. https://www.marketwatch.com/story/drone-warship-sea-hunter-of-the-us-navy-is-powered-by-artificial-intelligence-2019-07-03

[5] Defense Advanced Research Projects Agency, *AlphaDogfight Trials Foreshadow Future of Human-Machine Symbiosis* (Washington: Defense Advanced Research Projects Agency, 26 August 2020). https://www.darpa.mil/news-events/2020-08-26

land warfare, the United States Army (US Army) has determined that an AI-enabled force has some 10 times more combat power than a non–AI powered force.[6]

In China, the PLA is now applying AI to improve the speed and accuracy of its battlefield decision-making by automating command and control systems, developing predictive operational planning and addressing intelligence, surveillance and reconnaissance data fusion challenges. The PLA has also moved to start trialling AI-enabled USVs for potential use in the South China Sea and begun experimenting with uncrewed tanks, while a private Chinese company has publicly exhibited AI-enabled, armed, swarming drones.[7]

Russia lags the US and China, but is now implementing a national AI strategy to catch up.[8] In the military domain, Russia has several lines of effort underway. A major line focuses on applying AI to information operations, both tactically in waging psychological warfare and strategically in terms of damaging adversary nations' social cohesion. Another line is using AI to improve the effectiveness of land combat operations through developing uncrewed ground vehicles (UGVs), remote sensors, tactical command and control systems, and uncrewed aerial vehicles (UAVs). A further line of effort is the automation of the command and control systems in the national air defence network.[9]

The initial indications are that AI might be a very significant technology in future wars but there remain uncertainties. While widely used in the civil domain and particularly in consumer products, AI is only just nearing operational deployment in the military environment. Moreover, it remains unproven in the hard testing ground of real combat operations. Even so, AI has become a technology that cannot be ignored by military forces considering their future.

Importantly, the AI technology that is available for the foreseeable future is narrow, not general. Narrow AI equals or exceeds human intelligence for specific tasks within a particular domain; its utility is context dependent. In contrast, general AI equals the full range of human performance for any task in any domain. When general AI might be achieved remains debatable, but it appears to be several decades away.[10] The

[6] Sydney J. Freedberg Jr, 'AI & Robots Crush Foes in Army Wargame', *Breaking Defense*, 19 December 2019. https://breakingdefense.com/2019/12/ai-robots-crush-foes-in-army-wargame/

[7] Office of the Secretary of Defense, Annual Report to Congress, 161, 142–143.

[8] Nikolai Markotkin and Elena Chernenko, 'Developing Artificial Intelligence in Russia: Objectives and Reality', Carnegie Moscow Center, 8 May 2020. https://carnegie.ru/commentary/82422

[9] Margarita Konaev and Samuel Bendett, 'Russian AI-Enabled Combat: Coming to a City Near You?', *War on the Rocks*, 31 July 2019. https://warontherocks.com/2019/07/russian-ai-enabled-combat-coming-to-a-city-near-you/

[10] Ross Gruetzemacher, David Paradice and Kang Bok Lee, 'Forecasting Transformative AI: An Expert Survey', Computers and Society: Cornell University, 16 July 2019. https://arxiv.org/abs/1901.08579

global military interest for the near-to-medium term is in how narrow AI technologies could be employed in the modern battlefield.

Unsurprisingly, AI definitions tend to draw on parallels with human intelligence. For example, the 2018 US DoD AI strategy defines AI as 'the ability of machines to perform tasks that normally require human intelligence … '.[11] Such understandings anthropomorphise technology and can unintentionally constrain thinking about AI employment to only those tasks that can be performed by humans.

In some applications, AI may do more – or less – than a human. The Venn diagrams of AI and human capabilities may overlap in some areas, but it is somewhat disingenuous to suggest they coincide. AI may be intelligent in the sense that it provides problem-solving insights, but it is artificial and, consequently, thinks in ways humans do not.

Accordingly, this paper considers AI more by the broad functions such technology can perform than by its relationship to human capabilities. The 2019 Defense Innovation Board took this approach in defining AI as 'a variety of information processing techniques and technologies used to perform a goal-oriented task and the means to reason in pursuit of that task'.[12]

At first glance, the definition appears imprecise in not including the tasks AI might actually perform for military or civilian purposes. This vagueness though is a key attribute of contemporary AI applications. AI can be applied in multifarious ways and may be considered a general-purpose technology that is pervasive across society.[13] An earlier example of a general-purpose technology is electricity, now so widely used that its continual presence and use is, to all intents and purposes, simply assumed.[14] Electricity enlivens inert machines and so, in its own way, will AI, by

[11] The 2018 Department of Defense Strategy on Artificial Intelligence full definition of AI is 'the ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action—whether digitally or as the smart software behind autonomous physical systems', Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity*, published online 12 February 2019, United States of America Department of Defense, 5. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

[12] Defense Innovation Board, *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense Supporting Document*, November 2019, 10. https://media.defense.gov/2019/Oct/31/2002204459/-1/-1/0/DIB_AI_PRINCIPLES_SUPPORTING_DOCUMENT.PDF.pdf

[13] Manuel Trajtenberg, *AI as the Next GPT: A Political-Economy Perspective*, NBER Working Paper No. 24245, (Cambridge: National Bureau of Economic Research, January 2018). https://www.nber.org/papers/w24245

[14] Clifford Bekar, Kenneth Carlaw and Richard Lipsey, 'General Purpose Technologies in Theory, Application and Controversy: A Review', *Journal of Evolutionary Economics* 28, no. 5 (December 2017): 1005–1033, 1016–1017.

providing them with the ability to achieve tasks through reasoning. AI appears set to infuse many, if not most, military machines thus the future battlefield will inevitably be in some way AI-enabled.

To achieve battlefield dominance over their opponents, military forces continually seek ever greater combat effectiveness. Traditionally, technology has been employed on the battlefield in an integrated manner that makes the best use of the strengths of humans and machines, while trying to minimise the effects of the weaknesses of both. AI seems likely to be similar. AI can be expected to be most effective when carefully teamed with humans, rather than in some independent mode.[15]

Such considerations underline that new technology in itself does not suddenly give a battlefield advantage but, rather, it is how humans employ it. A historical analysis of earlier technological innovations noted that having sound concepts guiding how to employ these new technologies was the key to military forces bringing them into service successfully. Historians Williamson Murray and Allan Millet observed that:

> The evidence points, first of all, to the importance of developing visions of the future. Military institutions not only need to make the initial intellectual investments to develop visions of future war, but they must continue agonising over such visions to discern how those wars might differ from previous conflicts … [In this] any vision of future war is almost certain to be vague and incomplete rather than detailed and precise, much less predictive in any scientific sense. Vision, however, is not enough to produce successful innovation. One's view of future conflict must also be balanced and well connected to operational realities.[16]

The linkage to the gritty realities of war is strongest at the tactical level. Strategy sets out the objectives, the general approach and the forces to use, but it is tactics that handles these forces in battle against an intelligent and adaptive adversary. While success in battle may not lead to strategic success, as the US war in Vietnam illustrates, the converse is not true. A good strategy cannot succeed in the face of continuing tactical defeat. Clausewitz writes that 'Everything turn[s] on tactical results … [t]hat is why we think it useful to emphasize that all strategic planning rests on tactical success alone … this is in all cases the actual fundamental basis of the

[15] Peter Layton, *Algorithmic Warfare: Applying Artificial Intelligence to Warfighting*, (Canberra: Air Power Development Centre, 26 March 2018), 24–30. https://airpower.airforce.gov.au/Publications/Algorithmic-Warfare-Applying-Artificial-Intelligen

[16] Williamson Murray and Allan R. Millett (eds.), *Military Innovation in the Interwar Period* (Cambridge: Cambridge University Press, 1998), 406.

decision'.[17] Tactics are generally considered to involve the distributing and manoeuvring of friendly forces in relation to each other and to the enemy, and the employing of these forces on the battlefield.[18]

This paper draws these threads together. The paper aims to develop operational concepts for the employment of human–machine teams on the future AI-enabled battlefield. Such a battlefield, especially when expanded beyond land warfare to include air and naval warfare, will have a mix of linear and deep aspects featuring both attrition and manoeuvre concepts.[19] Devising these operational concepts will provide a broad vision of how potential narrow AI systems might be used at the tactical and operational level of war.

Initially, the paper discusses the various technical elements that combine to create the AI technology package. These include advanced computer processing and big data together with specific aspects related to cloud computing and the Internet of Things (IoT). The second chapter examines waging war using AI and develops generic operational concepts for defence and offence. These concepts are located at the blurred interface between the operational and tactical levels and concern the distribution and manoeuvre of friendly forces relative to the adversary, and of friendly force employment on the battlefield.

Chapters 3, 4 and 5 apply the two generic concepts of AI-enabled defence and offence into the sea, land and air domains, respectively. Combat in each domain is sufficiently different in terms of distributing and manoeuvring friendly forces and in engaging the enemy to necessitate individual AI employment concepts. No single employment concept can adequately encompass all three domains except at such a high level of abstraction that understanding the implications can become difficult. Suggesting such forward-leaning concepts may seem to verge on speculative fiction. To avoid this, each concept is deliberately grounded in contemporary

[17] For Clausewitz, tactics involved the use of armed forces in the engagement, while strategy was the purposeful use of a series of engagements to achieve the war's objective. Carl von Clausewitz,
On War, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 128, 386.

[18] Wayne P. Hughes and Robert Girrier, *Fleet Tactics and Naval Operations*, 3rd ed. (Annapolis: Naval Institute Press, 2018), 2.

[19] Linear battlefields are those where opposing forces meet along a line of contact. In contrast, deep battlefields are those where opposing forces attack across the depth of each other's forces. Sporting analogies can be used to illustrate the differences. A linear battlefield is like American football, where attacking and defending sides face one another on a fixed line of scrimmage. A deep battlefield is more akin to soccer, with opposing forces intermixed and moving fluidly across the entire field, where some on each side play offense and some play defence. Sean B. MacFarland, *Non-Linear Operations: A New Doctrine for a New Era* (Fort Leavenworth: School of Advanced Military Studies, 1994), 12. https://apps.dtic.mil/dtic/tr/fulltext/u2/a284137.pdf

operational thinking, and current and emerging AI-enabled sea, land and air platforms and systems are discussed to illustrate the ideas advanced.

The intent in devising these operational concepts is to stimulate thought and initiate vigorous debate about the future and how to prepare for it. The operational concepts presented in this paper are intended to be a basis for arguing over the practicalities, possibilities and usefulness of alternative, AI-enabled battlefield concepts. It is only through the dialectical process of critically analysing proposals and continually reconstructing them for further analysis and evolution that progress towards an optimum operational concept can be made.

The concepts discussed in this paper are deliberately constrained in nature and scope. In terms of nature, the sea, land and air concepts are just that – to keep each concept focused, they are not joint or combined. Importantly this narrowness means that some areas, like Russia's use of AI in influence warfare or China's AI employment in societal management and internal defence, are not included.[20] For similar reasons, each concept has a narrow scope, focused on warfighting with only limited attention to logistics and avoiding key areas such as education, training, administration and command and control. Notably, the new domains of cyber and space are not discussed except in terms of their relationship to tactical engagements in the traditional land, sea and air domains.

This paper takes AI and looks outward, relating this new technology to both operational ways of war and tactical employment options. With such a focus, the paper is then different to the numerous AI strategies and plans that many armed forces have formulated. In general, these look inward, aiming to set out how AI as a technology will be researched, acquired and introduced into their specific service.[21] This paper aims to complement those AI technology strategies and plans, playing a small part in connecting them to the broader business of warfighting.

[20] Concerning Russia, see Layton, *Algorithmic Warfare*, 56–58. For China, see Peter Layton, 'Artificial intelligence, big data and autonomous systems along the belt and road: towards private security companies with Chinese characteristics?' *Small Wars & Insurgencies* 31, no. 4 (June 2020): 874–897.

[21] An example is the Royal Australian Navy's RAS-AI Strategy 2040, released in October 2020. In this document, four lines of effort are set out to address 'many of the common challenges that RAS-AI adoption faces and key enablers that it will require. These include training and workforce transformation; research & development; and building collaborative partnerships with industry and allies to design and demonstrate RAS-AI capabilities'. Royal Australian Navy, *RAS-AI Strategy 2040* (Canberra: Royal Australian Navy, October 2020). https://www.navy.gov.au/sites/default/files/documents/RAN_WIN_RASAI_Strategy_2040f2_hi.pdf

CHAPTER 1
Technology drivers

Modern warfare both involves and is shaped by technology. The technologies used bound the possible actions military forces can take; they both empower and constrain force employment options at both the tactical and operational levels. Technology and warfare might be deeply interwoven but, in the field of AI, there is a subtle twist.

AI is in the main a commercially driven technology. Accordingly, it is incumbent on military forces to keep up with the commercial domain's development and exploitation of AI. This is a sharp contrast to when the military led technological development during the Cold War (1947–1991) and took a calculated approach to such change, as well as carefully managed any disruptions to the in-service force structure. Today, in AI, the demands of the commercial world and the opportunities of the marketplace drive technological innovation and its adoption. In-service military equipment may be made obsolete not to the timetable of the armed forces using it. Instead, the timetable may be decided by external commercial-domain and market forces.

Importantly AI, whether in civilian or in military applications, is not a stand-alone item. Instead, the application of AI is a combination of several technology building blocks, usefully termed by Carnegie Mellon University the 'AI stack'. The 'perceive' layer of the stack includes computing, wireless cloud networks and devices, such as sensors and the IoT that allow machines to perceive the world around them. The 'decide' layer encompasses massive data management, machine learning, digital models and decision support aids. Lastly, the 'act' layer covers planning and acting (optimisation, strategic reasoning, knowledge), autonomy technologies and human–machine interfaces that allow the human operators to orient themselves. Importantly, ethics is integral to all layers.[22]

[22] Shane Shaneman, 'The AI Stack: A Blueprint for Developing & Deploying AI', National Defense Industrial Association SO/LIC Symposium 2019, 3 February 2019, Slide 6. https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2019/solic/Shaneman.pdf

It is immediately obvious that the stack is not just AI but rather involves numerous technologies, all interacting. Operating together, these technologies generate combinatorial effects, boosting the capability and effects of each technology far more than if they were used in isolation. When managed adroitly, such an arrangement can create exponential change, where the rate of change rapidly escalates as more and more new technologies join the mix.[23]

There may, however, be a medium-term upper limit to the exponential change. Some already see an endpoint in sight, with forecasts of an emerging AI 'autumn' and possibly even a return to 'winter'.[24] AI has had two winters previously, when enthusiasm and funding declined: 1974–1980 and 1987–1993. If repeated, technological progress would plateau.

There would still be considerable innovation, but these would be within – not beyond – the current technological paradigm. Application of current or near-term AI technology to new tasks would then be the model. However, by comparison with the commercial realm, AI has not deeply penetrated the military domain. AI may be employed in many ways not yet explored by military forces. This chapter discusses technologies associated with AI and machine learning, big data, cloud computing and the IoT.

AI computing

AI dates back some 70 years to Alan Turing's seminal 1950 paper 'Computing Machinery and Intelligence'.[25] Even one of today's leading-edge concepts, neural networks, originated around 1957.[26] To a significant degree, the crucial deficiency has not been in AI ideas but rather in having adequate computing power for these ideas to be implemented.

By 1997, there was sufficient computing power to dramatically demonstrate AI's potential with the defeat of the world chess champion, Gary Kasparov, by the IBM Deep Blue computer. Deep Blue's AI used conventional rules-based software

[23] Mark Spelman et al., Digital Transformation Initiative: Unlocking $100 Trillion for Business and Society from Digital Transformation. Executive Summary (Cologny: World Economic Forum in collaboration with Accenture, January 2017), 6. https://www.accenture.com/_acnmedia/accenture/conversion-assets/wef/pdf/accenture-dti-executive-summary.pdf

[24] Sam Shead, 'Researchers: Are We on the Cusp of an "AI Winter"?', *BBC News*, 11 January 2020. https://www.bbc.com/news/technology-51064369

[25] A. M. Turing, 'Computing Machinery and Intelligence', *Mind* 59, no. 236 (October 1950): 433–460.

[26] Dave Martinez et al., *Artificial Intelligence: Short History, Present Developments, and Future Outlook*, (Boston: Massachusetts Institute of Technology, January 2019): 15. https://www.ll.mit.edu/sites/default/files/publication/doc/2019-09/Artificial%20Intelligence%20Short%20History%2C%20Present%20Developments%2C%20and%20Future%20Outlook%20-%20Final%20Report%20-%20Martinez.pdf

written in the C programming language. The software codified the knowledge of experts and was developed in cooperation between computer programmers and chess grandmasters.

In using symbolic representations of problems, logic and search, Deep Blue's rules-based AI is an example of GOFAI: Good Old-Fashioned Artificial Intelligence. Such handcrafted knowledge, 'expert' systems can be considered 'first-wave' AI. They are good at logical reasoning about narrowly defined problems but are poor at handling uncertainty and have no ability to learn or generalise.[27]

Second-wave AI has been enabled by two key advances. Affordable graphics processing units with massive parallel processing that can run machine-learning software became readily available to meet the demands of video gamers. Next, large datasets were created that machines with graphics processing units could use to learn from.

Modern AI is now focused on machine learning. Instead of programming the computer with each individual step, as Deep Blue did, machine learning uses algorithms to teach itself by making inferences from the data provided. Algorithms are the sequence of instructions and rules that computers use to solve problems. In machine learning, the algorithms create the rules that the AI uses, not external human computer programmers as in GOFAI. With different training data, the same learning algorithm can be used to generate new rules and instructions appropriate to new tasks. In general, the more data used to train the learning algorithm, the better the rules and instructions devised.

There are two principal machine-learning methods: supervised and unsupervised. In supervised learning the learning algorithms are given labelled data. For example, photos of transport aircraft labelled 'transport aircraft' are fed through the algorithm so it can devise the rules for classifying such pictures in the future. Supervised learning requires large numbers of people to categorise and tag the data.

Unsupervised learning uses unlabelled data. In this method, the machine-learning algorithm identifies patterns for itself in the data it is fed. An inherent problem is it is difficult to know what data associations the learning algorithm is actually making.

Supervised learning systems can achieve extremely high performance, but they require very large, labelled datasets to do so. In contrast, unsupervised learning systems can often be less predictable in their performance. The choice of learning

[27] Scott Jones, 'Third Wave AI: The Coming Revolution in Artificial Intelligence', *Medium*, 28 August 2018. https://medium.com/@scott_jones/third-wave-ai-the-coming-revolution-in-artificial-intelligence-1ffd4784b79e ; John Launchbury, *A DARPA Perspective on Artificial Intelligence*, Defense Advanced Research Projects Agency, 2017. https://www.darpa.mil/attachments/AIFull.pdf

system depends on the task, as both have strengths in solving different types of problems. An example might be detecting cases of fraud within large quantities of financial data. Supervised learning is preferred for identifying potential fraud that matches known behaviours. In contrast, unsupervised learning systems can find new, unidentified patterns of behaviour that might indicate new kinds of fraud practices.[28]

A type of unsupervised learning, reinforcement learning involves the learning algorithm interacting with a dynamic environment that provides feedback with rewards for doing tasks correctly and punishments for incorrect performance. The AlphaGo AI was trained through using reinforcement learning involving playing against expert humans; consequently, in 2016, it defeated the world Go champion. The strategy game of Go has long been considered a particularly difficult challenge for AI to master. This somewhat startling success significantly influenced Chinese military thinkers about the need to embrace AI.

Similar in concept are Generative Adversarial Networks (GAN) that compete against each other to improve their performance. Each network tries to trick the other by making it increasingly difficult for the other to correctly complete its task. This technique allows smaller datasets to be used for training because the opponent can generate increasingly realistic, but false, data against which to train.

AlphaGo Zero is a development of AlphaGo that uses a form of GAN training to play against itself, becoming progressively better each time. AlphaGo Zero only had the rules of Go, but after three days of self-training, involving playing millions of simulated games, it was able to beat the human-trained AlphaGo.[29]

While promising much in the laboratory, reinforcement learning and GANs have difficultly operating in the real world. The real world is not as constrained as games in terms of inputs, outputs and interactions. Some argue that AlphaGo Zero's remarkable success is partly due to the particular rules of Go that favour GAN training.[30] Moreover, the ability to learn takes time which cannot be accelerated outside laboratory simulations. Lastly, the consequences of real-world failures can be severe; these can have more serious implications than being simply a useful learning experience.

Reinforcement learning and GAN systems are most useful when they can generate their own data and not rely on it being provided, but are mainly used for applications where simulations can closely resemble the operational environment. This may be

[28] Greg Allen, *Understanding AI Technology* (Washington: Joint Artificial Intelligence Center, April 2020), 12–13. https://www.ai.mil/docs/Understanding%20AI%20Technology.pdf

[29] David Silver and Demis Hassabis, 'AlphaGo Zero: Starting from Scratch', *DeepMind*, 18 October 2017. https://deepmind.com/blog/article/alphago-zero-starting-scratch

[30] Xiao Dong, Jiasong Wu and Ling Zhou, 'Demystifying AlphaGo Zero as AlphaGo GAN', Cornell University, 24 November 2017. https://arxiv.org/pdf/1711.09091.pdf

more frequent than first thought – training a robot to walk up and down stairs, for example, could be potentially achieved using reinforcement learning.

The current, state-of-the-art machine learning is deep learning, where algorithms are stacked in layers to create an artificial neural network. These can improve their performance over time as they continually train themselves on new data received while in operation. They learn 'on the job' and so are capable of emergent behaviour that may surprise – for good or bad. In contrast, traditional unsupervised machine learning continues to rely on the original dataset training undertaken. AI systems using deep learning have now achieved a level of performance beyond that of humans in tasks involving image classification, speech recognition and gameplay.

A major issue with deep learning is low explainability. Romeo Kienzler, chief data scientist at IBM Watson IoT reportedly noted that 'We know deep learning works, and it works well, but we don't exactly understand why or how'.[31] This 'explainability problem' is sometimes perceived as a problem for all of AI, but it is primarily a problem for neural networks and deep learning. Many other types of machine-learning algorithms – for example, decision trees – have very high explainability. The paradox is that AI outputs that are easily explainable have much lower accuracy than those that do not.[32]

Second-wave AI is strong at perceiving and learning, possessing good classification and prediction capabilities. However, in contrast to first-wave AI, second-wave AI has minimal reasoning capability and cannot transfer what has been learned in one domain to another. The strengths and weaknesses of first-wave and second-wave AI mean that the newer, second-wave AI has not displaced the older first-wave AI; it is more that the innovation effort has shifted towards trying to apply the newer AI form. A strong AI advocate, former US Deputy Secretary of Defense Robert Work argues that both waves can and should be usefully combined:

> [W]ith the compute power we have now, I believe that we are spending far too much attention on the [second-wave] machine learning aspect and not enough on the [first-wave] expert systems, primarily because it uses if/then logic and you don't have to worry about explainability. It is built into the program. If a problem occurs, you can recreate the problem and know exactly what happened. [With] the autonomous ship that the [US Navy has] … you can press the

[31] George Anadiotis, 'Artificial Intelligence in the Real World: What Can It Actually Do?', ZDNet, 22 February 2017. https://www.zdnet.com/article/artificial-intelligence-in-the-real-world-what-can-it-actually-do/

[32] Alvin Wan, 'What Explainable AI Fails to Explain (and How We Fix That)', *Towards Data Science*, 17 April 2020. https://towardsdatascience.com/what-explainable-ai-fails-to-explain-and-how-we-fix-that-1e35e37bee07

> button and the thing will autonomously navigate between Norfolk and Bahrain. All of the [nautical] rules of the road are all first wave AI. It's just if/then. If the [approaching] ship is to the port [side] … [then] here are the sums you do. But [the ship] needed to have machine learning in the [bridge] camera just to say, 'Okay, is this a container ship bearing down on me or a sail boat? And how fast can it go?' So it was a [sensible] combination of machine learning and expert systems [that] would allow that thing to go … there is a lot still left to go in first wave.[33]

DARPA is now researching third-wave AI, that can adapt to the context encountered. This future third wave is envisaged as needing much less data to train properly, being able to converse in natural language and able to function with minimal supervision. The hypothesised third-wave AI may offer many of the capabilities that combining first-wave and second-wave AI could provide.[34]

Applying AI

Current AI can address some specific problems more consistently than humans or more conventional human-programmed, rules-based computers. Its results are generally probabilistic, providing confidence-weighted responses to problems but not necessarily giving the same result every time. AI can quickly identify patterns and detect items hidden within vast, unstructured data troves, which is important given that 80% of the world's data is unstructured. In broad terms, current generation AI is effective in five main areas:[35]

- **Identifying.** This involves classifying what something is – for example, diagnosing an issue given the symptoms, indications and warnings – and determining how items are connected – for example, relationships between data. Examples include image and face recognition, change detection and geolocation of images.
- **Grouping.** This involves clustering, where provided data can be analysed to determine correlations and subsets – for example, evaluating which factors cause a specific problem. An example is pattern-of-life analysis.
- **Generation.** This involves creating an image or text when given an input – for example, recognising speech and responding appropriately.

[33] Robert O. Work et al., 'Transcript from U.S. AI Strategy Event: "The American AI Century: A Blueprint for Action" ', *Center for a New American Security*, last modified 17 January 2020. https://www.cnas.org/publications/transcript/american-ai-century

[34] John Launchbury, 'A DARPA Perspective on Artificial Intelligence', Defense Advanced Research Projects Agency, streamed 15 February 2017, YouTube video, 16:11. https://www.youtube.com/watch?v=-O01G3tSYpU&list=LL5S74bRl-vBw9Fz8Gpxr6jQ&index=4537

[35] This listing is derived from: MMC Ventures, *The AI Playbook: The Step-by-Step Guide to Taking Advantage of AI in Your Business* (London: Barclays UK (BUK) Ventures, 2019), 16. https://www.ai-playbook.com/

- **Forecasting.** This involves predicting future changes given historical time series data – for example, predictive maintenance that determines when in the future a machine will fail.
- **Planning.** This involves running digital models of complicated activities to determine probable outcomes – for example, wargaming and providing decision-makers with what-if analyses.

Humans have traditionally undertaken these tasks, albeit increasingly with computational assistance. Where AI adds value is doing these tasks more effectively and efficiently, at much higher speed, without capacity constraints and possibly without human involvement. The benefits that AI bring can then be condensed to efficacy, velocity and scalability.[36]

Such attributes mean that AI-enabled systems can be given greater autonomy, allowing applications like autonomous land vehicles and swarming. The critical issue in granting partial or full autonomy is whether the decisions being made when undertaking the specified function can be based on data. AI analyses data using algorithms to make decisions. In broad terms, this means that first, problems need to be of a type able to be measured so that the appropriate data can be collected, and second, that these problems can be reduced to algorithms. Many problems meet these two criteria.

Shortcomings of AI

Humans may produce better results than AI in some circumstances. AI-enabled machines can be quite brittle, being generally unable to handle minor context changes. Moreover, they have poor domain adaptability in that they can struggle to apply knowledge learned in one context to another. Humans are also considered better at inductive thought: being able to generalise from limited information. Humans generally make better judgements in environments of high uncertainty.[37]

In terms of technological shortcomings, the most common reason for machine-learning failures is that the training data is not sufficiently representative of the real-world examples that AI encounters. This can occur for various reasons. The data used for training may be of higher quality than the data obtained by real-world observations while in normal use. Alternatively, the AI may have complete data on which to learn and derive solutions in the laboratory; but, in the real world, some input data may

[36] David Kelnar, *The State of AI 2019: Divergence* (London: Barclays UK (BUK) Ventures, 2019), 135. https://iec2021.aaru-confs.org/The-State-of-AI-2019-Divergence.pdf

[37] Layton, *Algorithmic Warfare*, 72.

be missing, obscured, corrupted or distorted, creating processing errors.[38] Finally, while AI training may be based on perfect information about all the participants or elements, in many real-world interactions, information can be hidden deliberately or unintentionally, or may simply be unknown.[39]

AI training failures can also come about from adversarial attacks. Armed forces or even individual civilians can be expected to try to deceive machine-learning AI systems. In this, the effort required to fool an AI algorithm is considerably less than that needed to develop one. An example is the devising of various active and passive means to thwart the facial recognition AI systems that are available to individuals.[40] A recent study noted that methods to defend AI machine learning can be divided into those that detect adversaries inputting false samples and those that improve the training phase, with the latter judged superior.[41]

Machine-learning AI also has an inherent design problem. Their real-world performance generally degrades over time if they are not updated regularly with new training data that matches the changing state of the world. Called 'concept drift', this characteristic reflects that real-world data often arrives in streams and evolves over time in non-obvious ways; the AI's machine learning gradually becomes out of date and increasingly less accurate when analysing input data.[42] For machine-learning AI, the old software engineering maxim 'software is never done' still holds.

This gradual degradation can become accelerated in AI systems that use on-the-job training, as adaptative AI does. Such systems can at first operate well but steadily become more erratic as they continually retrain. An example is Microsoft's experimental 'Tay' chatbot that was initially trained, apparently by neural networks.

Tay went 'live' and engaged with the public online using Twitter, aiming to improve its performance through machine learning from these interactions. However, Twitter

[38] Yasmin Afina, 'Rage Against the Algorithm: The Risks of Overestimating Military Artificial Intelligence', *Expert Comment*, Chatham House, last modified 27 August 2020. https://www.chathamhouse.org/2020/08/rage-against-algorithm-risks-overestimating-military-artificial-intelligence

[39] Joshua Sokol, 'Why Artificial Intelligence Like AlphaZero Has Trouble with the Real World', *Quanta Magazine*, 21 February 2018. https://www.quantamagazine.org/why-alphazeros-artificial-intelligence-has-trouble-with-the-real-world-20180221/

[40] Aaron Holmes, 'These Clothes Use Outlandish Designs to Trick Facial Recognition Software into Thinking You're Not Human', *Business Insider*, 13 October 2019, https://www.businessinsider.com.au/clothes-accessories-that-outsmart-facial-recognition-tech-2019-10?r=US&IR=T; 'Computer Vision Dazzle Camouflage', CV Dazzle, last modified 15 June 2020. https://cvdazzle.com/

[41] Nicolas Papernot et al., 'The Limitations of Deep Learning in Adversarial Settings', *IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE 2016, Saarbrucken, Germany, 21–24 March 2016, 15. https://arxiv.org/pdf/1511.07528.pdf

[42] AIM Implementation Team, *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines* (Washington: Office of the Director of National Intelligence, 2019), 3. https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf

trolls managed to retrain Tay using offensive tweets that caused Tay to respond erratically to some questions using racist slang and far-right ideology. Microsoft shut Tay down after 16 hours as its tweets steadily worsened.[43] Russia's Google rival, Yandex, also trialled a comparable experimental AI chatbot. 'Alice' went rogue within a day of going online, just like Tay.[44]

Conversely, AI trained using a single, fixed dataset gives more predictability but, as noted, is less able to manage environmental change.

The overall effect of these AI shortcomings is that human users must continually monitor AI system outputs to verify that they remain appropriate and update the systems when necessary. Humans are key, for theoretical studies to date provide few insights about when a machine-learning system may fail or even whether they will work as expected.[45] The failure modes of AI technologies are simply inadequately understood.[46] The result is that AI is not a technology that humans can 'set and forget'.

Big data

In 2018, the German Chancellor, Angela Merkel, famously declared that 'data is the raw material of the 21st century'.[47] AI needs data both to learn on and to process to produce outcomes; in a sense, data is the fuel on which AI runs.

AI can analyse both structured and unstructured data, giving it meaning in terms of relationships, patterns and associations. Structured data is organised for inputting into relational databases, such as spreadsheets, and is easily and quickly searchable using simple algorithms. Such data is purposefully formatted to fit the requirements of the computer systems being used. The IoT involves widespread, multiple-type sensor dispersion, many of which produce structured data allowing ready machine-to-machine interaction.

In contrast, unstructured data does not fit into the fields of row and column databases. Unstructured data files can include email messages, documents, social

[43] Sarah Perez, 'Microsoft Silences Its New A.I. Bot Tay, After Twitter Users Teach It Racism [Updated]', *Tech Crunch*, 25 March 2016. https://techcrunch.com/2016/03/24/microsoft-silences-its-new-a-i-bot-tay-after-twitter-users-teach-it-racism/

[44] Natasha Lomas, 'Another AI Chatbot Shown Spouting Offensive Views', *Tech Crunch*, 25 October 2017. https://techcrunch.com/2017/10/24/another-ai-chatbot-shown-spouting-offensive-views/

[45] AIM Implementation Team, *The AIM Initiative*, 11.

[46] 'AI Next Campaign', Defense Advanced Research Projects Agency, accessed 9 January 2020. https://www.darpa.mil/work-with-us/ai-next-campaign

[47] Angela Merkel, 'Speech by Federal Chancellor at the World Economic Forum Annual Meeting in Davos on 24 Jan 2018', The Federal Government, 2018, transcript, para 13. https://www.bundesregierung.de/breg-en/chancellor/speech-by-federal-chancellor-angela-merkel-at-the-world-economic-forum-annual-meeting-in-davos-on-24-january-2018-455144

media, videos, imagery, audio files, presentations and webpages. Such data may be generated by humans or by machines, such as uncrewed reconnaissance drones and remote imagery devices.

To analyse unstructured data, the AI must be trained. AI machine-learning becomes steadily more dependable as it is fed more and more data. However, while large data troves are needed for machine-learning AI, the quality of the data being used is just as important. Poor-quality data can mislead AI, making its outputs dubious. AI needs data that is standardised, normalised, verified, enriched and has duplicated data deleted; much of this process falls under the umbrella term of 'data wrangling'. In 2015, the US DoD prioritised data quality over data quantity for the first time.

Data storage has a role to play in ensuring quality. There should be only a single data view, even if the data is stored across multiple disparate systems. In achieving this, good data hygiene is crucial. The data should be clean, that is, mostly error free. In contrast, dirty data includes redundant data, erroneous data, incomplete data and outdated information. Organisations need to have sophisticated data strategies that address data availability, collection, hygiene and governance.

The task of cleaning data needs human involvement. Data-cleaning tools can expedite the task by automating many processes. However, these tools are not autonomous and require column-by-column guidance by a skilled data scientist. More complex issues that arise during data cleaning as a result of unknown unknowns tend to be unique to each dataset and, therefore, not well suited for automated tools. Data scientists with experience in specific datasets continue to be required.[48]

Data management

To become AI enabled, a military force needs access to data. While military forces have traditionally been avid record keepers and archivists, much of this data is in bureaucratic silos inaccessible to most across the whole organisation. The issue is being compounded by the uncertainty about what to collect that might be useful in the future. A 2020 RAND Corporation study into using AI in for United States Air Force (USAF) command and control purposes noted that:

> The commercial sector is … appearing to converge on the 'collect everything' philosophy toward data. The premise is that some data streams may contain undiscovered correlations and that it is difficult to anticipate future data needs. The data requirements of the Joint All Domain Command and Control are ever changing as [the] concept

[48] Sherrill Lingel et al., *Joint All-Domain Command and Control for Modern Warfare: An Analytic Framework for Identifying and Developing Artificial Intelligence Applications* (Santa Monica: RAND Corporation, 2020), 37–38. https://www.rand.org/pubs/research_reports/RR4408z1.html .

> of operations are actively developed and tested. To be in a position to satisfy all future data requirements, the Air Force needs to adopt a 'save everything' approach.[49]

Such an approach to saving data is now possible given that storage costs have plummeted. The emerging approach to mass data storage is for data to be ingested into a 'data lake', a low-cost, large-capacity computing environment that stores and manages unstructured and semistructured data. In the data lake, the purpose of the data has not yet been determined, that is, the data is 'raw', although easy to access and update. Such raw data can be used for AI machine learning. However, data lakes require management by data scientists to ensure appropriate quality and governance measures are in place to avoid creating a data swamp.

In hardware terms, a data lake is a network of connected computers that provides storage and computational resources to form a central repository for data collection and processing. This sharing of data in a distributed network environment allows ready access to data when and as required.

The application of this technology has led to concepts of 'data fabric', conceived in visual terms as 'a weave that is stretched over a large space that connects multiple locations, types and sources of data, with methods for accessing that data'.[50] Data fabric architectures envisage an integration platform that enables data management, access and use irrespective of where the data is held or generated. Such architectures enable a single and consistent data management framework that allows seamless data access and processing across otherwise siloed data storages.[51]

Data fabric architectures can have enterprise-level effects in terms of being able to reorganise and repackage business capabilities together. The data fabric can be the base upon which organisations can be quickly recomposed to meet new demands and circumstances. These so-called 'composable enterprise' designs allow modularity, efficiency, continuous improvement and adaptive innovation.[52]

Data problems

Machine-learning AI learn by studying training datasets. In so doing, the algorithms are determining facts about the dataset, not about the external world. If the dataset is too small, then the AI may gain a skewed or incomplete understanding of the

[49] Lingel et al., 35–36.

[50] Talend, 'What is Data Fabric?', paragraph 3, accessed 9 January 2020. https://www.talend.com/resources/what-is-data-fabric/

[51] 'Gartner Identifies Top 10 Data and Analytics Technology Trends for 2019', *Gartner*, media release 18 February 2019. https://www.gartner.com/en/newsroom/press-releases/2019-02-18-gartner-identifies-top-10-data-and-analytics-technolo

[52] Kasey Panetta, *5 Trends Drive the Gartner Hype Cycle for Emerging Technologies*, Gartner, 18 August 2020. https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020/

issue. Even if using large datasets the AI may not be able to determine which of the many decisions that need to be undertaken to complete a complicated task are actually critical. All decisions to be taken may be ranked as equally important. Further, for a variety of reasons, the datasets used to train AI can be biased, making the outputs less reliable.

In military operations, there are some further issues. The relevance of the data gathered may decline quickly as the tactical situation changes. It may rapidly become of historical value only. Conversely, operations are frequently undertaken in new environments and unique contexts. The available datasets may be sparse, providing the AI with limited training data, thus making its performance uncertain. Furthermore, it may be difficult to quickly retrain AI using just-collected data. There may not be sufficient time to take advantage of the new data.

Data is inherently a problem for second-wave AI. The task of collecting, labelling and cleaning the data needed to train AI using machine-learning techniques is generally time-consuming and often costly.[53]

Supporting technologies

Cloud computing

Many digital technologies are connected to the cloud, storing and accessing data and programs from external sources rather than from the device's own hard drive. In the late 1990s, a cumulus cloud drawing was used to represent the internet and so 'cloud' became a metaphor for accessing services over an internet.

Cloud-native computing is particularly important for AI, as machine learning often requires more data and processing power than the AI system has internally. Indeed, a crucial lesson learned from USAF AI implementation is that high-quality AI learning requires placing the latest data into the cloud quickly so it can be readily accessed, rather than using slower, manual entry methods.

Cloud data storage may seemingly make the location of the AI computer irrelevant, with connectivity instead the critical dynamic. However, in some situations, data sovereignty, spectrum availability and data latency may present difficulties. Moreover, some of the current cloud storage technologies are not optimised for use by AI machine-learning techniques. There are inherent challenges in cleaning, standardising and normalising data accessed in real time from many different sources including classified, private, public, domestic, international, human and machine. Moreover,

[53] 'AI Next Campaign'.

military clouds represent particular challenges, as they must be accessible by others in harsh electronic countermeasure environments.

In large organisations, there is a tendency for separate groups to each have their own cloud, each with different data formats, access procedures and authorised users. However, without a single common enterprise cloud data cannot be shared with all automatically, security patches cannot be fully distributed and new software cannot be widely incorporated. Commenting on US DoD efforts to build an enterprise cloud, the Chief of the US Joint Artificial Intelligence Center noted that '[w]ithout [an] enterprise cloud, there is no AI at scale: AI will remain a series of small-scale stovepipe projects'.[54]

Internet of Things

The IoT is a large-scale network of interconnected devices (things) exchanging information machine-to-machine without human involvement. In the civilian domain, the number of things connected to the internet is increasing rapidly, from 7 billion in 2018 to an estimated 35 billion in 2021.[55] Many of these are simple devices like motion sensors, thermostats, lighting, meters and imaging devices; more complicated devices include smart TVs, speakers and appliances, wearables, industrial robots, drones, autonomous vehicles and, in the military domain, weapons.

IoT networks allow remote monitoring and control but can generate vast amounts of data. For example, the Airbus A-350 airliner has some 6,000 sensors, generating 2.5 terabytes of data every day it operates. Connecting the IoT network to an edge device that can assess the data in real time, forward the most important information into the cloud, and then delete the remainder can reduce storage and bandwidth costs.[56]

Such edge computing places some of the data processing power at the network's edge rather than retaining it in a distant, centralised cloud facility. This can address cloud performance issues, such as latency, connectivity, privacy, security, bandwidth and a congested and contested electromagnetic environment. Computing can then be done at or near the origin of the data, instead of relying on the cloud at the remote centralised facility. Edge devices also often act as an entry or exit point into different networks, that is, into different clouds.

[54] Sydney J. Freedberg, 'Big Data for Big Wars: JEDI vs. China & Russia', *Breaking Defense*, 12 August 2019. Paragraph 7. https://breakingdefense.com/2019/08/big-data-for-big-wars-jedi-vs-china-russia/

[55] Gilad David Maayan, 'The IoT Rundown for 2020: Stats, Risks and Solutions', *Security Today*, 13 January 2020. https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?p=1

[56] Duncan Stewart et al., 'Bringing AI to the Device: Edge AI Chips Come into Their Own', *Deloitte Insights*, 9 December 2019. https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2020/ai-chips.html

Most edge computing is now done using AI chips. These are physically small, relatively inexpensive, use minimal power and generate little heat, allowing them to be readily integrated into handheld devices, such as smartphones, and non-consumer devices, such as industrial robots. Even so, in many applications, AI computing will be used in a hybrid fashion: some on the device and some in the cloud. The preferred mix will vary depending on the kind of AI processing to be undertaken.

An example of the possibilities is the low-cost drones with AI chips that use machine-learning algorithms to identify swimmers in danger in the surf or detect approaching sharks, all without a cloud-computing wireless connection.[57] Such drones are fitted with a smartphone system-on-a-chip applications processor that includes functions such as processing, graphics, memory, connectivity and AI.

IoT networks can be comprised of fixed and mobile devices, including drones. Mobile devices can be designed to collaborate with each other in swarms. There are two main approaches to the design of swarms. The simpler is the centralised system, where a central component (one of the robots or an external computer) coordinates all the robots and their tasks. While the centralised system is a straightforward system to implement, it is hard to expand, as adding more robots increases the central station processing load. Moreover, the system inherently does not fully utilise the computing power of each individual robot. The most serious issue for military purposes is that the central component is a single point of failure; a centralised system lacks robustness.[58]

The alternative approach is that the robots coordinate through exchanging wireless messages or indirectly by placing messages in the environment. Such distributed approaches are inherently robust, with no single point of failure. The loss of a single robot only reduces overall swarm performance by that quantum. Moreover, the distributed approach is more flexible and scalable. The robots can be divided into smaller swarms and used for multiple tasks if the whole swarm is not needed. Conversely, additional robots can be added easily if the task requires large numbers.[59]

The mosaic warfare concept devised by the US DARPA brings AI and several of the associated technologies together. Under the construct, the IoT systems arrayed across the battlefield are conceived as heterogeneous, being broadly divided

[57] Nabin Sharma and Michael Blumenstein, 'SharkSpotter Combines AI and Drone Technology to Spot Sharks and Aid Swimmers on Australian Beaches', *The Conversation,* 28 September 2018. https://theconversation.com/sharkspotter-combines-ai-and-drone-technology-to-spot-sharks-and-aid-swimmers-on-australian-beaches-92667

[58] Mordechai Ben-Ari and Francesco Mondada, *Elements of Robotics* (Cham: Springer Open, 2018), 252.

[59] Ben-Ari and Mondada, *Elements of Robotics*, 252.

into either sensors, weapons or decision elements. Crucially, the elements can all communicate among themselves and with the overarching command and control system through the cloud.

The kill chain model used by contemporary military forces tightly integrates the sense–decide–act logic flow. In contrast, the data flow across the large IoT field in the mosaic warfare construct creates a kill web, where the best path to achieve a task can be determined and used in near real-time. The use of the IoT field is then fluid and constantly varying, not a fixed data flow as the kill chain model implies. The outcome is that the mosaic warfare concept provides commanders with highly resilient networks of redundant nodes and multiple kill paths. Moreover, the mosaic concept aims to be scalable; the size and elements of the IoT field can be varied as battlefield circumstances demand.[60]

For the mosaic warfare concept to be practical, the IoT elements need AI edge computing. In addition, the overarching command and control system needs to use AI to support the human commanders in running the battle. There is considerable technical complexity in determining the optimum communications links and data flow across an ever-changing web comprising numerous heterogenous elements. In this web, the communications system that each element incorporates presents a technical challenge, as all must be able to pass data to the other elements involved.

[60] Bryan Clark, Daniel Patt and Harrison Schramm, *Mosaic Warfare Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations* (Washington: Center for Strategic and Budgetary Assessments, 2020), 27–32, https://csbaonline.org/uploads/documents/Mosaic_Warfare_Web.pdf; David A. Deptula et al., *Restoring America's Military Competitiveness: Mosaic Warfare* (Arlington: The Mitchell Institute for Aerospace Studies, 2019), 4, 7–8, 32.

CHAPTER 2
Waging war using AI

AI's greatest strength as a technology is enhancing efficiency. For military forces, its ability to identify patterns and detect items hidden within very large data troves exceptionally quickly stands out. It means AI can be used in fixed systems to analyse many hours of video from drones to find a specific person, or in mobile systems to discern obstacles in its sensor video images or even to take plain language instructions from human managers.

The principal consequence is that AI will make it much easier to detect, localise and identity targets across the battlespace. The battlefield will become transparent; adversary forces will be conspicuous and thereby quickly engaged with precision-guided weapons that have very high probabilities of kill. Both hiding and survival on the future AI-enabled battlefield will become increasingly difficult.

There are two noticeable effects of this. AI seemingly accelerates the decision-making cycle. However, this outcome is dependent on first being able to rapidly determine where the adversary is to allow ordering of decisive action. Quicker decisions are a result of AI's swift find capabilities, not a function of AI. Secondly, AI can also make very useful predictions. Of these forecasts, those which are especially useful are predictions that allow friendly military forces to be correctly positioned to engage adversary forces and thwart their actions. Again, this utility relies on first finding the enemy.

However, AI is not perfect. Well-known problems include being able to be fooled, being brittle in working properly only in the context trained for, being unable to transfer knowledge gained in one task to another and being dependent on data. The difficulties with AI are such that for practical purposes, AI must be teamed with humans. The upside to this is that the strengths of AI counterbalance the weaknesses in human cognition and vice versa: human strengths offset AI shortcomings.

AI is a general-purpose technology that is becoming all-pervasive across society, not least through smartphones. In the same manner, AI will infuse military machines and enable the battlespace. This infusion and enabling is for a specific purpose and, as Robert Work declares, 'The reason to pursue AI is to pursue autonomy'.[61]

There are two basic forms of autonomy: at-rest and in-motion. Autonomy at-rest systems include intelligence support systems, predictive maintenance tools, image recognition solutions and operations planning support. Autonomy in-motion systems include autonomous weapons, platforms and robots. Both the at-rest and in-motion forms are important, and both can employ one of the three main modes of autonomy:

> **Human-in-the-loop.** In this mode, humans retain control of selected functions, preventing actions by the AI without authorisation; humans are integral to the system's control loop. The difficult design issue is how to determine exactly where in the process human intervention should be undertaken, which will vary with the task and the capabilities of the machine. If too much human intervention is needed, its usefulness may be doubtful.
>
> **Human-on-the-loop.** The AI controls all aspects of its operation but humans monitor the operations and can intervene when, and if, necessary. In a variation, at a critical point – such as engaging a target – the AI might notify the human about impending action and either await positive authorisation or continue unless stopped. In contrast, some missile defence systems use human-on-the-loop techniques, whereby the system proceeds unless a human overrules the automated track engagement decision.
>
> **Human-out-of-the-loop.** The AI controls all aspects of system operation without human guidance or intervention. The machine engages without direct human authorisation or notification. This form of control is also termed human-off-the-loop, or fully autonomous.

AI's general-purpose nature means it is likely to be employed initially within existing operational level concepts. In the short-to-medium term, it will enable the battlespace, not remake it. Accordingly, the first section in this chapter discusses extant operational level concepts, while the second section develops two generic, somewhat abstract AI-enabled battlespace concepts: one concerning the defence and the other, the offence. Importantly, these two sections form the foundation for the more detailed and less abstract discussions in Chapters 3, 4 and 5 about specific AI-enabled sea, land and air operational employment concepts.

[61] Robert Work quoted in Kimberly Underwood, 'A Lack of Major Movement Toward Human-Machine Teaming', *Signal*, 2 September 2020. https://www.afcea.org/content/lack-major-movement-toward-human-machine-teaming

The third section in this chapter explores some germane general force-structure issues that the AI-enabled defence and offence concepts imply. These include the implications of AI's commercial origins, manufacturing issues and the idea of prototype warfare.

Operational level concepts

Russia, China and the US each have particular operational level concepts that abstractly describe how they may use their military forces in the battlespace. These concepts are more alike than not, and usefully detail several characteristics of the modern and emerging battlespace and the operations that occur on it. The ideas behind such concepts were first discussed in the interwar period by several Soviet military thinkers. These ideas had gained widespread acceptance by the time the Cold War ended, and were reflected in US AirLand Battle concepts and the successful 1991 Desert Storm campaign. The contemporary Russian, Chinese and US military doctrines and operational concepts have been created based on this heritage.

In the interwar period, Soviet strategists argued that instead of conceptualising the adversary force arrayed on the battlefield in a thin, linear fashion, it should instead be viewed as being a system. The adversary force was much more than solely the frontline of combat soldiers, and included second echelon forces, reserves, indirect fire units, transportation means, logistic support, and command and control elements. Like any system, this force was more than the sum of its parts. Given this, simply attacking the frontline was inadequate as new combat forces were always being moved forward into the frontline.[62] The Soviet thinkers now conceived the enemy as a system but, crucially, this was a system with considerable depth.

Soviet thinkers stressed defeating the system through shock, both physical and cognitive. The aim was to cause system paralysis, neutralising the opposing system's operational rationale so it could not perform the tasks assigned it by the strategic level.[63]

The way to achieve this shock was threefold. First, through placing an operational manoeuvring group into the defence's depth that fragmented the adversary forces, the frontline was then separated from its necessary rear support and overall force cohesion destroyed. Next, simultaneous attack of both the frontline and in depth

[62] John Erickson, 'The Development of Soviet Military Doctrine: The Significance of Operational Art and Emergence of Deep Battle', *The Origins of Contemporary Doctrine*, ed. John Gooch (Camberley: Strategic and Combat Studies Institute, September 1997), 83–92.

[63] Shimon Naveh, *In Pursuit of Military Excellence: The Evolution of Operational Theory* (London: Frank Cass, 1997), 164–208.

compelled the adversary force elements to fight independently, thus: destroying the system's synergies; preventing the adversary force from retiring in good order from the field of battle; stretching the adversary's fighting resources; and interrupting the command and control system's dynamics. Finally, maintaining the momentum relative to the adversary forces disrupted their movement and tempo.[64]

Today's Russian strategists have built on this Soviet legacy and incorporated experiences from campaigns in Syria and the Ukraine. The conceptualisation of the depth of the opposing system has shifted from being simply that of the military forces, as the interwar Soviet thinkers postulated, to encompassing the entirety of the opposing state, including its society. Accordingly, the deep penetration means have been broadened beyond just the military forces originally envisaged, into hybrid warfare, soft-power measures and information warfare. The system paralysis and shock sought to achieve victory is now not just to the adversary's military forces but instead to the functioning of the target state.

Expanding the parameters of system depth in this manner has meant a new stress on the initial period of war (IPW). Somewhat confusingly, the IPW is the phase of a war before the start of combat operations. It is the period during which the soon-to-be warring states conduct operations to create favourable conditions for when their military forces are finally committed.[65] The broad intent of this period of preparing the battlespace is to have pushed the adversary to the edge of defeat by the time hostilities begin through damaging its political and economic circumstances, including by using cyber attacks that disable the adversary's control of their country and armed forces.[66] The IPW will also feature intense reconnaissance activities against the target state.[67]

IPW activities not only increase the 'fog of war' for the adversary but also aim to manipulate them psychologically and cognitively.[68] In recent years, more emphasis has been placed on 'reflexive control', that is the systematic shaping of the adversary's perceptions and thus decisions, so that they voluntarily act in a way favourable to Russia's strategic interests. This is achieved by manipulating the adversary's 'sensory awareness of the outside world' through disinformation,

[64] Naveh, 213–221.

[65] Timothy L. Thomas, *Russian Military Thought: Concepts and Elements* (McLean: The MITRE Corporation, August 2019), 8-5. https://www.mitre.org/publications/technical-papers/russian-military-thought-concepts-and-elements

[66] Thomas, 10-3.

[67] S. G. Chekinov and S. A. Bogdanov, 'Initial Periods of War and Their Impact on a Country's Preparations for Future War', *Voennaya Mysl (Military Thought)*, no. 11 (2012): 24.

[68] Robert O. Work, Chris Dougherty and Paul Scharre. *Transcript from a Virtual Panel Discussion on Emerging Concepts in Joint Command and Control* (Washington: Center for a New American Security, 20 May 2020). https://www.cnas.org/publications/transcript/transcript-from-emerging-concepts-in-joint-command-and-control

repositioning military forces and creating time pressures to alter their understanding of 'the material world.'[69]

In their operational concepts, the Russians place much greater stress on attacking an adversary's cognition than either China or the US. This may be because their long-range strike capabilities are weaker, so compensation is sought by endeavouring to use an adversary's networks against it.[70]

Chinese military thinkers have paid close attention to Russian military thought. The development of the modern PLA has been strongly influenced by Soviet and now Russian strategic thinking, military doctrine and force structure developments.[71] Prominent in this is the PLA's adoption of also viewing war from a system perspective. The PLA considers contemporary military conflict as a 'systems confrontation' between 'opposing operational systems'. Accordingly, the PLA conceives of its war-winning entity as an operational 'system of systems' composed of five subsystems: the command system, the reconnaissance intelligence system, the firepower strike system, the information confrontation system and the support system. The firepower strike system and the information confrontation system are often combined and referred to as the integrated operational force system.[72]

The PLA's theory of victory is based on using information dominance, precision strikes and joint operations to paralyse, or ideally destroy, the critical functions of an enemy's operational system. These cyber, electronic and physical attacks aim to disrupt information flows within the adversary system, degrade its essential elements and nodes, and upset the adversary system's operating tempo. Once the adversary system cannot function effectively and becomes less than the sum of its parts, the enemy will then 'lose the will and ability to resist'.[73]

The PLA has long acknowledged cognition, particularly in terms of the 'three warfares": public opinion, psychological impact and legal warfare.[74] Moreover, there is an emerging interest in cognitive control warfare, which has some resonances with

[69] Can Kasapoglu, *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control* (Rome: NATO Defense College, November 2015), 6. https://www.files.ethz.ch/isn/195099/rp_121.pdf

[70] Work, Dougherty and Scharre. *Virtual Panel Discussion*.

[71] Mandip Singh, *Learning from Russia, How China Used Russian Models and Experiences to Modernize The PLA* (Berlin: Mercator Institute for China Studies, 23 September 2020). https://merics.org/en/report/learning-russia-how-china-used-russian-models-and-experiences-modernize-pla

[72] Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica: RAND Corporation, 2018), ix, 23. https://www.rand.org/pubs/research_reports/RR1708.html

[73] Engstrom, x, 15–17.

[74] Edmund J. Burke et al., People's Liberation Army Operational Concepts (Santa Monica: RAND Corporation, 2020), 15. https://www.rand.org/pubs/research_reports/RRA394-1.html

Russia's 'reflexive control' construct.[75] However, the PLA places greater importance on systems destruction through waging target-centric warfare aimed at either physically destroying the system or disrupting it technically.[76]

In returning to thinking about major wars, the US is beginning by building on its 1980s AirLand Battle concepts, which originally incorporated some Soviet thinking. The US has moved past the former, extended battlefield ideas into new notions of an expanded battlefield across the five domains of land, sea, air, cyber and space. In warfighting throughout these multiple domains, the focus is on achieving so-called convergence: 'the ability to enable any shooter, with any sensor, through any headquarters with the right authorities, in near real time'.[77] This operational concept abandons the older linear kill chains in single domains for resilient, multidomain ones that can leverage alternate or multiple pathways to achieve the same effect.

Like the original Soviet and AirLand Battle ideas, the new US multidomain operations concepts envisage simultaneously engaging the adversary in both close and deep areas. Firepower, manoeuvre and deception will be used to dislocate the enemy forces, fragmenting them physically and cognitively to allow friendly units to penetrate deep into rear areas, gain local superiority and achieve favourable force ratios.[78] This approach is anticipated to impose complexity on the enemy's command and control but, as in the PLA's concept, a significant focus in US thinking is on physical effects.

Russian thinking is also having an influence. In a manner similar to the Russian IPW construct, the US is placing renewed emphasis on the pre-war period, now reconceiving this as a time of continuous competition. The pre-war phase is envisaged to include detailed tactical and operational intelligence preparation of the battlefield, counter adversary reconnaissance activities, deception operations, information warfare and analysis of the operational environment and civil network.

Where the three national concepts all agree is that future war is, to use Chinese terminology, a system confrontation. The Russians and the Chinese include the wider society in envisaging the adversary system, while the US is more constrained, mainly focusing on hostile military forces. In this, Russia, China and the US have all raised the importance of the immediate pre-war period, all essentially

[75] Timothy Thomas, *The Chinese Way of War: How Has it Changed?* (McLean: The MITRE Corporation, June 2020), 29–38

[76] Work, Dougherty and Scharre, *Virtual Panel Discussion*; Burke et al., *People's Liberation Army*, 15–21.

[77] Eric J. Wesley and Robert H. Simpson, *Expanding the Battlefield: An Important Fundamental of Multi-Domain Operations*, Land Warfare Paper 131 (Arlington: Association of the United States Army, April 2020), 4–5.

[78] US Army, *The U.S. Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1 (Fort Eustis: U.S. Army Training and Doctrine Command, 6 December 2018), 25.

agreeing that this is ‘the initial period of war’. All stress fighting close and deep using multidomain attacks including kinetic, electronic and cyber. In this, the US and China are mainly seeking to impose adverse physical and technical effects on the opposing system whereas the Russians place much more emphasis on negatively impacting the adversary’s cognition.

In the short-to-medium term, AI is likely to be applied in ways influenced and shaped by the principal characteristics of these Russian, Chinese and American operational concepts. In retrospect, the main features of the three concepts form a long-term trendline from the interwar period to today and extending into the future. It is within this long-term trendline of operational thinking that AI will both fit and infuse.

AI-enabled battlespace concepts

Considering how AI may affect future warfighting is inherently an exercise in speculation. Nevertheless, much is known in terms of AI’s technology and usefulness. Similarly, future warfighting will involve both defence and offence, and these are useful poles with which to explore AI’s possible effects. Both defence and offence concepts can be unifying ideas that can bring the emerging capabilities that AI offers into sight.

AI’s future warfighting utility might be simply summed up as ‘find and fool’. AI, with its machine learning, is excellent at finding items hidden within a high-clutter background. In this role, AI is better than humans and tremendously faster. However, AI can be fooled through various means. AI’s great finding capabilities lack robustness.

AI’s ‘find’ abilities additionally provide mobile systems with a new level of autonomy, as the AI can analyse its surroundings to find important operating data. This means that both functions of ‘find and fool’ can be enhanced by using supporting mobile and at-rest systems with varying levels of autonomy. AI can bring to the modern warfighting system enhanced sensors, improved kinetic and non-kinetic kill systems, more convincing deception techniques and a wide array of ways to confuse. In this, it is crucial to remember that AI enlivens other technologies. AI is not a standalone actor; rather, it works in combination with numerous other digital technologies and provides them with a form of cognition.

Moreover, AI’s ‘find’ strengths change how the ‘systems confrontation’ between ‘opposing operational systems’ is conceived. Since the late-1990s rise of the network-centric warfare construct, military systems tend to be viewed as battling networks, with the linkages between the various nodes the crucial part. AI changes this. It is now the underlying data – not the communication linkages – that is key. Data brings all else to life and is the new foundation of the emerging AI-enabled ‘systems confrontation’.

A data-centric ecosystem perspective may bring further changes. An example may be the often used Observe–Orient–Decide–Action (OODA) loop that steps through each stage. This is inherently retrospective; an observation cannot be made until after the event has occurred. AI brings a subtle shift. Given suitable digital models and data about both the opponent and the friendly force, AI can predict the future actions an adversary could conceivably take and, from this, the actions the friendly force could take to counter these.

An AI-enabled decision-making cycle might be 'sense–predict–agree–act': AI senses the environment; predicts what the adversary might do and thus what future friendly force response should be; the human part of the human–machine team agrees with this assessment; and AI acts by sending machine-to-machine instructions to the diverse array of warfighting robots deployed en masse across the battlefield.[79] The data fabric on which the 'opposing operational systems' are built may then become the determining factor in battlefield success.

A generic defence concept

Traditionally, the defence has a home-ground advantage in being able to prepare the chosen battlespace. In an AI-enabled battlefield, many low-cost IoT sensors could be emplaced across the selected territory to be defended. Importantly, as this would be completed well in advance of hostilities, the sensors could be carefully placed in the optimum land, sea, air, space and cyber locations. From these, a deep understanding could be gained of the area's terrain, sea conditions, physical environment and local virtual milieu. Having this background data accelerates AI's detection of any changes in the defended territory and, in particular, of the movement of military forces across it. On the AI-enabled battlefield, the pre-combat operations period (the IPW) becomes important to subsequent combat success.

In addition, the defence can make use of AI-enabled, uncrewed vehicles (UVs) for a variety of mobile IoT roles. To support the 'find' function, UVs equipped with sensors could complement the fixed IoT network by roaming the near and far battlespace, providing higher granularity information about specific areas that become of greater interest as the battle evolves, or could temporarily replace any IoT sensors destroyed by hostile action.

The fixed and mobile IoT edge computing sensors could be connected to a robust cloud to reliably feed data back into remote command support systems. The command system's well-trained AI can then very rapidly filter out the important information from the background clutter. Using this information, AI could forecast adversary

[79] A broadly similar command and control flow is discussed in: Clark, Patt and Schramm, *Mosaic Warfare*, 35–40.

actions, and predict optimum own force employment and its likely combat effectiveness. Such predictions combine the sensed environmental data with modelling of the opposing forces' capabilities and performance. Such modelling is an important data task for the pre-combat IPW.

Hostile forces geolocated by AI can, after approval by human commanders, be quickly engaged using indirect fire, including mobile long-range guns, missiles or attack drones. Such an approach can engage close or deep targets, the key issues being data on the targets and the availability of variable range firepower. The result is that the defended territory quickly becomes a no-go zone.

To support the 'fool' function, UVs could be deployed across the battlespace, equipped with a variety of electronic systems suitable for the Counter Intelligence Surveillance and Reconnaissance and Targeting (C-ISRT) function. The intent is to defeat the adversary's AI 'find' systems. In being made mobile through AI, the friendly 'fool' systems will be harder for an adversary to physically attack than a fixed jammer. Moreover, in being semi-expendable, the AI-enabled UVs can be sent on high-risk missions to get close to approaching hostile forces, thereby maximising their jamming effectiveness. Such AI-enabled 'fool' UVs could also play a key role in deception, creating a false and misleading impression of the battlefield to the adversary.

Whether supporting 'find' or 'fool' tasks, the AI-enabled UVs would operate semi-autonomously, transit to nominated locations independently, analyse data from their sensors and communicate with other robots and their remote human commanders to coordinate attacks. This 'edge computing' approach of each robot looking after itself means humans do not need to control each machine individually, sharply lowering communications bandwidth requirements. Instead, an AI-enabled command support system would take mission orders from its human commanders and translate these into broad instructions for each individual robot.

In the reverse manner, the AI-enabled command support system would receive the land, sea, air, space and cyber sensor data and combine this in near real-time with data from the supporting UVs to develop a comprehensive multidomain picture. This gives the human commanders the necessary situational awareness to exercise tactical innovation, be creative and prudently direct the application of force. Acting through the AI-driven command support system, human commanders can give weapons engagement guidance and approval.

A generic offence concept

An offensive has both close and deep battle aspects. The close battle is maintained to ensure hostile forces do not penetrate friendly territory. Simultaneously, mobile forces attempt to break through the adversary frontlines to operate at depth in the adversary's rear. The close battle in the offence might then resemble the defence concept already discussed, with the offence, to an extent, simply added on. In an AI-enabled battlespace, this may be readily possible as many defence functions would be automated.

If, traditionally, the defence has a known-ground advantage, the attacker also has an advantage, in that they can choose the location and timing of the attack. Having the initiative means that the offence can mass UVs in large numbers in both space and time to break through a point in the defender's close battle zone. Given the defender must cover a large front, an attacker can fight attrition battles using semi-expendable UVs to force an opening that human and AI-enabled mobile forces following on can exploit. The intent would be to push the AI-enabled UVs forward so that they are the first to engage the adversary, not humans.

Beyond the close battle area, the attacker becomes vulnerable, given the defender's AI systems and their 'find' capabilities. The larger the penetrating force, the easier it is to find and engage. However, AI-enabled forces that are structured and operated as a swarm may offer a partial solution. AI can both create and help solve the tactical dilemma.

Rather than being by a single large force, the penetration can now be by numerous, small, fast manoeuvre units, connected through the cloud to each other and the command and control system. Each unit is a human–machine team of varying size and capabilities, designed to leverage AI and human strengths while offsetting their weaknesses. These units could mass, exchange target location data, swarm and then attack using their diverse capabilities. The swarm's overall situational awareness would come from each of the units exchanging data and would be supplemented by the more comprehensive surveillance and all-source data analysis provided by the remote AI-enabled command and control system located in friendly territory. Importantly, some of the swarms will undertake 'find' tasks while others perform 'fool' tasks; C-ISRT remains crucial deep into hostile territory.

There are two significant issues. First, each individual unit has limited survivability in being small and, at best, only lightly armoured; each needs to avoid being trapped by a larger adversary. Survivability is achieved by being only a single element within a much larger pack, being mobile, having good situational awareness and by presenting a lower signature than larger units would. Some swarm units could also have electronic jamming and deception roles to assist with force protection. The aim would be to deny an adversary that is targeting quality data primarily through movement and active deception; keeping the adversary uncertain would be critical.

Second, the logistics of these swarm units operating deep within hostile territory presents real difficulties. Historically, such support has proved problematic but, generally, has been provided by air. With an AI-enabled force, UVs of all types may be able to cross hostile ground to carry supplies to meet a swarm unit at an agreed time and place. Some logistics issues may also be eased by relying on off-board sources for intelligence, surveillance and reconnaissance, and exploiting distant fire support, including by air. However, the retrieval of injured personnel is an area of particular concern, although UVs may also assist in this function.

Force structure issues

Given that AI is a commercial technology sold globally, there is considerable expertise in AI in many countries. This propagation is extended by many of the AI algorithms being in the public domain and on-call, commercial cloud computing allowing ready access to considerable processing power. The key missing element is data, which can sometimes be proprietary. Importantly, it is necessary to have the right data for the specific problem being addressed and, at times, this can be difficult to obtain. However, such data may become less important as reinforcement learning and GAN systems are developed that can generate their own training data.

For military purposes, it should be assumed that an adversary could have similar, or even better, AI capabilities than friendly forces. AI is a general-purpose technology for all and sole access is improbable. This extends to non-state actors. The development and deployment of armed hobbyist drones by Islamic State in Iraq suggest that AI-enabled systems can be used by entities other than large states.

Widespread use of AI, especially in smartphones, partly obscures that there are manufacturing supply constraints. The computer chips used in AI are sold widely but are manufactured in few locations. The small number of firms that can design and produce state-of-the-art chips for AI and other purposes are located in the US, South Korea and Taiwan.[80] Moreover, as a consequence of high-capacity chip factories being costly to build, nearly 80% of the world's chip foundries and assembly/test operations have become concentrated in Northeast Asia.[81] Indeed, Taiwan's massive chip factories dominate the world in terms of annual chip output; its factories are at present irreplaceable and essential to meeting global demand.[82]

[80] Bipartisan Policy Center and Center for Security and Emerging Technology, *Artificial Intelligence and National Security* (Washington: Bipartisan Policy Center and Center for Security and Emerging Technology, June 2020), 12–13.

[81] Semiconductor Industry Association, *2020 State of the U.S. Semiconductor Industry* (Washington: SIA Semiconductor Industry Association, 2020), 8. https://www.semiconductors.org/wp-content/uploads/2020/06/2020-SIA-State-of-the-Industry-Report.pdf

[82] Steve Blank, 'The Chip Wars of the 21st Century', *War on the Rocks*, 11 June 2020. https://warontherocks.com/2020/06/the-chip-wars-of-the-21st-century/

China is actively developing its chip-manufacturing capabilities but requires specialised tooling made in the US, the Netherlands and Japan. Using the multilateral Wassenaar Arrangement concerning export controls and various targeted sanctions, the US is attempting to stymie China's plans to increase its in-country chip production from the current level of 10% to 70% by 2025. These constraints are particularly designed to prevent China from being able to mass produce the new, leading-edge, 5-nanometre chips; at present, China can only produce chips as small as 14 nanometres.[83]

Accordingly, the US can use the latest-design computer chips in its weapon systems while China has limits on the sophistication of the chips available to it. Russia, with little national production capability, relies mainly on imports. Some now advocate a ten-nation democratic technology alliance that would actively build chip supply chain resilience, protect critical technologies like tooling from being exported to China or Russia and prevent undesirable technology transfers to either.[84]

Manufacturing is important because, as the two concepts suggest, the AI-enabled battlespace will require large numbers of many different types of devices. The design and large-scale manufacture of these products is increasingly linked to the emerging fourth industrial revolution (4IR) built around digital technology. For military forces, the 4IR means that warfighters can be deeply involved in customising equipment to be optimal for their needs and operating environment.

Tantalisingly, the 4IR creates the possibility of a future defence force structure that rapidly evolves to meet emerging operational demands. The time lag between new challenges arising and technological responses to those challenges will reduce dramatically. Continual innovation may become the dominant quality of future armed forces.

This new paradigm allows the large-scale adoption of the prototype warfare concept. Due to the 4IR, prototypes proven in experimentation programs can now be affordably produced in limited numbers for quick introduction into service. It will be practical to rapidly field a variety of low-cost, less complex systems and then replace these with improved variants or something totally new on a regular basis. This prototype warfare construct is well suited to the demands of the future AI-enabled battlespace. [85]

[83] Assif Shameen, 'Why the US-China Chip War is Heating Up', *The Edge Malaysia Weekly*, 25 September 2020. https://www.theedgemarkets.com/article/tech-why-uschina-chip-war-heating

[84] Martijn Rasser et al., Common Code: An Alliance Framework for Democratic Technology Policy, (Washington: Center for a New American Security, October 2020), 20–22.

[85] Peter Layton, *Prototype Warfare and the Fourth Industrial Age* (Canberra: Air Power Development Centre, 2019), 11–32.

New AI-enabled, autonomous at-rest and in-motion systems could be designed, constructed and manufactured relatively quickly. Such uncrewed systems would simply need to be able to connect to the cloud and be compatible with the command and control system. The 4IR means that AI-enabled systems can be optimised for the forever changing tactical context.

The AI-enabled defence and offence operational concepts that have been developed are generic. They give an indication of the possibilities and spark the imagination but lack granularity. In particular, the concepts are abstractions as far as domains are concerned. In reality, land, sea and air operations are quite dissimilar. The generic concepts need to be placed into each of these three traditional domains and expanded upon. This step is undertaken in the following chapters.

CHAPTER 3
The AI-enabled war-at-sea

War-at-sea both draws on generic warfare concepts and has some unique context-specific matters. In terms of the Russian, Chinese and US operational concepts discussed in Chapter 2, there are strong resonances. The sea battlefield is deep in that it covers vast areas and is also three dimensional, including below the surface. The sea battlefield is less cluttered with people or their structures than on land, allowing opposing navies to clash seemingly unhindered. The oceans are, however, a great global commons used by the ships and aircraft of neutrals, partners and friends who may unexpectedly enter areas of combat operations. Wars at sea are also firmly multidomain, although it is important to have a good understanding of the marine environment, particularly the subsurface. Lastly, war-at-sea between large powers has become very much a war between opposing battle networks. Such conflicts are strongly influenced by technology, its promises and its shortcomings.

Contemporary war-at-sea thinking has some neglected aspects. Historically, the focus when considering war-at-sea has been to disregard that navies are only viable because of land-based support. This is changing as the danger that long-range ballistic and cruise missiles pose becomes more prominent. With this threat, the importance of shore-based, long-range targeting systems has also been highlighted. Even so, the crucial role of ports and shore-based logistic support plays in sustaining war-at-sea remains underemphasised. This may be partly because, since the Second World War, such facilities have been sanctuaries for political or practical reasons. Conceptually, the deep battlefield in war-at-sea ranges from the nearest adversary warship to the depths of the vessel's national – or international – support base.

Adopting such a perspective highlights that simultaneity – that is, simultaneous attacks on the entire depth of the defender's layout – may bring significant gains. Such attacks may force each element of the battle network to fight independently, without the benefits from network synergy. Furthermore, the adversary may be denied retreat; there is now no safe harbour to which to withdraw and adopt a fleet in being strategy.[86] With simultaneous attacks on near and deep targets, the adversary's fighting resources may be stretched to breaking point. Finally, the operational flow of the adversary command and control system may be interrupted, creating a sense of impending, catastrophic battle network fragmentation.[87]

Outside such operational level considerations, war-at-sea evokes visions of ship versus ship combat. Modern surface warships can have great firepower but their reliance on complex electronics means they are relatively fragile and can be rendered out of action by even small missiles. Such a mission kill may not sink the vessel, but it could be removed from battle for an extended period, maybe even for the rest of the war. Warships though are mobile, an attribute useful at the operational level of war in allowing fleets to deploy and manoeuvre relative to each other, and individually in that for a missile to hit a moving ship, it must have a terminal guidance system. Warships are easy for modern sensors located in any domain to detect; there is nothing to hide behind or among on the sea's surface. In contrast, submarines are remarkably hard to find. Unsurprisingly, some consider submarines the capital ships of the modern era, vessels of the first rank that are the great warship killers of our time.[88]

Wars at sea are inherently wars of attrition. The successful delivery of firepower is key, often with simultaneous attrition on both sides. Combat usually involves a series of consecutive weapon engagement sequences where one side follows the other until unable to, or until out of range. In contemporary war-at-sea this would involve several missile salvo pulses back and forth between the two opponents. Such combat is governed by Lanchester's square law of effectiveness: all else being equal, a small advantage in net combat power at the start will be decisive and the effect cumulative.[89] For naval tactics, the principal ambition is to deliver the first effective attack.[90] Modern warships are fragile, and an effective attack by an adversary will immediately reduce the overall task group or fleet combat capabilities considerably. Engaging first should mean an advantage in net combat power is quickly gained and unlikely to be reversed.

[86] Concerning the fleet in being concept see: John B. Hattendorf, 'The Idea of a "Fleet in Being" in Historical Perspective', *Naval War College Review* 67 no. 1 (Winter 2014): 43–60.

[87] Naveh, Pursuit of Military Excellence, 216.

[88] John Keegan, *The Price of Admiralty: The Evolution of Naval Warfare* (New York: Penguin,1988), 317–328.

[89] Niall MacKay, 'Lanchester Combat Models', *Mathematics Today* 42 (2006). https://pure.york.ac.uk/portal/en/publications/lanchester-combat-models(cdc24eeb-4fc6-44ca-9153-972edbd9a154)/export.html

[90] Hughes and Girrier, *Fleet Tactics,* 33, 168, 194.

An inference of this stress on attacking effectively first is that at the tactical level, there is no role for reserves; all should be committed, as nothing in battle is more crucial than delivering superior net combat power. There are also some negatives. Once fired, reloading ships with missiles generally means a return to a distant port and takes considerable time. Accordingly, it is important that the attack made is effective, not wasteful. Moreover, any warship lost means a significant loss of overall naval fleet firepower with potentially serious consequences at the national level. Ruminating over the First World War Battle of Jutland between German and British naval fleets, Winston Churchill later observed that a Royal Navy defeat could have seen Britain 'lose the war in an afternoon'.[91]

Making an effective attack relies on knowing where the adversary's ships are. Wayne Hughes, in his seminal work on naval tactics, writes that:

> At sea, better scouting, more than manoeuvre, as much as weapon range, and often as much as anything else, has determined who would attack – not merely who would attack effectively, but who would attack decisively first.[92]

Accurately determining where ships are in the vast ocean battlefields has traditionally been a difficult task. A great constant of such reconnaissance is that there never seems to be enough. Missiles can come from any direction. Accordingly, the area to be searched expands as the square of the weapon range, and, worryingly, weapons are becoming longer and longer ranged. However, against this, maritime surveillance and reconnaissance technology has been steadily improving since the early 20th century. The focus is now not on collecting information, but on improving the processing of the large troves of surveillance and reconnaissance data collected.[93] Finding the warship 'needle' in the sea 'haystack' is becoming easier.

This chapter discusses waging a naval war in an AI-enabled battlespace, principally through the 'find and fool' AI employment construct. The first section develops a war-at-sea defence concept that is extended to a war-at-sea offence concept in the second section. The final section notes specific force structure issues, including AI standardisation matters, optionally crewed systems and uncrewed ships remaining serviceable during long duration operations.

[91] Winston S. Churchill, *The World Crisis, vol.3* (New York: Charles Scribner's Sons, 1927), 106.

[92] Hughes and Girrier, *Fleet Tactics*, 200.

[93] Hughes and Girrier, 132, 198.

A war-at-sea defence concept

Defence is the more difficult tactical problem during a war-at-sea. Its intent is solely to gain time for an effective attack or counterattack. Hughes goes as far to declare that: 'All fleet operations based on defensive tactics … are conceptually deficient'.[94] Hughes's perspective is informed by careful analysis and historical examples; however, in the AI-enabled battlefield, there may be some subtle new twists.

Sensor field deployment

The generic defence concept in Chapter 2 envisaged a large IoT sensor field distributed across areas that hostile forces might move into or through. Such a concept is becoming possible in the maritime domain, given the developments in AI and associated technology.

DARPA's Ocean of Things (OoT) program aims to achieve maritime situational awareness over large ocean areas through deploying thousands of small, low-cost floats that form a distributed sensor network. Each smart float will have a suite of commercially available sensors to collect environmental and activity data; the latter function involves automatically detecting, tracking and identifying nearby ships and potentially close aircraft traffic. The floats use edge processing with detection algorithms, and periodically transmit the semiprocessed data to a cloud network, via the Iridium satellite, for on-shore storage. Real-time analysis using AI machine learning is then used to uncover insights from the sparse data.[95] The floats are environmentally friendly, have a life of around one year and, in purchases of 50,000, have a unit cost of about US$500. DARPA's OoT shows what is feasible using AI.

In addition to floats, there are numerous other low-cost mobile devices that could expand the OoT's capabilities. Indicative systems include:

> **EMILY Hurricane Tracker.** This uncrewed boat, measuring less than 2 m long, can operate in heavy weather for 5 to 10 days cruising at about 7 knots. It has a satellite link, video camera, hyperspectral imagers and a simple sonar.[96]

[94] Hughes and Girrier, 33, 166.

[95] John Waterston, 'Ocean of Things', Defense Advanced Research Projects Agency, accessed 9 January 2021, https://www.darpa.mil/program/ocean-of-things; 'DARPA Takes the IoT to Sea, *GCN*, 3 January 2020. https://gcn.com/articles/2020/01/03/darpa-ocean-of-things.aspx

[96] John Keller, 'Not Just for the Navy: Unmanned Surface Vessels (USVs) in Wide Use for Surveillance at NOAA', *Military & Aerospace Electronics*, 29 March 2016. https://www.militaryaerospace.com/unmanned/article/16714492/not-just-for-the-navy-unmanned-surface-vessels-usvs-in-wide-use-for-surveillance-at-noaa

Ocean Aero Intelligent Autonomous Marine Vehicles. These wind-powered and solar-powered ocean drones can both sail and submerge, and are capable of extended station keeping and monitoring. Rechargeable lithium-ion batteries power command systems, collision avoidance, sensor payload functions and satellite communications. Endurance is 3 months, with some versions including up to 8 days submerged.[97]

Seaglider Autonomous Underwater Vehicle. The 2 m long vehicle can carry a variety of sensors, passing data to a shore station via an Iridium satellite link that is also used for control. Seaglider has a maximum range of 4,600 km, typically involving 650 dives to depths of up to 1,000 m. Its maximum endurance is about 10 months.[98]

Liquid Robotics Wave Glider. The Wave Glider uses wave and solar power to continuously acquire data from the ocean surface for up to 12 months. Several have sailed autonomously between San Francisco and Australia (Hervey Bay), a 17,000 km journey.[99] Wave Gliders can also operate in fleets to create a data collection network.[100] In a 2015 UK Government mission around the Pitcairn Islands, a Wave Glider operated with an automatic identification system receiver, acoustic sensors and camera. The high definition camera (1080 pixels) captured images of vessel targets and sent thumbnails via an Iridium satellite back to a command centre. The Wave Glider then sailed itself some 5,200 km to Hawaii.[101] Wave Gliders can be fitted with thin line towed array sonars and electronic surveillance equipment.[102]

[97] Ocean Aero, *Ocean Aero Autonomous Underwater and Surface Vehicles* (San Diego: Ocean Aero, 2020). http://ems-ocean.com/catalogue2/Ocean%20Aero/OA%20AUSVs%202.19.pdf

[98] Kongsberg, *Seaglider* (Horten: Kongsberg, May 2014). https://www.hydroid.com/sites/default/files/product_pages/Seaglider_Data_Sheet.pdf

[99] Clay Dillow, 'Oceangoing Robot Comes Ashore in Australia, Completing a 9,000-Mile Autonomous Pacific Crossing', *Popular Science*, 5 December 2012. https://www.popsci.com/technology/article/2012-12/oceangoing-robot-comes-ashore-australia-completing-9000-mile-autonomous-pacific-crossing/

[100] Liquid Robotics, *The Wave Glider: Transform How You Understand the Ocean* (Sunnyvale: Liquid Robotics, 2017). https://www.seismic.com.au/assets/pdf/Liquid-Robotics-WG_DataSheet-1-2_web.pdf

[101] Liquid Robotics, *Liquid Robotics Case Study: Monitoring Marine Protected Areas* (Sunnyvale: Liquid Robotics, 2017), https://cdn2.hubspot.net/hubfs/287872/website-downloads/lr-cs-Pitcairn-mda_FINAL_web.pdf; Mike Ball, 'Liquid Robotics Wave Glider USV Travels More Than 2800 Nautical Miles', *Unmanned Systems Technology*, 7 July 2016. https://www.unmannedsystemstechnology.com/2016/07/liquid-robotics-wave-glider-usv-travels-more-than-2800-nautical-miles/

[102] 'SEA Provides Leading ASW Sensor System for Australian Autonomous Surveillance Capability Trial', *EDR Online*, 15 October 2020, https://www.edrmagazine.eu/sea-provides-leading-asw-sensor-system-for-australian-autonomous-surveillance-capability-trial; Joseph Trevithick and Tyler Rogoway, 'Mysterious Wave Glider Spotted Off Florida Keys Had Electronic Intel Gathering System (Updated)', *The Drive,* 29 June 2020. https://www.thedrive.com/the-war-zone/34485/mysterious-wave-glider-vessel-spotted-off-florida-keys-has-electronic-intel-gathering-system.

Ocius Technology Bluebottle. This uncrewed, autonomous, 5 kt surface vessel operates on solar, wave and wind power and can carry a payload of some 300 kg, including thin line sonar arrays, radar, 360-degree cameras, automatic identification system and other sensors. Bluebottle incorporates AI neural networks, edge computing processing of sensor signals, low bandwidth communication links and a 'team' based software architecture where peer vessels independently manoeuvre to achieve the group's assigned common goals, such as making an interception. In 2021, five Bluebottles operating as an intelligent network will patrol the northern Australian Indian Ocean waters fitted with a payload able to detect unauthorised vessels, alert a shore-based command centre and then approach the intruder for detailed investigation.[103] Future concepts include several vessels acting together as a wide area sonar array to detect submarines and a single Bluebottle acting as a 'gateway node' between underwater UVs or a seabed sensor system and a shore-based data centre.[104]

In addition to the emerging mobile, low-cost autonomous devices plying the sea, there is an increasing number of small satellites (smallsats) being launched by governments and commercial companies into low Earth orbit to form large satellite constellations. Most of these will use AI and edge computing, and some will have sensors able to detect naval vessels visually or electronically.[105] For example, Kelos is launching smallsats with radio frequency sensors able to detect and geolocate concealed maritime activity, such as fishing vessels not activating their automatic identification system or when weather conditions are unfavourable for imagery. The company aims to deliver radio frequency Reconnaissance Data-as-a-Service to governments and commercial organisations.[106]

There is also the existing large array of more traditional military maritime surveillance and reconnaissance systems, ranging from space-based systems, to crewed aircraft, to surface ships and undersea sensors. The latest system introduced into service is the MQ-4C Triton UAV, with a range of some 15,000 km and endurance of up to 30 hours.[107] In time, the system's capabilities could be significantly

[103] Sandy Milne, 'Bluebottle USVs Green-Lit for Autonomous Operation', *Defence Connect*, 8 July 2020. https://www.defenceconnect.com.au/strike-air-combat/6414-bluebottle-usvs-green-lighted-for-autonomous-operation

[104] Ewen Levick, 'Ocius Launches Latest USV', *ADM: Australian Defence Magazine*, 27 August 2020. https://www.australiandefence.com.au/news/ocius-launches-latest-usv

[105] William Williamson, 'From Battleship to Chess', *USNI Proceedings*, 146/7/1,409, July 2020. https://www.usni.org/magazines/proceedings/2020/july/battleship-chess

[106] 'Kleos Scouting Mission Smallsats Deployed', *Satnews*, 10 November 2020. https://news.satnews.com/2020/11/10/kleos-scouting-mission-smallsats-deployed/

[107] Richard R. Burgess, 'Triton Deploys at Last: The Navy Takes Its New UAV to the Western Pacific', *Seapower*, 29 April 2020. https://seapowermagazine.org/triton-deploys-at-last-the-navy-takes-its-new-uav-to-the-western-pacific/

enhanced through AI.[108] The next advance may be the USN's proposed medium unmanned surface vessel (MUSV), a 500 ton vessel with intelligence, surveillance and reconnaissance payloads and electronic warfare systems, intended to cruise autonomously at 15 kts for some 60 days, with a 8,000 km range and the ability to be refuelled at sea.[109]

With so many current and emerging maritime surveillance systems, the idea of a digital ocean is becoming practical. This concept envisages the data from thousands of persistent and mobile sensors being processed by AI, analysed though machine learning and fused into a detailed ocean-spanning, three-dimensional comprehensive picture.[110] Oceans remain large expanses, making this a difficult challenge. However, a detailed near real-time digital model of smaller spaces – such as enclosed waters like the South China Sea, national littoral zones or limited ocean areas of specific import – appears practical using current and near-term technology.

Being able to create a digital ocean model may prove revolutionary. At the least, it will noticeably advance the long-term trend of increasingly better scouting. Professor William Williamson, of the USN Naval Postgraduate School, declares:

> On the "observable ocean", the Navy must assume that every combatant will be trackable, with position updates occurring many times per day. Never again will it face an enemy incapable of locating the … fleet beyond the horizon. In short, the Navy will have lost the advantages of invisibility, uncertainty and surprise. The level of detail available to adversaries will enable them to fuse multiple modes of information - imagery, radar and signals - not only to determine ships' locations, but also to infer the health and operational status of the vessels and to monitor logistical considerations. Vessels will be observable in port, and the number and type of supplies brought on board will also be subject to near-real-time observation. When a ship departs, the preparations will be noted and the time of departure known to within hours or even minutes. This is true for submarines as well as for surface ships.[111]

[108] George Galdorisi, 'The Navy Needs AI, It's Just not Certain Why', *USNI Proceedings,*145/5/1,395, May 2019. https://www.usni.org/magazines/proceedings/2019/may/navy-needs-ai-its-just-not-certain-why

[109] Bryan Clark and Timothy A. Walton, *Taking Back the Seas: Transforming the U.S. Surface Fleet for Decision-Centric Warfare* (Washington: Center for Strategic and Budgetary Assessments, 2019), 65. https://csbaonline.org/uploads/documents/Taking_Back_the_Seas_WEB.pdf

[110] Liquid Robotics, *The Digital Ocean: How Systems Can Work Together to Solve Our Planet's Biggest Challenges*, last modified 2016. http://cdn2.hubspot.net/hubfs/287872/LR_DigitalOcean_eBook.pdf

[111] Williamson, 'From Battleship to Chess', paragraph 16.

Defending warships

In a future major conflict, the default assessment by each warship's captain will be that the adversary probably knows the ship's location. Defence then moves from being 'conceptually deficient' to being the foundation of all naval tactics in an AI-enabled battlespace. The emerging AI-enabled maritime surveillance system of systems will potentially radically change traditional war-at-sea thinking. The 'attack effectively first' mantra may need to be rewritten to 'defend effectively first'.

The digital, 'observable ocean' will ensure warships are aware of approaching hostile warships and the consequently increasing risk of attack. To address this, three broad, alternative approaches for the point defence of a naval task group might be considered. First, warships might cluster together to concentrate their defensive capabilities and avoid any single ship being overwhelmed by a large multi-axis, multimissile attack. In this, AI-enabled ship-borne radars and sensors will have improved capabilities to track incoming missiles among the background clutter. Moreover, AI-enabled command systems will also be able to prioritise and undertake missile engagements much more rapidly. Nearby AI-enabled USVs may switch on active illuminator radars, allowing crewed surface combatants to use the received reflections to create fire control quality track data. The speed and complexity of the attacks will probably mean that human-on-the-loop is the generally preferred AI-enabled ship weapon system control, switching to human-out-of-the-loop as the number of incoming missiles rises or more hypersonic missiles are faced.

Next, instead of clustering, warships might scatter so that an attack against one will not endanger others. Crucially, modern technology now allows dispersed ships to fight together as a single package. The 'distributed lethality' concept envisages distant warships sharing precise radar tracking data across a digital network, forming a composite picture from the various inputs and then using this detailed picture to engage hostile targets – even if they themselves do not directly hold the target on their own radar.[112] In this scenario, there are issues of data latency that limit how far apart the ships that are sharing data for this purpose can be. An important driver of the 'distributed lethality' concept is to make adversary targeting more difficult. With the digital ocean, this driver may be becoming moot.

Finally, the defence in depth construct offers new potential through becoming AI-enabled, particularly when defending against hostile submarines, although the basic ideas also have value against surface warship threats. In areas through which adversary submarines may transit, stationary, relocatable sensors – like the USN's

[112] Peter Layton, 'Fifth Generation Surface Warfare Fleet Emerges', *Defence Today,* September 2017, 13–18.

Transformational Reliable Acoustic Path System – could be employed, backed up by unpowered, long endurance gliders towing passive arrays. These passive sonars would use automated target recognition algorithms supported by AI machine learning to identify specific underwater or surface contacts.[113] The experimental uncrewed Sea Hunter, noted earlier as using both first-wave and second-wave AI, was originally designed under the Continuous Trail Unmanned Vessel program. The vessel's primary mission was envisaged as tracking quiet diesel–electric submarines by detecting, localising and then trailing a submarine continuously.[114] The USN's projected new MUSVs may be used in this role as well.

Closer to the friendly fleet, autonomous MUSVs could use low frequency, active, variable depth sonars supplemented by medium-sized uncrewed underwater vehicles with passive sonar arrays. Surface warships or the MUSVs could further deploy small uncrewed underwater vehicles carrying multistatic, active coherent sensors already fielded in expendable sonobuoys.[115] Warships could employ passive sonars to avoid counter-detection and take advantage of multistatic returns from the active variable depth sonars deployed by MUSVs.[116]

Fool function AI

The digital ocean significantly increases the importance of deception and confusion operations. This 'fool' function of AI may become as vital as the 'find' function, especially in the defence. In the war-at-sea, the multiple AI-enabled systems deployed across the battlespace offer numerous possibilities for fooling the adversary.

Deception involves reinforcing the perceptions or expectations of an adversary commander and then doing something else. However, its effectiveness is rather uncertain, as the thinking of the other commander will always be somewhat unknown. Even so, in being a low-risk tactic, it is worth employing, whether or not it works. To do so, multiple false cues will need seeding, as some clues will be missed by the adversary, and having more than one will only add to the credibility of the deception.[117] For example, a number of USVs could set sail as the warship leaves port,

[113] Bryan Clark, Seth Cropsey and Timothy A. Walton, *Sustaining the Undersea Advantage: Disrupting Anti-Submarine Warfare Using Autonomous Systems* (Washington: Hudson Institute, September 2020), 7–9. https://s3.amazonaws.com/media.hudson.org/Clark%20Cropsey%20Walton_Sustaining%20the%20Undersea%20Advantage.pdf

[114] Joseph Trevithick, 'Navy's Sea Hunter Drone Ship Is Getting a New Owner, New Abilities, and a Sister', *The Drive*, 6 February 2020. https://www.thedrive.com/the-war-zone/18264/navys-sea-hunter-drone-ship-is-getting-a-new-owner-new-abilities-and-a-sister

[115] Multi-Static Active Coherent (MAC) System as outlined in the Director, Operational Test and Evaluation, *FY 2015 Annual Report*, (Washington: Department of Defense, January 2016), 263-265. https://www.dote.osd.mil/Portals/97/pub/reports/FY2015/other/2015DOTEAnnualReport.pdf?ver=2019-08-22-105555-363

[116] Clark and Walton, *Taking Back the Seas*, 36.

[117] Hughes and Girrier, *Fleet Tactics*, 251.

all actively transmitting a noisy facsimile of the warships electronic or acoustic signature. The digital ocean may then suggest to the commander multiple identical warships are at sea, creating some uncertainty as to which is real.

In terms of confusion, the intent might not be to avoid detection as this might be very difficult, but to prevent an adversary from classifying vessels detected as warships or identifying them as a specific class of warship. This might be done using some of the large array of AI-enabled floaters, gliders, autonomous devices, underwater vehicles and USVs to confuse the digital ocean picture.[118] The aim would be to change the empty oceans – or at least the operational area – into a seemingly crowded, cluttered, confusing environment, where detecting and tracking the real warships being sought is problematic and, at best, fleeting. If AI can find targets, AI can also obscure them.

A war-at-sea offence concept

The offence begins from the defence. The aim is to defend against a hostile attack for long enough to reach a missile-firing position suitable for engaging the adversary fleet. In a conflict where both sides are employing AI-enabled systems, targeting adversary warships may become problematic. The 'attack effectively first' mantra may further evolve to simply 'attack effectively'. Missiles that miss their target represent a significant loss of the task group's or fleet's net combat power and take considerable time to be replaced. Several alternatives may be viable.

In a coordinated attack, the offence might use a mix of crewed and uncrewed vessels. One option is to use three ships: a large, well-defended, crewed ship that carries a considerable number of various types of long-range missiles, but which remains remote to the high threat areas; a smaller, crewed warship pushed forward into the area where adversary ships are believed to be, both for reconnaissance and to provide targeting for the larger ship's long-range missiles; and an uncrewed, stealthy ship operating still further forward in the highest risk area, primarily collecting crucial, time-sensitive intelligence and passing this back through the smaller crewed warship onto the larger ship in the rear.

The logic of the coordinated attack is that close to the adversary fleet, there will be extensive electronic deception and jamming. Two-way communications are likely to be unreliable and subject to repeated interference, making controlling or connecting with autonomous vessels at long-range difficult. However, the three vessels cooperating at somewhat shorter ranges may be able to work through the electronic interference sufficiently to pass high-quality targeting data back from the small, close-in, uncrewed ship to the crewed vessel and then on to the distant, missile-carrying, large warship.

[118] Clark and Walton, *Taking Back the Seas*, 28.

The intermediate, small, crewed vessel can employ elevated or tethered systems and uncrewed communications relay vehicles to receive the information from the forward uncrewed vessel, and act as a robust survivable gateway into the fleet's tactical grid through using resilient communications systems and networks. Moreover, by being closer to the uncrewed vessel, the intermediate, smaller crewed vessel will be able to control it as the tactical situation requires and, if the context changes, adjust the uncrewed vessel's mission.

This intermediate ship will probably also have small numbers of missiles available to use *in extremis* if the backward link to the larger missile ship fails. Assuming that communications to all elements of the force will be available in all situations may be unwise. The group of three ships should be network enabled, not network dependent, and this could be achieved by allowing the intermediate ship to be capable of limited independent action.[119]

The coordinated attack option is not a variant of the distributed lethality concept noted earlier. The data being passed from the stealthy, uncrewed ship and the intermediate, crewed vessel is targeting – not fire control – data. If it were the latter, the integration would need to be much tighter as the quality would need to be high and the data latency very low.[120] The coordinated attack option has only loose integration that is both less technically demanding and more appropriate to operations in an intense electronic warfare environment.

An alternative concept is to have a crewed, large vessel at the centre of a networked constellation of small-sized and medium-sized, uncrewed air, surface and subsurface systems.[121] A large ship offers potential advantages in being able to incorporate advanced power generation to support emerging defensive systems like high energy lasers or rail guns. In this, the large, crewed ship would need good survivability features; suitable defensive systems; an excellent command and control system to operate its multitude of diverse, uncrewed systems; and a high bandwidth communication system linking back to shore-based facilities and data storage services.

The crewed ship would employ mosaic warfare techniques to set up extended kinetic and non-kinetic kill webs through the uncrewed systems to reach the adversary warships. The ship's combat power is not then in the crewed vessel but principally in its

[119] Jeffrey E. Kline, 'Impacts of the Robotics Age on Naval Force Design, Effectiveness, and Acquisition', *Naval War College Review* 70, no. 3 (Summer 2017): 77. https://digital-commons.usnwc.edu/nwc-review/vol70/iss3/5

[120] Megan Eckstein, 'Wargames This Year to Inform Future Surface Combatant Requirements', *USNI News*, 21 February 2017. https://news.usni.org/2017/02/21/wargames-future-surface-combatant-requirements

[121] Harry Bennett, 'Capital Ship 2035: The Mission Command Vessel (MCV)', *Center for International Maritime Security*, 31 August 2017. https://cimsec.org/capital-ship-2035-mission-command-vessel-mcv/33891

uncrewed systems, with their varying levels of autonomy, AI application and edge computing. The large ship and its associated constellation would effectively be an at-sea form of the Soviet reconnaissance–fire complex. [122]

An AI-enabled war-at-sea might involve duelling constellations, each seeking relative advantage. Sidharth Kaushal usefully observes that:

> [Large warships] may have a role … in a future dominated by distributed networks of cheap assets. Despite the growing importance of smaller distributed manned and unmanned assets, middleweight ships which can be built in large enough numbers to not represent a single point of failure but which have an organic capacity for battle management and command and control will be critical to ensuring that networks of distributed assets retain coherence. As such, a distributed future fleet of small [crewed and uncrewed] vessels may yet find itself knitted together by large surface combatants.[123]

Two new proposed uncrewed vessels might support both the coordinated attack option and the networked constellation ship alternative. The first may be an arsenal ship that carries large numbers of missiles to increase the weight of any attack substantially. The USN is actively developing a large USV, of some 1,000–2,000 ton displacement, to be an external missile magazine that can autonomously sail to the fleet, expend its missiles as required and then return to port to be reloaded.[124] The concept envisages that large USVs will be capable of semi-autonomous or fully autonomous operation, with the firing of weapons authorised by remote operators at sea or in shore-based control stations using human-in-the-loop or human-on-the-loop autonomy.[125]

The second type of proposed vessel is an extra-large, uncrewed, underwater vehicle that would be launched from shore, not from a transporting ship or submarine. Such vehicles are planned to have a range of up to 13,500 kms, accommodate a modular payload section and periodically establish communications to receive

[122] Kline, *Impacts*, 76.

[123] Sidharth Kaushal, 'The Type 055: A Glimpse into the PLAN's Developmental Trajectory', *RUSI Defence Systems 22*, no. 1 (19 October 2020). https://rusi.org/publication/rusi-defence-systems/type-055-glimpse-plan%E2%80%99s-developmental-trajectory

[124] David B. Larter, '5 Things You Should Know about the US Navy's Plans for Autonomous Missile Boats', *Defense News*, 13 January 2020. https://www.defensenews.com/digital-show-dailies/surface-navy-association/2020/01/13/heres-5-things-you-should-know-about-the-us-navys-plans-for-big-autonomous-missile-boats/

[125] 'U.S. Navy Selects Lockheed Martin to Deliver Large Unmanned Surface Vessel Study', *Navy Recognition*, 18 September 2020. https://www.navyrecognition.com/index.php/news/defence-news/2020/september/9005-u-s-navy-selects-lockheed-martin-to-deliver-large-unmanned-surface-vessel-study.html

or transmit data to distant ships or shore bases.[126] Such vessels may be able to contribute to planned attacks or assist in providing targeting data in high threat environments.[127] In being uncrewed, they can be risked and, if need be, risked to gain critical information.

A more complicated attack option may be that noted previously: using swarm tactics. While dangerous in constrained littoral environments, swarm attacks using uncrewed surface craft may be less effective further at sea where high speeds are harder to attain. Some have suggested swarming sea mines but, again, this seems useful mainly in shallow littoral waters.[128]

In the AI-enabled offence concept, there are two issues of concern. The uncrewed vessels envisaged in the coordinated attack option may be expendable *in extremis* but they are not meant to be expended. Their loss would adversely affect the overall combat effectiveness of the task group or fleet. Much of the current design work on the larger USVs has focused on the leading-edge electronics and information technology needed to make the concepts practical. Their hull design and general configuration has, accordingly, been more conventional and is often based on that of crewed ships.

DARPA and the USN are now considering No Manning Required Ship (NOMARS) designs. Such fully robotic ships would bring several advantages, but the most important combat benefit would be increased survivability through being able to achieve the same combat power from a smaller, stealthier, more agile ship.[129] The additional benefits expected include reduced size, lower acquisition and sustainment costs, improved at-sea reliability, better performance in high sea states and hydrodynamic efficiency from not needing to consider crew safety or comfort.[130] Given AI's expected technological development path, NOMARS vessels appear inevitable.

[126] Valerie Insinna, 'Navy to Kick Off Extra Large UUV Competition This Month', *Defense News*, 10 January 2017. https://www.defensenews.com/digital-show-dailies/surface-navy-association/2017/01/10/navy-to-kick-off-extra-large-uuv-competition-this-month/

[127] David B. Larter, 'To Compete with China, an Internal Pentagon Study Looks to Pour Money into Robot Submarines', *Defense News*, 1 June 2020. https://www.defensenews.com/naval/2020/06/01/to-compete-with-china-an-internal-pentagon-study-looks-to-pour-money-into-robot-submarines/

[128] Zachary Kallenborn, 'Swarming Sea Mines: Capital Capability?', *Center for International Maritime Security*, 29 August 2017. http://cimsec.org/swarming-sea-mines-capital-capability/33836

[129] Mallory Shelbourne, 'DARPA Testing the Limits of Unmanned Ships in New NOMARS Program', *USNI News*, 2 November 2020. https://news.usni.org/2020/10/27/darpa-testing-the-limits-of-unmanned-ships-in-new-nomars-program

[130] David B. Larter, 'DARPA's Latest Mad Science Experiment: A Ship Designed to Operate Completely Without Humans', *Defense News*, 21 January 2020. https://www.defensenews.com/naval/2020/01/21/darpas-latest-mad-science-experiment-a-ship-designed-completely-without-humans/

Secondly, deploying uncrewed vessels into and out of distant combat zones can be difficult, given that their smaller size means their range is reduced and they are more affected by higher sea states. DARPA's sea train concept entails several USVs sailing connected or in collaborative formations to reduce hull drag and gain cruise efficiencies. The concept envisages four or more AI-enabled autonomous USVs joining up, transiting 12,000 km, disaggregating to individually conduct separate tasks and then later reassembling for return transit.[131] With such concepts, USVs may not need to be resupplied at sea under hazardous operational conditions but would, instead, return to port after a replacement sea train arrived.

Force structure issues

By design, the AI-enabled battlefield diffuses AI and its associated technologies widely, having proven systems and common standards in areas such as autonomy, algorithms, data management, machine-learning techniques, edge computing, networks and control stations. Modern warships may be built to new hull designs but they deliberately use existing weapons systems, sensor packages and command and control systems rather than design everything new each time. In a similar way, designers of new AI-enabled, uncrewed vessels may focus on unique aspects of importance while incorporating agreed AI standards, common core technologies and already developed systems.[132]

AI-enabled, uncrewed designs have distinct advantages over crewed ship designs, as the NOMARS concept suggests. In the maritime domain, though, being crewed does address some concerns. In peace or war, uncrewed vessels may be susceptible to being captured or boarded as there are no crews to fight off intruders. For example, the PLA Navy abducted – and later returned – a Solcum Sea Glider operating in the eastern South China Sea just as a USN research vessel was trying to retrieve it.[133] Similarly, in January 2018, Houthi forces captured a USN REMUS 600 uncrewed underwater vessel found off the coast of Yemen.[134]

[131] Brandi Vincent, 'DARPA Wants Help Developing a "Sea Train" of Unmanned Warships', *Nextgov*, 9 January 2020. https://www.nextgov.com/emerging-tech/2020/01/darpa-wants-help-developing-sea-train-unmanned-warships/162342/; John Keller, 'Pentagon Gets Serious about Unmanned Surface Vessels', *Military & Aerospace Electronics*, 29 September 2020. https://www.militaryaerospace.com/unmanned/article/14184308/unmanned-surface-vessels-usv

[132] Megan Eckstein, 'Common Standards, Software Key to Navy's Common Standards Unmanned Systems Future Unmanned Systems', *USNI News,* 10 September 2020. https://news.usni.org/2020/09/10/common-standards-software-key-to-navys-future-unmanned-systems

[133] Tyler Rogoway, 'China Gives Drone Back—But Why Did They Grab It in The First Place?', *The Drive*, 20 December 2016. https://www.thedrive.com/the-war-zone/6604/china-gives-drone-back-but-why-did-they-grab-it-in-the-first-place

[134] Ben Werner, 'VIDEO: Houthi Forces Capture U.S. Navy Unmanned Underwater Vehicle Off Yemen', 3 January 2018, *USNI News*. https://news.usni.org/2018/01/03/houthi-rebels-find-likely-u-s-navy-unmanned-underwater-vehicle

Such possibilities may constrain what systems are placed on AI-enabled, uncrewed vessels, especially when undertaking peacetime tasking. Such vessels might be used in peacetime or times of crisis for data collection; however, the possibility of their capture may mean the onboard systems are those whose compromise is acceptable. There are a variety of possible anti-tamper methods and intruder warning systems that could be installed, but all have their shortcomings. It may be prudent for AI-enabled, uncrewed vessels on peacetime missions to use readily available commercial systems rather than the possibly more capable classified systems.[135]

The recent development of large uncrewed vessels has raised concerns over reliability. Larger ships have always been designed assuming that the onboard crew can both maintain the vessels and repair any failures. Ship engines, for example, are not designed to run for 90 days without human oversight and maintenance, but new uncrewed vessel concepts are seeking such performance levels. Beyond reliability, there are other issues about addressing mechanical failures at sea, the degree of redundancy needed and the actions to take when warned of impending failure.[136]

Maintenance issues are more ones of applied engineering than of innovation. Indeed, AI, with its expanding role in predictive maintenance, may solve many concerns. Some argue that AI-enabled, uncrewed vessels should be thought of more as satellites than as traditional ships. Satellites are self-contained, self-aware, have backup systems, operate in a harsh environment and can reconfigure themselves if needed to achieve a mission. Such a conceptualisation could help inform AI-enabled, uncrewed vessel reliability and maintenance design aspects.[137]

The AI-enabled battlespace creates a different war-at-sea. Most obvious are the autonomous systems and vessels made possible by AI and edge computing. However, the bigger change may be to finally take the steady scouting improvements of the last 100 years or so to their final conclusion. The age of AI, machine learning, big data, IoT and cloud computing appear set to create the 'observable ocean'. By combining these technologies, near real-time digital models of the ocean environment can be made that highlight the man-made artefacts present.

[135] Megan Eckstein, 'Navy to Field "Optionally Unmanned" Vessels to Supplement Future Surface Combatant', *USNI News*, 25 June 2018. https://news.usni.org/2018/06/25/navy-looking-at-optionally-unmanned-vessel-to-supplement-future-surface-combatant-program

[136] Megan Eckstein, 'Program Office Maturing USVs, UUVs with Help from Industry, International Partners', *USNI News*, 23 June 2020. https://news.usni.org/2020/06/23/program-office-maturing-usvs-uuvs-with-help-from-industry-international-partners

[137] Megan Eckstein, 'Navy, Industry Pursuing Autonomy Software, Reliable HM&E Systems for Unmanned Ships', *USNI News*, 31 January 2020. https://news.usni.org/2020/01/31/navy-industry-pursuing-autonomy-software-reliable-hme-systems-for-unmanned-ships

The digital ocean means that warships become the prey as much as the hunters. Such a perspective, however, brings a shift in thinking about what the capital ship of the future might be. Capital ships were originally conceived as being of the first rank; navies could be built around them, and they posed a clear and present danger to all lesser warships. Sailing 'ships of the line' were the first capital ships; by the early 1900s, it was the great dreadnoughts, then, in the mid-20th century, aircraft carriers emerged. As noted, some now argue that the title has passed to submarines.[138]

Now a new capital ship may be emerging. A recent study looked at the development of the new digital technologies, including AI, and concluded that the 'Navy's next capital ship will not be a ship. It will be the Network of Humans and Machines, the Navy's new centre of gravity, embodying a superior source of combat power'.[139] Tomorrow's capital ship looks set to be the human–machine teams operating on the future AI-enabled battlefield.

[138] John L. Fleming, *Capital Ships: A Historical Perspective* (Newport: Naval War College, 1994), 4–20.

[139] 'The Network of Humans and Machines as the Next Capital Ship', CNO Strategic Studies Group 35 Final Report (31 July 2016), quoted in Bill Glenney, 'Institute For Future Warfare Studies Wants Your Writing On The Capital Ship Of The Future', *Center for International Maritime Security*, 18 July 2017, paragraph 1. http://cimsec.org/institute-for-future-warfare-studies-wants-your-writing-on-the-capital-ship-of-the-future/33307

CHAPTER 4
The AI-enabled war-on-land

At the operational level, the war-on-land generally accords with the generic warfare concepts. The battlefield can be deep, extending into hostile territory, although not as far as in sea or air warfare. However, unlike the air and sea battlefields, the land battlefield is heavily cluttered with people and their structures that significantly obstruct and constrain the clash of the opposing military forces. Over the last century, wars on land have steadily become multidomain, with the addition of cyber and space further expanding this long-term trend. Similarly, since the later part of the Cold War, a war-on-land between large, well-equipped, modern armies has increasingly become considered as a war between opposing battle networks. At the moment, though, this is mostly prophesy. There have been no recent, large-scale conflicts between leading-edge land forces where both sought victory through employing a 'systems confrontation' between 'opposing operational systems'.

In 1926, Colonel J. F. C Fuller ended his book, judged at the time as the first that applied science to the art of war, with a capitalised maxim: 'GUARD, MOVE, HIT'.[140] Across various usages, the precise words vary, but Fuller's underlying logic has proven compelling. Ever since, land forces have been framed in terms of protection, mobility and firepower.[141]

Protection involves a military unit protecting itself, not others. Such protection may be active, such as through using armour, or passive, such as using camouflage. Mobility

[140] Colonel J. F. C. Fuller, *The Foundations of the Science of War* (London: Hutchinson & Co, 1926), 335; Michael Welch, 'The Science of War: A Discussion of J. F. C. Fuller's Shattering of British Continuity', *Journal of the Society for Army Historical Research* 79, no. 320 (Winter 2001): 320–334.

[141] The protection, mobility and firepower triad can be applied to equipment appraisals as much as to units. For example, the Rheinmetall Boxer CRV, a large, armoured reconnaissance vehicle is considered to emphasise protection and firepower at the expense of mobility. See: Edward Howson, 'Moving Forward – The Future of Cavalry Reconnaissance', *The Cove,* 12 August 2020. https://cove.army.gov.au/article/moving-forward-the-future-cavalry-reconnaissance

relates to changing position and includes velocity; large units are generally slower moving and have lower acceleration rates than small units. Firepower is related to the employment of weapons to attack the enemy. Such fire may be direct, such as firing a bullet at a target within the line-of-sight of the firer, or indirect, beyond the line-of-sight of the firer, such as long-range artillery. Importantly, depending on the way a unit's commander decides to fight, the balance between the three elements changes.

Positional warfare emphasises mobility and protection with firepower implicit. Formations are placed in a location that compels the enemy to attack but that are favourable to the defence. With the defence considered the stronger form of war, the adversary is placed at a disadvantage from the start of the battle in needing to attack a well-protected, entrenched force.[142] Positional warfare aims to impose high attrition on the attacking enemy forces, progressively destroying an adversary's equipment, personnel and resources at a pace greater than they can be replenished.[143]

In contrast, manoeuvre warfare stresses mobility and firepower, with protection reduced and achieved implicitly. Through maintaining momentum, a highly mobile attacking force can protect itself, as the enemy lacks sufficient time to respond. Manoeuvre then tries to avoid enemy strength as much as possible, thus, rendering this strength irrelevant.[144] Manoeuvre aims to create panic, or cognitive paralysis, leading to a collapse in the adversary's will to resist and, in doing so, gaining a position of advantage in relation to the adversary.[145]

Between positional and manoeuvre warfare lies a newcomer. Interchangeability warfare accentuates protection and firepower, with mobility restrained. In this form of warfare, a force positions itself at a central location and, from there, engages the enemy, whether they are advancing or not. The force does not move around the battlefield, instead letting the range and lethality of its firepower substitute for mobility.[146] Interchangeability warfare reflects a belief that there is emerging a period of firepower dominance. In considering future peer-competitor, force-on-force land battles, a former commander of the North Atlantic Treaty Organization's Central Army Group, retired General Glenn Otis, declared that:

> I believe we're at the threshold of a major change for the combined arms team – the ascendancy of fires. What that means is that we …

[142] Robert R. Leonhard, *Fighting by Minutes: Time and the Art of War*, 2nd ed. (n.p.: CreateSpace Independent Publishing Platform, 2017), 30–32.

[143] Amos C. Fox, 'A Solution Looking for a Problem: Illuminating Misconceptions in Maneuver-Warfare Doctrine‘, *Armour: Mounted Maneuver Journal* CXXIX, no. 4 (Fall 2017): 18–23.

[144] Leonhard, *Fighting by Minutes*, 32–33.

[145] Fox, 'A Solution Looking for a Problem', 18.

[146] Leonhard, *Fighting by Minutes*, 33–34.

> will fight conventional battles using firepower of all kinds from longer ranges, much of it indirect – not eyeball-to-eyeball using direct fire. We'll use long-range fires as the spearhead of the attack to the extent that the ground manoeuvre forces may only need to mop up after the fires. That's a totally different concept of operations. This concept aims at achieving decisive results while minimizing the usual high casualties of the direct fire battle.[147]

Otis argued that firepower ascendancy was because modern battlefield surveillance systems could locate forces reliability and accurately, and that artillery fire and close air support was becoming increasingly accurate, given precision munition developments. Almost 20 years later, this assessment appears vindicated.

On 11 July 2014, the Ukrainian 24th Mechanised Brigade was manoeuvring near Zelenopillya, about 10 km from the Russian border. At around 4:20 am, small Russian UAVs were noticed apparently observing the column. Shortly after, some 40 salvos of Russian surface-to-surface rockets struck the Ukrainian force.[148] Within a five minute period, the equipment of two understrength battalions was destroyed, some 30 soldiers killed and several hundred injured. Indirect fire had seemingly moved from having a supporting role to being the decisive element of land combat power.

Central to this attack was the Russian reconnaissance–fire complex model that combined good battlefield surveillance with massed fires.[149] In Ukraine, the Russian kill chain took 12–15 minutes from finding a target to its destruction.[150] With the introduction of 'first-wave' AI-equivalent expert command and control systems, cloud computing and networked sensors broadly similar, conceptually, to the IoT, the detection-to-engagement time on Russian training exercises is now reported as 3–4 minutes.[151]

The Zelenopillya attack both highlighted and raised significant concerns among many Western militaries over the emerging firepower ascendancy and the reconnaissance–fire complex model.[152] Such worries are deepening now that the PLA Ground Force appears to be embracing the Russian model.[153] Applying second-wave AI

[147] Glenn K. Otis, 'Ascendancy of Fires: The Evolution of the Combined Arms Team', 18–19 in *Field Artillery*, (June 1995): 17–18.

[148] Jack Watling, *The Future of Fires: Maximising the UK's Tactical and Operational Firepower* (London: Royal United Services Institute for Defence and Security Studies, November 2019), 1.

[149] Amos C. Fox, *Hybrid Warfare: The 21st Century Russian Way of War* (Fort Leavenworth: School of Advanced Military Studies, 2017), 34–39. http://www.dtic.mil/dtic/tr/fulltext/u2/1038987.pdf

[150] Watling, The Future of Fires, 6.

[151] Lester W. Grau and Charles K. Bartles, *The Russian Reconnaissance Fire Complex Comes of Age* (Oxford: Changing Character of War Centre, May 2018), 11. http://www.ccw.ox.ac.uk/blog/2018/5/30/the-russian-reconnaissance-fire-complex-comes-of-age

[152] Watling, The Future of Fires, 1.

[153] Singh, *Learning from Russia*, 10.

to the complex's indirect fire kill chains is likely to further strengthen the emerging firepower ascendancy.

The United States Marine Corps (USMC) considers Otis's observation that such an ascendancy relies on good surveillance an important judgement. In the USMC's Operating Concept, countering the firepower ascendancy requires a 'battle of signatures':

> Tomorrow's fights will involve conditions in which 'to be detected is to be targeted is to be killed.' Adversaries will routinely net together sensors, spies, UA[Vs], and space imagery to form sophisticated 'ISR-strike systems' that are able to locate, track, target, and attack an opposing force … No matter the means of detection, unmanaged signatures will increasingly become a critical vulnerability … our units will need to adapt how they fight, emphasizing emissions control and other means of signature management to increase their survivability.[154]

AI's warfighting usefulness was earlier summarised as 'find and fool'. In war-on-land, 'find' is fundamental to the emerging firepower ascendancy, while 'fool' is captured within the 'battle of signatures'. This chapter discusses waging war-on-land in an AI-enabled battlespace, principally through the 'find and fool' AI employment construct. The first section develops a war-on-land defence concept, and the second section extends this into a war-on-land offence concept. The final section briefly notes some germane force-structure issues, including force AI 'system of systems' integration, cyber and force transformation.

A war-on-land defence concept

Sensor field deployment

The generic defence concept discussed in Chapter 2 envisaged distributing IoT sensors throughout areas through which hostile forces might traverse. These areas are usually determined by the terrain; there are some areas that allow easy land force mobility and others where movement is difficult and slow. Terrain constraints are most evident when a land force is undertaking an offensive during a large-scale conflict. In such conflicts, land forces require considerable logistic support in terms of supplies and maintenance, and receiving this support requires ready access and connectivity.

[154] Department of the Navy, *The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century* (Washington: Headquarters United States Marine Corps, September 2016), 6. https://www.mcwl.marines.mil/Portals/34/Images/MarineCorpsOperatingConceptSept2016.pdf

The creation of large depots in the rear areas of a mobile land force is inevitable, particularly in this time of firepower ascendancy. A very noticeable feature of the Russian reconnaissance–fire model is the presence of very considerable quantities of ammunition in rear areas, together with the critical, connecting, logistic supply links necessary to bring the ammunition forward to the guns and rocket launchers in a timely manner.[155] This may also be a feature of PLA Ground Force operations, given that they have embraced Russian thinking concerning artillery being the 'finishing arm' and dramatically increased their firepower capabilities and capacities.[156]

The large logistic tail is an obvious indicator of where adversary land forces intend to conduct an offensive and, thus, where the defenders should seed their IoT sensor field. Given this information, the defenders can use interchangeability warfare to impose high attrition on adversary forces whether they are advancing, preparing to move or static.

The deployed IoT sensor field can use a diverse array of fixed and mobile cross-domain sensors. The fixed sensors can be deployed in advance and might include seismic, acoustic, imaging, active and passive electronic systems. The deployment design might be layered, with the granularity of sensor data increasing in terms of identity, accuracy and timeliness as the hostile force moves further into the engagement zone. The mobile sensors to be deployed when appropriate could include space-based active and passive systems, UAVs and UGVs, all employing AI edge computing processing. The US Army Research Laboratory is presently studying IoT technology possibilities under the rubric of the Internet of Battlefield Things.[157]

Early deployment of the IoT sensor field will greatly increase the amount of environmental and contextual data to be collected. This will allow the AI 'find' systems to be better trained using machine learning. The IoT sensor field elements, however, will each have operating power limitations that will shape when and where they can be deployed.

The mobility of AI-enabled UV does offer some new surveillance options. UAVs and UGVs can be aggressively employed in a less covert manner to gain information, as their loss or damage to hostile action may be acceptable.[158] Small UAVs and UGVs can be used to saturate an area of interest, forcing any adversary to reveal themselves to friendly forces.

[155] Watling, The Future of Fires, 7.

[156] Singh, Learning from Russia, 10.

[157] U.S. Army Research Laboratory, *Internet of Battlefield Things* (Durham: U.S. Army Research Laboratory, 2020). https://www.arl.army.mil/business/collaborative-alliances/current-cras/iobt-cra/

[158] J. Frederick Dente and Timothy Lee, 'Robots and Reconnaissance: We May Never Be Stealthy and Deliberate Again', *Armour: Mounted Maneuver Journal* CXXXIII, no. 2 (Spring 2020): 15–16.

Command and control

The IoT sensor field would feed data through the cloud into a fusion facility where AI would process this into tactically useful information, including predictions of the adversary's likely courses of action and movements. The next AI layer, aware of the friendly firepower units available, would pass to the commander for approval a prioritised list of targets, the optimum types of cross-domain attack to employ and the timings involved. In the human–machine team, the human would retain in-the-loop or on-the-loop control, as desired. After human approval, the next AI layer would assign the preferred weapons to each target, passing the requisite targeting data automatically, ensuring deconfliction with friendly forces, confirming when the target was engaged and potentially ordering munition resupply. The cycle would complete as the IoT sensor field detected and passed data back through the command and control system concerning the attack's effectiveness.

In this way, the AI-enabled command and control system would progressively build a near real-time digital model of the battlefield while providing the defenders with a digital backbone that feeds relevant information and orders to all land force participants. Two aspects should not be overlooked: the cloud has a central role in connecting all involved, and all must use common data standards and architectures.[159]

An example of some aspects of this system of systems is a recent US Army live-fire demonstration in Germany. Satellite data flowed into the Tactical Intelligence Targeting Access Node ground station. There, the Prometheus data fusion AI machine learning sifted through the data to locate and identify targets. Another algorithm called SHOT matched the targets to appropriate weapons given information on their availability provided by the Advanced Field Artillery Tactical Data System.[160] The use of AI dramatically shortened the time required to engage the target, 'a process that would otherwise take minutes or even hours dwindled—in an experimental setting—to a few seconds'.[161] Some similar functionality to that tested in the US Army trial is already in Russian Army service, in the steadily evolving Strelets reconnaissance, command and control and communications system.[162]

[159] Sydney J. Freedberg Jr, 'Army Future Ops Depend on Cloud – But Not on JEDI', *Breaking Defense*, 29 July 2020. https://breakingdefense.com/2020/07/army-future-ops-depend-on-cloud-but-not-on-jedi/

[160] Nathan Strout, 'How the Army Plans to Use Space and Artificial Intelligence to Hit Deep Targets Quickly', *Defense News*, 5 August 2020. https://www.defensenews.com/digital-show-dailies/smd/2020/08/05/how-the-army-plans-to-use-space-and-artificial-intelligence-to-hit-deep-targets-quickly/

[161] Steve Trimble and Lee Hudson, 'U.S. Army Flexes New Land-Based, Anti-Ship Capabilities', *Aviation Week,* 20 October 2020, Paragraph 14. https://aviationweek.com/defense-space/missile-defense-weapons/us-army-flexes-new-land-based-anti-ship-capabilities

[162] Grau and Bartles, *The Russian Reconnaissance,* 12–13.

The depth of the extended land battlefield is related to the range of the firepower being employed. Artillery systems now fire out to some 70 km, with rockets engaging targets out to 300 km and in the foreseeable future out to 500 km. Beyond this, air power is available, although there is interest in very long-range cannons that may engage targets at some 3,000 km.[163]

The combination of the AI-enabled IoT sensor field, cloud computing and the command and control system allows centralised coordination of the multiple, dispersed, cross-domain weapon systems, removing the need for an intermediate level of firepower management. With this expedited, digital kill chain in place, cross-battlefield, small-scale weapon packets could now be more rapidly concentrated, increasing the tempo of engagements. In this, the side that prevails might be that which can most swiftly bring fires to bear.[164]

AI-enabled manoeuvre forces

Firepower may not be enough in itself to completely and successfully defend areas; manoeuvre forces are likely to remain necessary. Glenn Otis asserts that with firepower ascendancy:

> The fundamental tenet … is that we not expose our forces to enemy fires any more than we have to. The construct says, ‘I’m going to fight the enemy by fire first and then by movement and fire’ … If you put superior firepower on the enemy and maintain freedom of movement to position your troops advantageously, you win. Your fire prevents the enemy from moving freely while you fire and move on the enemy freely.[165]

Accordingly, the battlefield may be conceived as three distinct zones:

1. **The zone of advantage:** the near region in which friendly fires outweigh those from adversary forces; friendly forces can concentrate more than the enemy.
2. **The contested zone:** the middle region in which both sides are able to deliver effective fires and, hence, all must fight dispersed to survive.
3. **The zone of vulnerability:** the far region in which the adversary can bring down greater and more responsive volumes of firepower and, accordingly, when within can more readily concentrate forces.

[163] Steven A. Yeadon, ‘A New Combined-Arms Approach for the Armored Brigade Combat Team‘, *Armour: Mounted Maneuver Journal* CXXXIII, no. 3 (Summer 2020): 16–17; David Axe, ‘In a War with China, Where Should the U.S. Army Put Its Thousand-Mile Cannons?’, *Forbes*, 11 August 2020. https://www.forbes.com/sites/davidaxe/2020/08/11/in-a-war-with-china-where-should-the-us-army-put-its-thousand-mile-cannons/?sh=25387e1c49c8

[164] Watling, *The Future of Fires*, 28–29.

[165] Otis, ‘Ascendancy of Fires’, 19.

Expressed as units, battlegroups may be used in the nearer zone of advantage with reinforced company and smaller groups in the two more distant others.[166]

Mechanised battlegroups are likely to be used against the smaller adversary units operating within the friendly zone of advantage. Friendly armoured vehicles may act as ‘motherships’, deploying and controlling smaller AI-enabled robots. The US Army envisages three future UGV types. The light Robotic Combat Vehicle (RCV), with a sensor array to provide close-in reconnaissance; the medium RCV, carrying a medium-calibre gun and anti-tank guided missiles to augment the unit’s direct firepower capability; and the large RCV, fighting with its own weapon systems as a ‘wingman’ that manoeuvres in tandem with M-1 Abrams main battle tanks or within an all-robotic platoon.[167]

Such RCVs are expected to use AI for autonomous driving and automated threat recognition; both are crucial to reducing the workload for humans in the battle-groups’ numerous human–machine teams. Current autonomous driving systems avoid solid obstacles like trees and rocks but are troubled by voids such as ditches or potholes. Similarly, imagery threat recognition works well when the RCVs are stationary, but poorly when moving and when the imagery is jittery. Today, operating an RCV takes two people controlling it remotely: a driver and a gunner/sensor operator. By 2035, with AI enhancements, one person should be able to control 12 RCVs.[168]

In the contested zone and the zone of vulnerability, smaller-sized units will need to be used to achieve adequate survivability levels. However, AI can make these units much more capable than they have traditionally been. A platoon-sized unit using UAVs and UGVs can control much larger areas, with initial assessments indicating an increase from 1 km^2 to some 75 km^2. The individual UAVs and UGVs would use AI for mobility, understanding sensor data and communications.

In this, the central element may be the overarching AI system that both informs and coordinates the whole unit. Having good situational awareness is the key driver to modern, small-unit combat success and AI can help ensure it.[169] The overarching AI layer could give a detailed tactical picture across the 75 km^2 area, highlight nearby friendly and adversary forces to each solider, suggest courses of action and control the UAVs and UGVs as directed. This overarching AI layer may reside in the cloud,

[166] Watling, *The Future of Fires*, 38–39.

[167] Cory W. Wallace et al., ‘Army Modernization in Next-Generation Vehicles Will Change the Battlefield’, *Armour: Mounted Maneuver Journal* CXXXIII, no. 2 (Spring 2020): 9–11.

[168] Sydney J. Freedberg Jr, ‘Robots & Puddles: Surprises from Army RCV Test’, *Breaking Defense*, 7 August 2020. https://breakingdefense.com/2020/08/robots-vs-puddles-surprises-from-army-rcv-test/

[169] Dan Skinner, ‘The Integrated Digital Soldier System: Close Combat in the 21st Century’, *The Cove*, 6 August 2019. https://cove.army.gov.au/sites/default/files/the_integrated_digital_soldier_concept_v1.pdf

distributed across multiple mini-servers carried by the UGVs and, possibly, individual soldiers. With this approach, there is no single point of failure and communications can be made more robust.[170]

The smaller human–machine teams operating in the contested zone and the zone of vulnerability will face resupply problems from hostile firepower interdiction. These may be lessened by use of small UGVs optimised for logistics functions and, possibly, medevac. So-called LOGBOTs could make logistic support 'hard to find, hard to hit and hard to kill'.[171]

UK forces are trialling Titan, a modified Estonian UGV, that can be controlled by a human or dispatched on tasks autonomously. Titan's AI machine-learning software allows it to recognise patterns in the images created by its onboard sensors and then use these patterns to assist travel to the chosen destination.[172] In a similar manner, the USMC have experimented with robotic resupply vehicles, ranging from the K-MAX uncrewed helicopter in Afghanistan to mini-drones carrying individual clips of ammunition, canteens and packs of batteries. A recent US experiment involved a small logistic resupply Multi-Utility Tactical Transport (MUTT) UGV:

> [W]ith a pair of Pegasus mini-drones on its back. One Pegasus carried a sensor package: When needed, it took off from the MUTT and scouted ahead, reporting on part of the route that was out of sight around a corner. The second Pegasus carried a small but crucial resupply item, a battery, that it delivered to a different location than the MUTT's main load, saving the ground vehicle a side trip and cutting delivery time. Another portion of the route was monitored by a prepositioned radar sensor called a SUAVI – a $400 version fits in your hand and runs off battery power for 24 hours – which fed real-time updates to the MUTT.[173]

Implications of AI-enabled interchangeability warfare

The AI-enabled interchangeability warfare construct hides some issues. If Russian forces need large munition-storage areas in the rear, so would friendly forces. The three zone construct, in reality, would be effectively three concentric circles around a central combat service support core. This core is needed not just for the munition

[170] Freedberg, 'AI & Robots'.

[171] Jacob Choi, '#LOGBOTs – Making Army Logistics "Hard to Find, Hard to Hit and Hard to Kill" ', *Grounded Curiosity*, 18 November 2018. https://groundedcuriosity.com/logbots-making-army-logistics-hard-to-find-hard-to-hit-and-hard-to-kill/#.X5JHUlMzZwe

[172] Michael Dempsey, 'Robot Tanks: On Patrol but Not Allowed to Shoot', *BBC News*, 21 January 2020. https://www.bbc.com/news/business-50387954

[173] Sydney J. Freedberg Jr, 'Marines Explore Robots & 5G Networks for Future Wars', *Breaking Defense*, 31 August 2020. https://breakingdefense.com/2020/08/marines-explore-robots-5g-networks-for-future-wars/

stocks and the normal support of the crewed land force units but also for the maintenance of the robotic forces and, possibly, a logistic support airfield. The numbers of soldiers in combat in the field may be reduced by increasing the numbers and use of robots, but the penalty is having a sizeable robot support tail.[174]

This central combat service support core then becomes a critical target as destroying this node could incapacitate many AI-enabled robot systems, given that they cannot maintain and repair themselves. The node is protected by the friendly ground forces in the three zones but will inevitably become the target for many adversary indirect-fire weapons, some of which might have long ranges. Accordingly, such nodes may need comprehensive defence packages to protect them, including layered counter-rocket artillery and mortar systems, high energy lasers, high-powered microwaves, jamming, ground-based air defences, electronic deception and perhaps even limited ballistic missile defence.[175]

AI-enabled interchangeability warfare may lead to tactical-level fighting becoming increasingly fluid, with small, dispersed units from the opposing sides entangled across the three zones. In contrast, with combat service support nodes critical to sustaining operations, the battlefield at the operational level may become static and location-dependent.[176]

Much of the AI-enabled interchangeability warfare construct hinges on the ‘find’ capabilities of AI. To avoid being engaged by high-precision firepower, friendly force units will need to avoid detection, disperse and use effective and layered countermeasures. This makes the AI’s ‘fool’ capabilities critical.

To survive adversary fire, friendly force signatures will need to be well concealed through comprehensive passive and active masking efforts. These could include visual and electronic camouflage, decoys, deception and electronic jamming.[177] Moreover, given the adversary IoT sensor field will be cross domain, the friendly force ‘fool’ activities will need to be both sophisticated and innovative: sophisticated in convincingly fooling across different sensor types, and innovative in needing to deceive AI machine-learning data fusion and command and control systems for an extended period, possibly until conflict termination. AI-enabled mobile systems may be crucial to allow such protracted deception.

Perhaps less obvious, the ‘fool’ function could be usefully coordinated with kill measures. The near real-time digital model of the battlefield created by AI’s ‘find’

[174] Peter Layton, ‘Our New Model Robot Armies’, *Small Wars Journal*, 7 August 2018. https://smallwarsjournal.com/index.php/jrnl/art/our-new-model-robot-armies

[175] Watling, The Future of Fires, 38.

[176] Watling, The Future of Fires, 52.

[177] Yeadon, ‘Combined-Arms Approach’, 18–19.

capabilities may reveal where the adversary's 'find' systems are located. Attacking the adversary's IoT sensor field or data fusion facility through kinetic and non-kinetic means will slow the opponent's 'find' capabilities and reduce their effectiveness. Such attacks would create new avenues for 'fool' assaults, in particular in deception and confusion.

A war-on-land offence concept

The defence concept may avoid defeat but still not end the war. An adversary may simply accept the firepower imposed attrition and remain aggressive. Offensive manoeuvre by friendly forces deep into the zone of vulnerability could be necessary to achieve decisive results. The aim of such a manoeuvre may be to bypass the adversary's central combat service support nodes, cutting them off from their essential logistics train, including fuel resupply and energy sources.

If this can be achieved, the forward, in-contact combat forces will collapse and the adversary's military activities will become dislocated. The adversary battle network may then be paralysed in a manner that means it cannot attain its strategic objectives.[178] Of course, the adversary may also be endeavouring to achieve this same objective; in the Ukraine, mutual operational penetration of up to 200 km was achieved by small units.[179]

Tactical success by the dispersed small units will depend on their agility and flexibility in manoeuvring for advantage across a dangerous, fire-dominated battlespace. The constant threat from artillery means that protected mobility is essential, with firepower traded off as necessary. Overall, the manoeuvre tempo can be expected to increase as units try to quickly move beyond the contested zones and vulnerable areas.[180]

Importantly, the small units penetrating the adversary defences are not fighting as individual entities but rather in a distributed manner where each supports the others to advance. These small units working together need to maintain momentum, combining the effect of their dispersed mass with the higher speeds possible due to their size. To achieve such synergies, connectivity to the overarching AI-enabled command and control system is required. This will allow the dispersed units to maintain good situational awareness, be supported by friendly, long-range fires and be integrated into a coherent battle plan.

The small units involved may use robotics and AI in ways similar to those described in the defence concept. The units could use infiltration techniques to slip past the

[178] Naveh, Pursuit of Military Excellence, 211.
[179] Watling, The Future of Fires, 39
[180] Watling, 41–42.

close-contact battle lines into the rear areas. Traditionally, such tactics have not been favoured because they are too dangerous, with real risks to the small units' survival. However, through providing additional firepower and mobility, the use of AI-enabled UAVs and UGVs creates new opportunities. The UAVs and UGVs can be readily hazarded and, if necessary, lost to ensure a safe, small-unit manoeuvre. For example, UGVs could undertake risky diversionary operations to hold adversary forces in place while small units infiltrated. Conversely, the small units could employ their UAVs and UGVs in massed swarm attacks to gain a tactical advantage.[181] Some envisage UGVs being airdropped into hostile territory to manoeuvre and fight until their fuel and munitions are expended, aiming to create confusion and a distraction.[182]

Even so, the survival and utility of these small, dispersed units will greatly hinge on the success of the C-IRST efforts. The small units will need to win the 'battle of the signatures' and stay hidden as much as possible from the adversary's AI 'find' system. This success will require support from multiple 'fool' capabilities distributed across the close and deep battlefield. Again, the use of AI-enabled airborne and ground-borne mobile 'fool' systems would be important to creating false targets and incorrect perceptions as part of actively deceiving the adversary command and control system.

Force structure issues

The war-on-land concepts envisage a wide diffusion of AI across the force structure, both horizontally and vertically. The various layers of AI systems will need to work with each other and their human team members. Currently, most AI systems each use a unique customised software–hardware core that is specifically designed for their intended purpose. There is no controlling means to integrate the multiple AI systems working independently and on multiple levels. Additional disorder might be created as some AI systems use machine learning and self-evolve their programming, and as allied nations add their own AI systems to the operational mix. However, without seamless integration, the desired benefits from the overall system

[181] Jules Hurst, 'Robotic Swarms in Offensive Maneuver', *Joint Force Quarterly* no. 87 (4th Quarter, October 2017): 108–110.

[182] Kyle Mizokami, 'This Robot Tank Is the Future of Armored Warfare', *Popular Mechanics*, 23 June 2020. https://www.popularmechanics.com/military/weapons/a32947926/type-x-robot-combat-vehicle/

of systems may not be realised.[183] Certainly, the overall reliability in combat might be questioned. The 'fog of war' might be replaced by a 'fog of systems'.[184]

In a similar vein, relying on AI-enabled capabilities opens up the cyberspace attack vector. Present trends suggest combat and weapons systems will remain vulnerable to cyber attacks.[185] This susceptibility may be exploited to aid AI's 'fool' capabilities, but it does make AI's 'find' capabilities much less operationally robust.

More broadly, this war-on-land concept has, in the main, simply added AI across and to more traditional combat systems. AI then becomes an effectiveness and efficiency multiplier. However, the result of discarding the current force structures and considering whole new approaches has been left unexamined. The technological core of the AI-enabled battlefield is comprised of IoT fields, the cloud, AI machine learning and edge computing. If these were used as the basis of a future land force structure rather than the traditional triad of protection, mobility and firepower, a very different force structure might emerge with unique and unexpected capabilities.[186]

[183] Zachary S. Davis, *Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise* (Lawrence Livermore National Laboratory: Center for Global Security Research, March 2019), 10–11. https://cgsr.llnl.gov/content/assets/docs/CGSR-AI_BattlefieldWEB.pdf

[184] Franz-Stefan Gady, 'What Does AI Mean for the Future of Manoeuvre Warfare?', *International Institute for Strategic Studies*, 5 May 2020.https://www.iiss.org/blogs/analysis/2020/05/csfc-ai-manoeuvre-warfare

[185] Gady, 'Future of Manoeuvre Warfare'

[186] Zachery Tyson, National Security Fellow, Truman National Security Project, correspondence with author, 4 August 2020.

CHAPTER 5
The AI-enabled war-in-the-air

War-in-the-air combines generic warfare concepts and context-specific aspects. The air battlefield is deep in covering vast areas; the sky is generally uncluttered and opposing air forces clash apparently unimpeded. In this, the two enduring constants of war-in-the-air are being both multidomain and involving opposing battle networks. The nature of the air environment means that war-in-the-air is significantly influenced by technology, its possibilities and its deficiencies. In terms of the Russian, Chinese and US operational concepts, two particular areas have been embraced by modern airpower thinkers.

First, the concepts stress trying to paralyse the opposing command and control system, thereby dislocating and disrupting the opposing battle networks. Influential airpower thinkers, John Boyd and John Warden, share this vision. Boyd advocated manoeuvring inside the adversary's OODA decision-making loop. [187] This would disrupt the enemy commander's cognition, creating for them a seemingly menacing situation, and incapacitate the adversary force's ability to adapt to a now too-rapidly changing environment. In a similar vein, John Warden stressed directly or indirectly targeting adversary leadership to cause system paralysis and psychological pressure.[188]

Second, the Russian, Chinese and US operational concepts all argue that simultaneous attacks across the entire depth of the defender's layout may bring significant gains. In 1921, Giulio Douhet first suggested offensive air operations against several different target sets at both the strategic and tactical levels.[189] However, the con-

[187] David S. Fadok, 'John Boyd and John Warden: Airpower's Quest for Strategic Paralysis', in *The Paths of Heaven: The Evolution of Airpower Theory*, ed. Phillip S. Meilinger (USAF Maxwell Air Force Base: Air University Press, 1997), 364–368.

[188] Fadok, 373–376.

[189] Phillip S. Meilinger, 'Giulio Douhet and the Origins of Airpower Theory', in *The Paths of Heaven The Evolution of Airpower Theory*, ed. Phillip S. Meilinger (USAF Maxwell Air Force Base: Air University Press, 1997), 15–16.

cept only became feasible in the 1990s with the introduction of precision-guided munitions. This was quickly grasped by Warden, who was influential in advocating its acceptance by the USAF – and consequently other air forces – under the term of parallel warfare.[190]

Outside such operational level considerations, war-in-the-air at the tactical level directly involves aircraft. Compared to other weapon systems, modern aircraft are highly mobile at both the tactical and operational levels of war and can readily employ precisely targeted firepower in all weathers, day and night. However, aircraft are inherently easy for modern sensors to detect against the uncluttered sky background and, given this, are relatively straightforward for contemporary weapon systems to engage. In response, there is a range of specialised aircraft and tactics that strive to prevent detection through active, passive, technical and tactical means. All aircraft, however, are relatively fragile and can be disabled by even small missiles or projectiles. Compounding this sensitivity to injury, returning a damaged aircraft to combat-ready status can be problematic, depending greatly on logistic support availability.

Like war-at-sea, air combat is governed by Lanchester's square law of effectiveness: given evenly matched forces, a small advantage in net combat power at the start will be decisive and the effect cumulative.[191] This makes mass, in terms of numbers of aircraft, important in both the defence and the offence. All else being equal, a larger force imposes a much higher rate of attrition on a smaller force than the smaller force can in response: 20 aircraft engaging 10 aircraft can destroy all 10 for the loss of only 3 aircraft.[192]

Mass is problematic for contemporary air forces given the cost of modern aircraft and of training high-competency aircrews. AI-enabled UAVs offer a possible solution to this problem in replacing hard-to-acquire individual human skills with readily replicable software. The 4IR and its prototype warfare possibilities offer tantalising visions of using advanced manufacturing techniques to produce large robot air forces on demand, including having AI-enabled UAVs quickly tailored for specific operations or conflict.[193]

[190] John R. Pardo, 'Parallel Warfare: Its Nature and Application', in *Challenge and Response: Anticipating US Military Security Concerns*, ed. Karl P. Magyar (USAF Maxwell Air Force Base: Air University Press, August 1994), 322–323.

[191] MacKay, 'Lanchester Combat Models'.

[192] Andrew Davies, 'Geek of the Week: Frederick Lanchester and Why Quantity Has a Quality All of its Own', *The Strategist*, Australian Strategic Policy Institute, 20 September 2013. https://www.aspistrategist.org.au/geek-of-the-week-frederick-lanchester-and-why-quantity-is-a-quality/

[193] Layton, *Prototype Warfare and the Fourth Industrial Age,* 11-17.

This chapter discusses waging war-in-the-air in an AI-enabled battlespace through the 'find' and 'fool' AI employment construct. Conceptually, counter-air operations involving two sides trying to defeat each other are divided into defensive counter-air and offensive counter-air operations. The first section, accordingly, develops a war-in-the-air defence concept with the second building from this into a war-in-the-air offence concept.

Airpower can also be used for strategic strike and to support land and maritime operations. Importantly, this chapter focuses solely on counter-air operations; considerations arising from air attacks on surface targets are not discussed. Moreover, the chapter does not include ballistic missile defence in the defensive air concept, instead concentrating on aircraft-related matters; it is solely about war-in-the-air.

A war-in-the-air defence concept

Air defence aims to reduce the effectiveness of adversary air attacks and impose an unacceptable attrition rate on the attacking aircraft. The two aims are compatible but, generally, either one or the other is prioritised as friendly force disposition and employment varies depending on the primary intent. In this regard, a defensive posture cedes the initiative to the adversary who can then choose when and where to mass forces for attack. In a major conflict between powers, an air defence system is unlikely to be wholly effective in preventing air attacks; some aircraft will penetrate the system and deliver weapons on their chosen target.

Air defence involves active and passive measures to protect friendly forces from air attack. The active measures are usually combined into an integrated air defence system (IADS) comprised of fighter aircraft, surface-to-air missiles (SAM), anti-aircraft artillery (AAA), air and ground-based radar systems, and a command and control system. The defending fighter aircraft are generally employed as either combat air patrol (CAP) or ground-alert interceptors (GAI). The CAP involves an airborne standing patrol positioned to intercept hostile aircraft either before they attack or when they are outbound after an attack. In contrast, the GAI waits on the ground until an approaching air attack is detected and is ordered to scramble by the command and control system.[194]

Passive air defence measures include camouflage, concealment, decoys, electronic deception or interference, hardening, dispersion and reconstitution. In the late–Cold War period, hardened aircraft shelters were built on many air bases to make destroying aircraft on the ground much more difficult. The underlying premise was that air attacks would use only free-fall, unguided weapons. Now, with widespread

[194] Robert L. Shaw, *Fighter Combat: Tactics and Maneuvering* (Annapolis: Naval Institute Press, 1985), 325.

precision-guided weapons proliferation, hardened aircraft shelters may be much less efficacious. Conversely, decoys appeared successful in the Kosovo war in countering guided weapons, suggesting their utility continues.[195]

Sensor field deployment

The generic defence concept described in Chapter 2 envisages a large IoT sensor field distributed across areas that hostile forces might move into or through. In some respects, this idea is already in place in air defence concepts that include chains of surface-based radar stations complemented by airborne early warning and control aircraft to detect high-flying and low-flying aircraft. The war-in-the-air, AI-enabled defence concept suggests a massive supplementation of this existing high-cost, limited-number sensor deployment through using large numbers of AI-enabled, small, low-cost surface and airborne sensors.

The smaller elements of the expanded IoT sensor field can use AI edge computing, with partly processed data sent through the cloud to a fusion centre and then into the command and control system. These smaller IoT sensors could be active, short-range radar emitters, but power constraints may limit the use of this technology. More likely to be used are passive IoT sensors that detect emissions across the electromagnetic spectrum, including the acoustic, ultraviolet, infrared, radio and radar bands. Each sensor individually may have relatively low performance but, when its outputs are combined with potentially several hundred others, it may be possible to track and identify air traffic, perhaps in three dimensions.

The surface air defence IoT sensors might be fixed and persistent, whereas sensor-equipped UAVs could have endurance varying from hours up to a day. There are emerging IoT applications that might considerably increase this endurance, including high altitude balloons, smallsats and pseudosatellites, all potentially incorporating AI.[196]

Having a large IoT sensor field that uses passive detection means that penetrating aircraft must avoid using transmitting systems, such as radars, data links and communications, to avoid detection. Even so, normal aircraft emissions, such as noise, temperature and its visual signature, may still reveal the aircrafts' presence. In this, having a deep IoT sensor field is important. As they approach known sensors, aircraft may manoeuvre to limit their emissions, particularly those emanating from the aircraft's forward sector. A deep field means that a penetrating aircraft may be detected on its flanks and in its rear sector even if it is not detected when approaching directly.

[195] Dag Henriksen, 'Control of the Air', in *Routledge Handbook of Air Power*, 1st edition, ed. John Andreas Olsen (London: Routledge Taylor & Francis Group, 2018), 87.

[196] For pseudosatellites see: Michael Spencer, *Pseudosatellites Disrupting Air Power Impermanence* (Canberra: Air Power Development Centre, 2019).

Command and control

The very large IoT sensor field made possible by AI would feed partly processed data through the cloud into a fusion facility where AI would undertake further processing. In considering these steps, the OODA model is useful. In terms of 'Observe', as already noted, AI would be involved in each IoT's edge computing and then again in the fusion centre. In terms of 'Orient', AI would play an important part in the battle management system.[197] AI would not only produce a comprehensive, near real-time air picture but would also predict the enemy's courses of action and movements in the air.

The next AI layer, 'Decide', which manages and is aware of friendly air defence units availability, would pass to the human commander for approval a prioritised list of approaching air targets to engage, the optimum types of cross-domain attack to employ, the timings involved and any deconfliction considerations. In the human–machine team, the human would retain in-the-loop or on-the-loop control, as desired. For 'Decide', humans would remain deeply engaged.

After obtaining human approval, the final 'Action' AI layer would assign specific friendly weapons to engage each adversary aircraft target, pass targeting data automatically, deconflict with friendly forces, confirm when the target is engaged, undertake engagement assessment and if necessary request friendly weapon resupply. The 'Action' step leads to the engagement of the target by AAA, SAM systems or fighters. Over time, AI will probably become widely used in all three weapon system types.

Considering AAA, the Phalanx close-in gun has a rules-based expert system and has been employed by navies for many years for last-ditch, anti-ship missile defence. Used only once in combat in the human on-the-loop control mode, the gun, at that time engaged a chaff decoy cloud rather than the attacking missile.[198] Considering SAMs, the Patriot SAM system also employs an expert system akin to simplified first-wave AI in its human-on-the-loop control mode. Patriot has proven effective in shooting down attacking very high-speed ballistic missiles but has also failed twice and shot down two friendly aircraft.

The combat performance of both systems suggests that future AI-enabled AAA and SAM systems could also fail, making human involvement vital. Accordingly, humans in these human–machine teams need to be wary of developing a false sense of security in their AI systems. Given that failures may be rare and unpredictable, and

[197] Chris Westwood, *5th Generation Air Battle Management* (Canberra: Air Power Development Centre, 2020), 22.

[198] Robert H. Stoner, 'R2D2 with Attitude: The Story of the Phalanx Close-In Weapons', NavWeaps, October 2009, http://www.navweaps.com/index_tech/tech-103.php

that the system-monitoring load may be high, the people involved may inadvertently slip into being system monitors rather than fully engaged active controllers.[199]

AI-enabled fighter aircraft

AI is now being considered for future uncrewed fighter aircraft applications. A recent DARPA air combat experiment saw an AI-piloted F-16 simulation consistently defeat an experienced human–piloted F-16 simulation. The successful AI used reinforcement learning, the machine-learning technique discussed in Chapter 1 that proved very effective in learning how to play Go.[200] In the DARPA F-16 case, the AI agent controlled both flying the aircraft and the making of tactical decisions.

There are other AI possibilities that an AI-enabled, uncrewed aircraft could use, including having a second-wave AI learning algorithm making tactical decisions while a first-wave AI expert system flew the aircraft. Alternatively, first-wave AI could do both tasks. In the DARPA simulation trials, it appears that all three approaches produced reasonable results, but the reinforcement learning method proved superior. In the physical world, the outcome may be different.

With several high-performance UAVs already flying,[201] developing a within-visual-range, air-to-air combat UAV that used AI for tactical decision-making during dogfights appears a straightforward engineering task. Indeed, the US plans to repeat the 2020 AI-piloted aircraft versus a human piloted–aircraft experiment in 2024, but this time not with simulations but with full-scale tactical aircraft. [202] An operational, optimised, AI-enabled, short-range, dogfighting UAV could be smaller, lighter and lower cost than a crewed aircraft and, in a defensive role, may not need to be armed to disrupt an incoming adversary air attack.

[199] John K. Hawley, *Patriot Wars: Automation and the Patriot Air and Missile Defense System* (Washington: Center for a New American Security, 2017), 9–10. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/CNAS-Patriot%20Wars.pdf

[200] Patrick Tucker, 'An AI Just Beat a Human F-16 Pilot In a Dogfight – Again', *Defense One*, 20 August 2020. https://www.defenseone.com/technology/2020/08/ai-just-beat-human-f-16-pilot-dogfight-again/167872/

[201] For examples see: Joseph Trevithick, 'Navy Establishes First Squadron to Operate Its Carrier-Based MQ-25 Stingray Tanker Drones', *The Drive*, 1 October 2020, https://www.thedrive.com/the-war-zone/36859/navy-establishes-first-squadron-to-operate-its-carrier-based-mq-25-stingray-tanker-drones; Kyle Mizokami, 'Russia's "Hunter" Is Unlike Anything in America's Arsenal', *Popular Mechanics*, 10 August 2020, https://www.popularmechanics.com/military/aviation/a33548209/russia-hunter-combat-drone/; Rick Joe, 'China's Growing High-End Military Drone Force', *The Diplomat*, 27 November 2019. https://thediplomat.com/2019/11/chinas-growing-high-end-military-drone-force/

[202] Mark T. Esper, 'Secretary of Defense Remarks for DOD Artificial Intelligence Symposium and Exposition', US Department of Defense, 9 September 2020, transcript. https://www.defense.gov/Newsroom/Speeches/Speech/Article/2341130/secretary-of-defense-remarks-for-dod-artificial-intelligence-symposium-and-expo/

The UAV might simply be allocated, by the command and control system, an adversary aircraft to engage, close in on and begin dogfighting. The crewed aircraft would be distracted and its attack approach disrupted, making it vulnerable to other crewed weapon systems. Moreover, if the adversary's crewed aircraft manoeuvres, it will have a higher rate of fuel usage and may need to quickly break off to return to its more distant home base.

Conversely, an armed, AI-enabled fighter could operate under human in-the-loop or human-on-the-loop as appropriate. The downside is that arming an aircraft creates engineering design issues and imposes tactical concerns about safe weapons carriage and employment. For several reasons, it may be easier to have, as noted for the USN's Sea Hunter uncrewed vessel, a UAV that engages and 'locks on' to an adversary aircraft and then trails it continuously, broadcasting to all the adversary's track and details.

An AI-enabled aircraft could operate in CAP or GAI roles. For CAP, the UAV would need to be physically larger than would be required for a GAI role so as to allow additional fuel to be carried and provide a usefully long endurance on station. Even so, a CAP UAV's endurance is likely to be much greater than a similar-sized crewed aircraft can achieve, as space and weight provision would not need to be made for the crew. A counter argument is that the larger the UAV, the more design and operating complications are introduced.

For GAI, the UAV could be relatively small in size and perhaps more like a missile than an aircraft, with recovery probably by parachute. For example, USAF's experimental XQ-58A Valkyrie UAV becomes airborne from a static launcher and lands using a parachute; there are proposals to base this UAV in relocatable shipping containers.[203]

If a GAI, AI-enabled, UAV fighter does not need airfields, defence in depth approaches become easier but, crucially, new concepts like distributed air defence become possible. Dispersed within the IoT sensor field may be GAI, AI-enabled, UAV fighters that can be remotely dispatched by the command and control system on short-range, quick reaction intercept missions. These point defence UAV fighters would then work in conjunction with crewed aircraft flying CAP to provide area coverage. Again, such UAVs would not necessarily need the complexity of being armed to be useful.

Importantly, in such an AI-enabled IADS, there would be a separation of tasks between humans and UAVs. The humans would be responsible and accountable

[203] Joseph Trevithick, 'This Containerized Launcher for the XQ-58A Valkyrie Combat Drone Could Be a Game Changer', The Drive, 16 October 2019. https://www.thedrive.com/the-war-zone/30474/this-containerized-launcher-for-the-xq-58a-valkyrie-combat-drone-could-be-a-game-changer

for the higher-level cognitive functions, such as developing an overall engagement strategy, selecting and prioritising targets, and approving weapons engagements. The AI would undertake lower-level cognitive functions, such as manoeuvring the aircraft and dogfight tactics.[204]

Fool function AI

The 'find' function of AI can be most advantageous when complemented by the 'fool' function. An adversary needs considerable information about the target and its defences to reliably mount successful attacks. AI-enabled 'fool' systems could be dispersed across the battlefield, both physically and in cyberspace. A long duration IoT field may be used for the C-ISRT function. The intent is to defeat the adversary's 'find' by building up a misleading, or at least confusing, picture of the battlefield. AI-enabled 'fool' systems may also be used in conjunction with a sophisticated deception campaign.

In addition, small, mobile, edge computing systems widely dispersed could create complicated electronic decoys by transmitting a range of signals of varying fidelity. These systems might be mounted on UAVs for the greatest mobility, although UGVs using the road network may also be useful for specific functions, such as pretending to be mobile SAM systems. The aim is simply to obscure the battlefield for the quite limited time that an attack is in progress.

A more costly approach might be UAVs that electronically replicate the defending fighters, creating an impression of unexpectedly large numbers of airborne fighters in various CAP stations defending the target area. This may encourage the adversary attackers to retire to avoid seemingly high attrition.

The 'fool' function can be further extended and integrated with passive defence measures and operating approaches. The principal target of adversary counter-air attacks is often the air base, an inherently large, static, easy to find target complex. This seemingly replicates the war-on-land central combat service support nodes noted in Chapter 4, and implies a similar need for comprehensive defence packages, including layered counter-rocket artillery and mortar systems, high energy lasers, high-powered microwaves, jamming, ground-based air defences, electronic deception and perhaps limited ballistic missile defences. Such a concentration of defensive systems would always be beneficial if expensive.

The air base, however, is not quite the same as the war-on-land service support node. There are some differences that AI-enabled systems might be able to leverage

[204] Daniel Javorsek, 'Air Combat Evolution (ACE)', Defense Advanced Research Projects Agency, accessed 10 January 2021. https://www.darpa.mil/program/air-combat-evolution

advantageously. An air base is often established well in advance of hostilities, and can be designed to be resilient under attack. As noted earlier, hardened aircraft shelters are now less efficacious. The alternative of dispersion may be a better contemporary option, especially given that AI could make this more practical than it has been for several decades.

A permanent air base could have several satellite airfields around it. These airfields can be designed to have a limited life of weeks or months rather than decades as with the permanent air base. In times of conflict, aircraft from the permanent air base can continually move around between it and the short-term airfields. This movement would be closely integrated with the AI-enabled 'fool' actions. The intent would be to deceive, perplex and confuse the adversary so that they do not know where to attack and then, after finally having decided, attack where there are no friendly-force aircraft. Such a tactic increases the 'fog of war', offers some possibilities for manipulating adversary perceptions and purposefully harms adversary force combat effectiveness.

An adversary has only a limited number of aircraft, stand-off weapons and ballistic missiles to employ in a counter-air campaign. Attacking airfields where there are no friendly-force aircraft located exposes the adversary's crewed aircraft to unnecessary attrition while using stand-off weapons and ballistic missiles simply wastes scarce – and, in a short conflict, irreplaceable – stockholdings. The combination of 'fool' AI and physical dispersion supports both air defence aims of reducing the effectiveness of adversary air attacks and exposing the adversary to attrition.

A previous, major problem with such aircraft dispersion notions has been that operating combat aircraft from several short-term airfields requires significant and costly duplication of logistic support and associated workforce across multiple locations. AI-enabled systems can overcome this issue.

In terms of logistic support, the permanent air base can have well-established corridors linking its large warehouses and consumable supply storage facilities to the short-term airfields. For the warehousing end of the support and supply corridors, there is considerable existing AI-enabled technology that can be employed.

State-of-the-art warehouses already feature real-time monitoring of inventory; real-time ordering using AI machine learning, the cloud, big data and IoT; order picking by advanced robotics; and stock movement by autonomous vehicles. Some warehouses are now embracing on demand 3D printing to meet one-time requests for rarely required spare parts of newer equipment and to save holding large stocks of parts for older equipment. Logistics control towers have been introduced that integrate digital information from numerous sources and use big data analytics to provide a real-time 'big picture' of the complete supply chain, including transportation activities.[205] The same technologies could be used to control and direct consumable supply storage facilities.

In terms of the corridors along which supplies and support could flow, AI-enabled logistics could use robot trucks employing follow-the-leader autonomy. This capability, also called 'platooning', has the crewed lead truck guiding several UVs following closely behind. To ensure safety, these uncrewed trucks would have emergency obstacle avoidance systems that used machine learning–developed algorithms.[206] There is already considerable work underway, with the US Army recently receiving some uncrewed trucks for training and evaluation.[207] Devising uncrewed air base logistics distribution trucks would be a much easier task technically, than for land force resupply vehicles. The former would operate principally on pre-surveyed, paved or graded roads and would probably use GPS.

At the short-term airfield end of the logistic corridors, AI-enabled systems could be omnipresent. Using AI, machine learning, big data, cloud computing, the IoT, autonomous operations and robotics such bases could generate aircraft sorties faster and with considerably fewer people than would be needed today. Robot turns of serviceable aircraft, including refuelling and weapons loading, could be possible. AI-enabled predictive maintenance would make unscheduled maintenance rare, or at least uncommon. The airfields might appear uninhabited, being managed remotely by engineering and logistics personnel at central control centres at the permanent air bases or elsewhere. Such airfields might even generate their own power using renewables and batteries to become partially self-sufficient.[208]

The equipment needed to make such a short-term airfield functional might be already installed, simply waiting for the conflict to be activated. Conversely, the airfields could have the necessary networks in place, ready to quickly incorporate 'plug

[205] Stefan Schrauf and Philipp Berttram, 'Industry 4.0: How Digitization Makes the Supply Chain More Efficient, Agile, and Customer-Focused', *Strategy&,* Munich: PwC Network, 7 September 2016. https://www.strategyand.pwc.com/gx/en/insights/digitization-more-efficient.html#Download

[206] Samuel Cox, 'An Interview with Robin Smith: Robotic and Autonomous Systems in the Australian Army', *Grounded Curiosity*, 2 March 2020, https://groundedcuriosity.com/wp-content/uploads/2020/02/LTCOL-Robin-Smith-Interview-APPROVED.pdf; Deakin University, 'Australian Army Funding Drives Deakin's Autonomous Vehicle Research', media release, 24 August 2020. https://www.deakin.edu.au/about-deakin/media-releases/articles/australian-army-funding-drives-deakins-autonomous-vehicle-research

[207] 'Oshkosh Defense Delivers Autonomous Vehicles', *Nation Shield: Military and Strategic Journal*, 2 February 2020. http://nationshield.ae/index.php/home/details/reports/oshkosh-defense-delivers-autonomous-vehicles/en#.X5JSdlMzZTZ

[208] Peter Layton, *Surfing the Digital Wave: Engineers, Logisticians and the Future Automated Airbase* (Canberra: Air Power Development Centre, 2020), 27–44.

and play' systems and vehicles into the short-term airfield's own system of systems when these were delivered, possibly in the initial follow-the-leader truck convoys.

A war-in-the-air offence concept

Offensive counter-air operations encompass four well-defined missions:

- attack operations that seek to destroy or disrupt on-ground infrastructure, such as command and control systems, airfields, runways, logistic support and air base facilities
- suppression of enemy air defence operations that deliberately attack adversary AAA and SAM systems using kinetic and non-kinetic means
- fighter sweeps into adversary air space to engage the airborne enemy aircraft encountered
- escort for fighters protecting other aircraft, such as bomber or transport aircraft, as they conduct a mission into adversary airspace.[209]

Conceptually, offensive counter-air operations have a shortcoming in that the battlefield only extends to the hostile air base; this is not deep from a system perspective. Beyond the air base, most air forces have important maintenance and support facilities that, while not directly affecting the immediate battle, have a substantial effect on longer-term force sustainability and in permitting operational level manoeuvring. Warden argues that where to attack depends on the context but, if the choice made is incorrect, there may not be a second chance. He writes that:

> The enemy's air centre of gravity may lie in equipment (numbers of places or missiles); in logistics (the quantity and resilience of supply support); geography (location and number of operational and support facilities); in personnel (numbers and quality of pilots); or in command and control (importance and vulnerability).[210]

To be able to engage the various potential targets means first gaining air superiority. The air superiority term has several graduations but, in general, it concerns gaining sufficient control of the air to allow air attacks on the enemy without suffering unacceptable attrition. Modern air defence involves a systems approach as encapsulated in the already described IADS. Gaining air superiority involves neutralising the IADS and its associated defending fighters, SAM systems and AAA through a combination of system paralysis and attrition. This neutralisation may be for a certain time or restricted to a particular geographic location.

[209] Henriksen, 'Control of the Air', 85.

[210] John A. Warden III, *The Air Campaign: Planning for Combat* (Washington: National Defense University Press, 1988), 40.

Offensive counter-air operations have several inherent advantages: the attacker has the initiative, the defender is forced to respond and the attacker can choose the location and timing of the attack. Conversely, the defender will usually have concentrated defensive systems around their air bases. With air bases well inside hostile territory, the adversary may receive considerable warning of an approaching attack, any attacking aircraft that is damaged may not be able to safely return to friendly territory and any aircrew that eject in hostile territory will no longer have a role in the war.

In offensive counter-air operations, the 'find' and 'fool' functions of AI work in conjunction.

In terms of 'find', in the initial stages of an operation the adversary IADS needs to be mapped comprehensively, particularly in terms of effectiveness, vulnerabilities, element location, communication flows and electronic signatures. AI-enabled UAVs can fly either just outside or penetrate inside the hostile airspace to stimulate the adversary IADS and generate a reaction, including the activation of SAM systems and launch of defending fighters. AI edge computing embedded within the UAVs' sensor systems could then both collect and partly process data onboard before forwarding it to the cloud. In being so risked, the UAVs may be engaged by the adversary air defence system and destroyed, making returning information in real-time via the cloud essential.

The electronic information collected will be especially useful in updating the crewed aircraft's mission data files.[211] This collection activity may be protracted and become increasingly aggressive with deeper and deeper incursions. AI allows UAVs to undertake this mission successfully at no risk to humans and crewed assets.

These initial AI-enabled reconnaissance UAVs may be autonomous for much of their flight. Without weapons, human involvement may not be necessary unless to alter planned routing or collection profiles as tactical circumstances mandate. These UAVs may be sent as single air vehicles or in interacting collection formation teams, at high or low altitude, as required to stimulate the adversary IADS.

After developing a high-quality map of the opposing IADS, there is an argument for then moving to attacking the IADS simply through using similar AI-enabled UAVs. While conceivable in some circumstances, there are some issues to note. The IADS map is unlikely to be completely correct, as adversaries will be constantly moving their mobile defensive systems and continually changing the IADS's electronic signature. Moreover, second-wave AI has difficulty handling context changes and in

[211] Peter Layton, *Fifth Generation Air Warfare*, Working paper 43 (Canberra: Air Power Development Centre, 2017), 8–9. https://airpower.airforce.gov.au/APDC/media/PDF-Files/Working%20Papers/WP43-Fifth-Generation-Air-Warfare.pdf

war-in-the-air, constant changes can be anticipated. Some of these changes may perplex the AI, necessitating a human to solve the problem.

This issue would be of greatest concern if the friendly AI-enabled attack UAV is armed and engages targets autonomously. While, theoretically, a deep attack UAV could remain under human-in-the-loop or on-the-loop control, this would require unimpeded, long-range, high-quality communications with very low latency. Relying on such communications in a major war combat situation where an adversary was actively jamming and deceiving would be imprudent on several levels. Continuing to use UAVs in their 'find' and, as later discussed, 'fool' role may be preferred.

An attack on the IADS is likely to involve crewed and AI-enabled UAVs operating as human–machine teams. Historically, using mass sharply reduces attrition, as the IADS becomes overwhelmed and its effectiveness declines.[212] An attack then may involve a small number of crewed aircraft attackers and a large number of supporting UAVs.

The supporting UAVs undertaking 'find' tasks will be collecting data to be both used during the attack and also to inform future attack planning. In terms of using data during an attack, the UAVs could pass information directly to the crewed aircraft, albeit there are considerable dangers in saturating the crew with information. More realistically, the data would be sent via the cloud to a fusion centre to update the situational awareness of the command and control centre. The centre's commander would then approve what data was time-critical to pass to the airborne attack aircraft; this is a task best left for a human.

The supporting UAVs would also have an important 'fool' role. The reconnaissance UAVs may incorporate first-wave or second-wave AI to instruct them on how to avoid being engaged. The 'fool' UAVs may be the opposite, actively trying to drag the defending fighters towards them. With AI, the UAVs could emit a convincing electronic signature that would at least confuse the adversary IADS, affecting the hostile commander's cognition and slowing down decision-making. There are also a large number of electronic deception techniques and decoy approaches for the 'fool' UAVs to use to neutralise – at least for a time – the adversary's SAM systems.

The large gaggle of UAVs performing 'find and fool' roles simultaneously and in coordination with the crewed aircraft attack will present the adversary IADS with several interlinking problems. There is a view that rather than a massed, deliberately obvious attack that stealth aircraft operating as 'alone and unafraid' singletons could achieve similar results. However, in some earlier conflicts, stealth aircraft operated with electronic warfare support. The idea being that the low signature stealth aircraft

[212] Warden, *The Air Campaign*, 70–73, 170–171.

would be hidden among the barrage of very noisy, false electronic transmissions. In considering major peer conflict, continuing with this 'belts and braces', bootstrap approach may be sensible.[213] Regardless of which option is chosen, stealth aircraft would still need good adversary IADS mapping before penetrating hostile airspace.

The 'find and fool' UAVs so far have been envisaged as being used independently of the crewed aircraft, albeit coordinated with them in time, space and manoeuvres. In that vein, various loyal wingman concepts are emerging that envisage crewed aircraft and UAVs working closely together. Australia, the United Kingdom, Russia and the US are each actively investigating alternatives.[214]

The term 'loyal wingman' is perhaps a little misleading. Wingmen, in a traditional sense, provide mutual support in expected and unexpected circumstances, in particular, to warn of a sudden surprise attack when aggressively manoeuvring or in level flight.[215] This seems a step beyond what first-wave or second-wave AI can achieve. Such AI can undertake specific allocated tasks, but mutual support is considerably more complicated.

Instead, a crewed aircraft could operate in conjunction with several UAVs flying in a tactically-appropriate mixed formation. The crewed aircraft would dispatch each UAV sequentially or together to undertake specific tasks as the mission progressed.[216] One task might be sending a first-wave or second-wave AI-enabled UAV to engage an approaching fighter in the manner detailed earlier in the defence concept. The UAV might be unarmed but would definitely distract the adversary aircraft in being a potential threat that needed to be honoured. Similar confusion might be possible in allocating a UAV to joust with a SAM system that suddenly activated and posed particular problems. Another option may be an accompanying UAV carrying weapons that the crewed aircraft could authorise to fire at a human-approved air or surface

[213] Dave Majumdar, 'Stealth vs. Electronic Attack', *USNI News*, 21 April 2014. https://news.usni.org/2014/04/21/stealth-vs-electronic-attack

[214] Examples include: Andrew McLaughlin, 'First RAAF Loyal Wingman Unmanned Combat System Rolled Out', *ADBR*, 5 May 2020, https://adbr.com.au/first-raaf-loyal-wingman-unmanned-combat-system-rolled-out/; Joseph Trevithick, 'Here's Who's in the Running to Build the Royal Air Force's First Loyal Wingman Drones', *The Drive*, 30 June 2020, https://www.thedrive.com/the-war-zone/34498/united-kingdom-will-decide-soon-who-will-build-its-first-loyal-wingman-drones; Joseph Trevithick, 'Watch Russia's S-70 Unmanned Combat Air Vehicle Fly With an Su-57 for the First Time', *The Drive*, 27 September 2019, https://www.thedrive.com/the-war-zone/30053/watch-russias-s-70-unmanned-combat-air-vehicle-fly-with-an-su-57-for-the-first-time; Garrett Reim, 'US Air Force Launches Skyborg Competition, Artificial Intelligence for Loyal Wingman UAV', *Flight Global*, 19 May 2020. https://www.flightglobal.com/military-uavs/us-air-force-launches-skyborg-competition-artificial-intelligence-for-loyal-wingman-uav/138426.article

[215] Shaw, *Fighter Combat*, 195–196.

[216] Japan's proposed next-generation fighter aircraft is apparently being designed to direct up to 3 accompanying 'loyal wingman' UAVs: Stephen Kuper, 'Japan Reveals More Details on Future Fighter Development Program', *Defence Connect*, 9 November 2020. https://www.defenceconnect.com.au/strike-air-combat/7150-japan-reveals-more-details-on-future-fighter-development-program

target. Indeed, this is one of the rationales for mutual support: the ability to bring concentrated fire to bear. These various uses of accompanying UAVs would be very useful tactically but, in requiring deliberate remote aircrew command and control, are not equivalent to a warning of a surprise attack that a crewed 'loyal wingman' aircraft can provide.

The offensive counter-air concept uses AI-enabled UAVs for numerous diverse tasks. The UAV mix would then be heterogeneous, with different designs for different missions. Some UAVs may be designed to be expendable, some reusable and some able to be lost if necessary. Equally, some may require runways to operate from whereas others might be air-launched from transport aircraft or zero-launched from the ground and recovered by parachute.[217] The runway-using UAVs could be larger and thus have a longer range and carry more payload. The air-launched and zero-launched alternatives may be smaller and cheaper with more limited capabilities but, in having considerable basing flexibility, might operate closer to hostile territory or when airfields are unavailable or interdicted.

Force structure issues

The war-in-the-air concept imagines a wide diffusion of AI both horizontally and vertically across an air force structure. However, unlike at sea or on land, there is a significant constraint in where AI can be easily applied. Crewed aircraft cannot be readily modified. Instead, with flight safety critical, they must go through a long and laborious development and test process. AI can be much more easily incorporated in surface systems and UVs, as these do not have safety-critical issues. Accordingly, the initial AI-enabled, war-in-the-air operational concepts will most likely involve developing and using appropriate surface systems and UVs, rather than modifying crewed aircraft.

The wide diffusion mentioned raises network concerns. The cloud that interconnects the diverse AI-enabled systems and vehicles needs to be common, not bespoke to each. Crewed aircraft are traditionally designed to be proprietary products, where the original aircraft manufacturer tightly controls software and hardware engineering. Seemingly anomalies then occur by design. For example, USAF's Lockheed Martin-built F-22 and F-35 stealth fighters can data link information between themselves but not to other aircraft types or each other. Maintaining this closed system approach in an era of AI-enabled, war-in-the-air operational concepts would be problematic. Instead, an open system approach needs to be embraced so that new AI-enabled

[217] Mark Gunzinger and Lukas Autenried, *Understanding the Promise of Skyborg and Low-Cost Attritable Unmanned Aerial Vehicles* (Arlington: The Mitchell Institute for Aerospace Studies, September 2020), 17. https://a2dd917a-65ab-41f1-ab11-5f1897e16299.usrfiles.com/ugd/a2dd91_2a1da65374434775b321619daf50a0a3.pdf

equipment and networks are ‘plug and play’. Having common data standards and an accessible cloud is essential.

In a future, AI-enabled war-in-the-air, the rules of engagement may be more permissive then currently. Today, a crewed reconnaissance aircraft collecting IADS-related information in peacetime in international airspace will not be engaged, given that the perceived penalties in global disdain and the possibility of unintentionally starting a war are just too high. Uncrewed reconnaissance vehicles, however, appear different. The US accepted the loss of a Global Hawk UAV to an Iranian SAM system without responding.[218] This may have set a behavioural norm.

In the same vein, bringing down a UAV in international airspace may be done deliberately in an attempt to gain technical intelligence on the UAV and its surveillance systems. Parts of the Global Hawk drone were recovered by Iran, allowing detailed inspection.[219] Several years earlier, Iran also recovered a USAF RQ-170 Sentinel reconnaissance UAV, reverse-engineered it and put a copy into service, as they had done before that with a small USN Scan Eagle drone.[220] This retrieval, inspection, copy and manufacture process may become customary.

Iranian actions have some resonances with the cases of the retrieval of the Sea Glider by China and the REMUS 600 by the Houthis. Overall, it seems prudent for AI-enabled UAVs on peacetime missions to use readily available commercial reconnaissance systems rather than possibly more capable but classified, intelligence collection systems. Moreover, it should always be remembered in tasking such missions that there is a possibility that a downed UAV may be reverse-engineered and used by an adversary.

[218] Jeff Mason and Susan Heavey, ‘Trump Says He Aborted Retaliatory Strike to Spare Iranian Lives’, *Reuters*, 20 June 2019. https://www.reuters.com/article/us-mideast-iran-usa-idUSKCN1TL07P

[219] H. I. Sutton, ‘Iran Rebuilds U.S. Navy Global Hawk UAV It Shot Down’, *Forbes*, 14 July 2020. https://www.forbes.com/sites/hisutton/2020/07/14/shot-down-us-navy-global-hawk-reconstructed-by-iran/?sh=4bc0fb337fd1

[220] Barbara Opall-Rome, ‘Israel Air Force Says Seized Iranian Drone Is a Knockoff of US Sentinel’, *Defense News*, 12 February 2018. https://www.defensenews.com/global/mideast-africa/2018/02/12/israel-air-force-says-seized-iranian-drone-is-a-knockoff-of-us-sentinel/; Michael Peck, ‘Iran Gifts ScanEagle Copy to Russia’, *C4ISRNET*, 2 November 2015. https://www.c4isrnet.com/unmanned/uas/2015/11/02/iran-gifts-scaneagle-copy-to-russia/

Conclusion

In the near-to-medium term, AI's principal attraction for military forces will be its ability to quickly identify patterns and detect items hidden within very large data troves. AI will make it much easier to detect, localise and identity objects across the battlespace. Hiding will become increasingly difficult.

However, the technology of contemporary AI has inherent problems. It is brittle, in being able to operate only in the context it has been trained for; it is unable to transfer knowledge gained in one task to another and it is dependent on data. Accordingly, AI when used in real-world situations needs to be teamed with humans. The strengths of AI can then counterbalance the weaknesses in human cognition and vice versa. World chess champion Garry Kasparov observed of a chess tournament involving human-machine teams that:

> Teams of human plus machine dominated even the strongest computers … Human strategic guidance combined with the tactical acuity of a computer was overwhelming … [W]e could concentrate on strategic planning instead of spending so much time on calculations. Human creativity was even more paramount under these conditions.[221]

As a general-purpose technology, AI is becoming all-pervasive and will over time infuse most military equipment. Such ubiquity though means AI is likely to be initially employed within existing operational level thinking. In the short-to-medium term, it will enable the battlefield, not remake it.

In simple terms, AI's principal warfighting utility can be expressed as 'find and fool'. With its machine learning, AI is excellent at finding items hidden within a high-clutter background. In this role, AI is better than humans and tremendously faster. On the

[221] Garry Kasparov, 'The Chess Master and the Computer', review of Chess Metaphors: *Artificial Intelligence and the Human Mind*, by Diego Rasskin-Gutman, trans. Deborah Klosky, *The New York Review of Books*, 11 February 2010, paragraph 22–24. https://www.nybooks.com/articles/2010/02/11/the-chess-master-and-the-computer/

other hand, AI can be fooled through various means. AI's great finding capabilities lack robustness.

AI's 'find' abilities further provide mobile systems with a new level of autonomy, as the AI can analyse its surroundings to discern important operating data. This means that 'find and fool' tasks can be undertaken using in-motion and at-rest, AI-enabled systems featuring varying levels of autonomy. AI can bring to modern warfighting enhanced sensors, improved kinetic and non-kinetic kill systems, more convincing deception techniques and a wide array of ways to confuse. In this, it is crucial to remember that AI enlivens other technologies. AI is not a stand-alone actor, rather it works in combination with numerous other digital technologies, providing a form of cognition to these.

If being used for defensive tasks, a large number of low-cost IoT sensors using AI edge computing could be emplaced in the optimum land, sea, air, space and cyber locations in a territory in which an attacking force may move across. From these sensors, a deep understanding would be gained of the area's terrain, sea conditions, physical environment and local virtual milieu. Having this background data accelerates AI's detection of any movement of hostile military forces across it.

The fixed and mobile IoT sensors are connected into a robust cloud to reliably feed data back into remote command support systems that, using well-trained AI, can rapidly filter out important information. Using this, AI is able to forecast adversary actions, and predict optimum own force employment and its combat effectiveness.

Hostile forces geolocated by AI can, after approval by human commanders, be quickly engaged using indirect fire including long-range guns, missiles or attack drones. Such an approach can engage close or deep targets, the key issues being data on the targets and the availability of suitable range firepower. A defended territory can quickly become a no-go zone.

To support the 'fool' function, UVs could be deployed across the battlespace, equipped with a variety of electronic systems designed to defeat and deceive the adversary's AI 'find' capabilities. In being made mobile through AI, these UVs will be harder for an enemy to destroy than fixed jammers. Moreover, mobile UVs can be risked and sent close in to approaching hostile forces to maximise jamming effectiveness.

In the offence, the attacker can choose the location and timing of the attack. The offence can thus mass UVs in large numbers in both space and time to break through a point in the defender's close battle zone. As the defender must cover a large front, an attacker can fight attrition battles using semi-expendable UVs to create an opening that forces following on can exploit.

Rather than being by a single large force, the penetration can now be by numerous, small, fast manoeuvre units that employ UVs and are connected through the cloud to each other and the command and control system. These units could mass, exchange target intelligence, swarm and then attack using their diverse capabilities. The swarm's overall situational awareness would come from each of the units exchanging information, supplemented by the more comprehensive surveillance provided by the remote AI-enabled command and control system located in friendly territory.

The defence and offence operational concepts discussed are generic, greatly abbreviated and rather abstract as far as domains are concerned. In reality, land, sea and air operations are quite dissimilar. In this paper, the generic concepts were placed into each of the three traditional domains and expanded upon to give a greater level of detail and highlight additional issues and concerns.

This paper aimed to stimulate thinking about human–machine teams operating on the future, AI-enabled battlefield. Beyond this, a suitable next step may be to wargame, model or simulate the various sea, land and air concepts described. This would help advance the long process of evolving the optimum operational concepts for the future, AI-enabled battlefield.

Such wargaming could build from this paper into two new areas. The first is joint warfare. This paper considered sea, land and air separately and at the tactical level. Joint warfare concepts that integrate across the three domains, and perhaps include space and cyber, need developing. The second area is to shift from a focus on own force to instead force-on-force. Future peer-competitor conflicts will be systems confrontations between opposing battle networks. Adversary battle networks will probably use AI for different purposes than this paper outlines and accordingly fight using different operational concepts. The interactions between the battle networks and their interdependencies will be important to understand and, to achieve victory, to exploit.

Several nations are already experimenting with new AI-enabled equipment in challenging battlefield scenarios and realistic exercises. As military forces usually take considerable time to reorient, there is no time like the present to begin the journey into an AI-enabled future.

Bibliography

Afina, Yasmin. 'Rage Against the Algorithm: The Risks of Overestimating Military Artificial Intelligence'. Last modified 27 August 2020. https://www.chathamhouse.org/2020/08/rage-against-algorithm-risks-overestimating-military-artificial-intelligence.

AIM Implementation Team. *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines.* Washington: Office of the Director of National Intelligence, 2019. https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf.

Allen, Greg. *Understanding AI Technology*. Washington: Joint Artificial Intelligence Center, April 2020. https://www.ai.mil/docs/Understanding%20AI%20Technology.pdf.

Anadiotis, George. 'Artificial Intelligence in the Real World: What Can It Actually Do?' *ZDNet*, 22 February 2017. https://www.zdnet.com/article/artificial-intelligence-in-the-real-world-what-can-it-actually-do/.

Axe, David. 'In a War with China, Where Should the U.S. Army Put Its Thousand-Mile Cannons?' *Forbes*, 11 August 2020. https://www.forbes.com/sites/davidaxe/2020/08/11/in-a-war-with-china-where-should-the-us-army-put-its-thousand-mile-cannons/#3b8e042249c8.

Ball, Mike. 'Liquid Robotics Wave Glider USV Travels More Than 2800 Nautical Miles'. *Unmanned Systems Technology*, 7 July 2016. https://www.unmannedsystemstechnology.com/2016/07/liquid-robotics-wave-glider-usv-travels-more-than-2800-nautical-miles/.

Bekar, Clifford, Kenneth Carlaw and Richard Lipsey. 'General Purpose Technologies in Theory, Application and Controversy: A Review'. *Journal of Evolutionary Economics* 28, no. 5 (2018): 1005–1033.

Ben-Ari, Mordechai and Francesco Mondada. *Elements of Robotics*. Cham: Springer Open, 2018.

Bennett, Harry. 'Capital Ship 2035: The Mission Command Vessel (MCV)'. *Center for International Maritime Security*, 31 August 2017. http://cimsec.org/capital-ship-2035-mission-command-vessel-mcv/33891.

Bipartisan Policy Center and Center for Security and Emerging Technology. *Artificial Intelligence and National Security*. Washington: Bipartisan Policy Center and Center for Security and Emerging Technology, June 2020. https://bipartisanpolicy.org/wp-content/uploads/2020/07/BPC-Artificial-Intelligence-and-National-Security_Brief-Final-1.pdf.

Blank, Steve. 'The Chip Wars of the 21st Century'. *War on the Rocks*, 11 June 2020. https://warontherocks.com/2020/06/the-chip-wars-of-the-21st-century/.

Burgess, Richard R. 'Triton Deploys at Last: The Navy Takes Its New UAV to the Western Pacific'. *Seapower*, 29 April 2020. https://seapowermagazine.org/triton-deploys-at-last-the-navy-takes-its-new-uav-to-the-western-pacific/.

Burke, Edmund J., Kristen Gunness, Cortez A. Cooper III and Mark Cozad. *People's Liberation Army Operational Concepts*. Santa Monica: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RRA394-1.html.

Chekinov, S. G. and S. A. Bogdanov. 'Initial Periods of War and Their Impact on a Country's Preparations for Future War'. *Voennaya Mysl (Military Thought)*, no. 11 (2012): 14–27.

Choi, Jacob. '#LOGBOTs – Making Army Logistics "Hard to Find, Hard to Hit and Hard to Kill"'. *Grounded Curiosity*, 18 November 2018. https://groundedcuriosity.com/logbots-making-army-logistics-hard-to-find-hard-to-hit-and-hard-to-kill/#.X5JHUlMzZwe.

Churchill, Winston S. *The World Crisis.* Vol.3. New York: Charles Scribner's Sons, 1927.

Clark, Bryan, Seth Cropsey and Timothy A. Walton. *Sustaining the Undersea Advantage: Disrupting Anti-Submarine Warfare Using Autonomous Systems*. Washington: Hudson Institute, September 2020. https://s3.amazonaws.com/media.hudson.org/Clark%20Cropsey%20Walton_Sustaining%20the%20Undersea%20Advantage.pdf.

Clark, Bryan, Daniel Patt and Harrison Schramm. *Mosaic Warfare Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations.* Washington: Center for Strategic and Budgetary Assessments, 2020. https://csbaonline.org/uploads/documents/Mosaic_Warfare_Web.pdf.

Clark, Bryan and Timothy A. Walton. *Taking Back the Seas: Transforming the U.S. Surface Fleet for Decision-Centric Warfare*. Washington: Center for Strategic and Budgetary Assessments, 2019. https://csbaonline.org/uploads/documents/Taking_Back_the_Seas_WEB.pdf.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1984.

'Computer Vision Dazzle Camouflage'. CV Dazzle. Last modified 15 June 2020. https://cvdazzle.com/.

Cox, Samuel. 'An Interview with Robin Smith: Robotic and Autonomous Systems in the Australian Army'. *Grounded Curiosity*, 2 March 2020. https://groundedcuriosity.com/wp-content/uploads/2020/02/LTCOL-Robin-Smith-Interview-APPROVED.pdf.

'DARPA Takes the IoT to Sea'. *GCN*, 3 January 2020. https://gcn.com/articles/2020/01/03/darpa-ocean-of-things.aspx.

Davis, Zachary S. *Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise*. Lawrence Livermore National Laboratory: Center for Global Security Research, March 2019. https://cgsr.llnl.gov/content/assets/docs/CGSR-AI_BattlefieldWEB.pdf.

Davies, Andrew. 'Geek of the week: Frederick Lanchester and Why Quantity Has a Quality All of its Own'. *The Strategist,* Australian Strategic Policy Institute, 20 September 2013. https://www.aspistrategist.org.au/geek-of-the-week-frederick-lanchester-and-why-quantity-is-a-quality.

Deakin University. 'Australian Army Funding Drives Deakin's Autonomous Vehicle Research'. Media release 24 August 2020. https://www.deakin.edu.au/about-deakin/media-releases/articles/australian-army-funding-drives-deakins-autonomous-vehicle-research.

Defense Advanced Research Projects Agency. 'AI Next Campaign'. Accessed 9 January 2021. https://www.darpa.mil/work-with-us/ai-next-campaign.

Defense Advanced Research Projects Agency. 'AlphaDogfight Trials Foreshadow Future of Human-Machine Symbiosis'. Last modified 26 August 2020. https://www.darpa.mil/news-events/2020-08-26.

Defense Innovation Board. *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense. Supporting Document.* Defense Innovation Board, November 2019. https://media.defense.gov/2019/Oct/31/2002204459/-1/-1/0/DIB_AI_PRINCIPLES_SUPPORTING_DOCUMENT.PDF.pdf.

Dempsey, Michael. 'Robot Tanks: On Patrol but Not Allowed to Shoot'. *BBC News*, 21 January 2020. https://www.bbc.com/news/business-50387954.

Dente, J. Frederick and Timothy Lee. 'Robots and Reconnaissance: We May Never Be Stealthy and Deliberate Again'. *Armour: Mounted Maneuver Journal* CXXXIII, no. 2 (Spring 2020): 14–17.

Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy-Harnessing AI to Advance Our Security and Prosperity*, published online 12 February 2019 United States of America Department of Defense, Washington DC. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

Department of the Navy. *The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*. Washington: Headquarters United States Marine Corps, September 2016. https://www.mcwl.marines.mil/Portals/34/Images/MarineCorpsOperatingConceptSept2016.pdf.

Deptula, David A., Heather R. Penney, Lawrence A. Stutzriem and Mark A. Gunzinger. *Restoring America's Military Competitiveness: Mosaic Warfare*. Arlington: The Mitchell Institute for Aerospace Studies, 2019.

Dillow, Clay. 'Oceangoing Robot Comes Ashore in Australia, Completing a 9,000-Mile Autonomous Pacific Crossing'. *Popular Science*, 5 December 2012. https://www.popsci.com/technology/article/2012-12/oceangoing-robot-comes-ashore-australia-completing-9000-mile-autonomous-pacific-crossing/.

Director, Operational Test and Evaluation *FY 2015 Annual Report*, (Washington: Department of Defense, January 2016). https://www.dote.osd.mil/Portals/97/pub/reports/FY2015/other/2015DOTEAnnualReport.pdf?ver=2019-08-22-105555-363

Dong, Xiao, Jiasong Wu and Ling Zhou. 'Demystifying AlphaGo Zero as AlphaGo GAN'. Cornell University, 24 November 2017. https://arxiv.org/pdf/1711.09091.pdf.

Dujmovic, Jurica. ‘Drone Warship Sea Hunter of the U.S. Navy is Powered by Artificial Intelligence’. *MarketWatch*, 3 July 2019. https://www.marketwatch.com/story/drone-warship-sea-hunter-of-the-us-navy-is-powered-by-artificial-intelligence-2019-07-03.

Eckstein, Megan. ‘Common Standards, Software Key to Navy’s Common Standards Unmanned Systems Future Unmanned Systems’. *USNI News*, 10 September 2020. https://news.usni.org/2020/09/10/common-standards-software-key-to-navys-future-unmanned-systems.

Eckstein, Megan. ‘Navy, Industry Pursuing Autonomy Software, Reliable HM&E Systems for Unmanned Ships’. *USNI News*, 31 January 2020. https://news.usni.org/2020/01/31/navy-industry-pursuing-autonomy-software-reliable-hme-systems-for-unmanned-ships.

Eckstein, Megan. ‘Navy to Field “Optionally Unmanned” Vessels to Supplement Future Surface Combatant’. *USNI News*, 25 June 2018. https://news.usni.org/2018/06/25/navy-looking-at-optionally-unmanned-vessel-to-supplement-future-surface-combatant-program.

Eckstein, Megan. ‘Program Office Maturing USVs, UUVs with Help from Industry, International Partners’. *USNI News*, 23 June 2020. https://news.usni.org/2020/06/23/program-office-maturing-usvs-uuvs-with-help-from-industry-international-partners.

Eckstein, Megan. ‘Wargames This Year to Inform Future Surface Combatant Requirements’. *USNI News*, 21 February 2017. https://news.usni.org/2017/02/21/wargames-future-surface-combatant-requirements.

Engstrom, Jeffrey. *Systems Confrontation and System Destruction Warfare: How the Chinese People’s Liberation Army Seeks to Wage Modern Warfare*. Santa Monica: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR1708.html.

Erickson, John. ‘The Development of Soviet Military Doctrine: The Significance of Operational Art and Emergence of Deep Battle’. In *The Origins of Contemporary Doctrine*, edited by John Gooch, 81–112. Camberley: Strategic and Combat Studies Institute, September 1997.

Esper, Mark T. ‘Secretary of Defense Remarks for DOD Artificial Intelligence Symposium and Exposition’, US Department of Defense, 9 September 2020. Transcript, https://www.defense.gov/Newsroom/Speeches/Speech/Article/2341130/secretary-of-defense-remarks-for-dod-artificial-intelligence-symposium-and-expo/.

Fadok, David S. ‘John Boyd and John Warden: Airpower’s Quest for Strategic Paralysis’. In *The Paths of Heaven: The Evolution of Airpower Theory*, edited by Phillip S. Meilinger, 357–398. USAF Maxwell Air Force Base: Air University Press, 1997.

Fleming, John L. *Capital Ships: A Historical Perspective*. Newport: Naval War College, 1994.

Fox, Amos C. *Hybrid Warfare: The 21st Century Russian Way of War*. Fort Leavenworth: School of Advanced Military Studies, 2017. http://www.dtic.mil/dtic/tr/fulltext/u2/1038987.pdf.

Fox, Amos C. ‘A Solution Looking for a Problem: Illuminating Misconceptions in Maneuver-Warfare Doctrine’. *Armour: Mounted Maneuver Journal* CXXIX, no.4, (Fall 2017): 17–26.

Freedberg, Sydney J. Jr. ‘AI & Robots Crush Foes in Army Wargame’. *Breaking Defense*, 19 December 2019. https://breakingdefense.com/2019/12/ai-robots-crush-foes-in-army-wargame/.

Freedberg, Sydney J. Jr. 'Army Future Ops Depend on Cloud – But not on JEDI'. *Breaking Defense*, 29 July 2020. https://breakingdefense.com/2020/07/army-future-ops-depend-on-cloud-but-not-on-jedi/.

Freedberg, Sydney J. Jr. 'Big Data for Big Wars: JEDI vs. China & Russia'. *Breaking Defense*, 12 August 2019. https://breakingdefense.com/2019/08/big-data-for-big-wars-jedi-vs-china-russia/.

Freedberg, Sydney J. Jr. 'Marines Explore Robots & 5G Networks for Future Wars'. *Breaking Defense*, 31 August 2020. https://breakingdefense.com/2020/08/marines-explore-robots-5g-networks-for-future-wars/.

Freedberg, Sydney J. Jr. 'Robots & Puddles: Surprises from Army RCV Test'. *Breaking Defense*, 7 August 2020. https://breakingdefense.com/2020/08/robots-vs-puddles-surprises-from-army-rcv-test/.

Fuller, Colonel J. F. C. *The Foundations of the Science of War*. London: Hutchinson & Co., 1926.

Gady, Franz-Stefan. 'What Does AI Mean for the Future of Manoeuvre Warfare?' *International Institute for Strategic Studies* (blog), 5 May 2020. https://www.iiss.org/blogs/analysis/2020/05/csfc-ai-manoeuvre-warfare.

Galdorisi, George. 'The Navy Needs AI, It's Just not Certain Why'. *USNI Proceedings*, 145/5/1,395, May 2019. https://www.usni.org/magazines/proceedings/2019/may/navy-needs-ai-its-just-not-certain-why.

Gartner. 'Gartner Identifies Top 10 Data and Analytics Technology Trends for 2019'. Media release 18 February 2019. https://www.gartner.com/en/newsroom/press-releases/2019-02-18-gartner-identifies-top-10-data-and-analytics-technolo.

Glenney, Bill. 'Institute for Future Warfare Studies Wants Your Writing on the Capital Ship of the Future'. *Center for International Maritime Security*, 18 July 2017. http://cimsec.org/institute-for-future-warfare-studies-wants-your-writing-on-the-capital-ship-of-the-future/33307.

Grau, Lester W. and Charles K. Bartles. 'The Russian Reconnaissance Fire Complex Comes of Age'. *Changing Character of War Centre* (blog), May 2018. http://www.ccw.ox.ac.uk/blog/2018/5/30/the-russian-reconnaissance-fire-complex-comes-of-age.

Gruetzemacher, Ross, David Paradice and Kang Bok Lee. 'Forecasting Transformative AI: An Expert Survey'. *Computers and Society: Cornell University*, 16 July 2019. https://arxiv.org/abs/1901.08579.

Gunzinger, Mark and Lukas Autenried. *Understanding the Promise of Skyborg and Low-Cost Attritable Unmanned Aerial Vehicles*. Arlington: The Mitchell Institute for Aerospace Studies, September 2020. https://a2dd917a-65ab-41f1-ab11-5f1897e16299.usrfiles.com/ugd/a2dd91_2a1da65374434775b321619daf50a0a3.pdf.

Hawley, John K. *Patriot Wars: Automation and the Patriot Air and Missile Defense System*. Washington: Center for a New American Security, 2017. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/CNAS-Patriot%20Wars.pdf.

Hattendorf, John B.. 'The Idea of a "Fleet in Being" in Historical Perspective,' *Naval War College Review* 67 no. 1 (Winter 2014): 43-60.

Henriksen, Dag. 'Control of the Air'. In *Routledge Handbook of Air Power*, 1st ed., edited by John Andreas Olsen, 83–94. London: Routledge Taylor & Francis Group, 2018.

Hoadley, Daniel S. and Kelley M. Sayler, *Artificial Intelligence and National Security: Updated November 10, 2020* (Washington DC: Congressional Research Service, 2020). https://crsreports.congress.gov/product/pdf/R/R45178/10

Holmes, Aaron. 'These Clothes Use Outlandish Designs to Trick Facial Recognition Software into Thinking You're Not Human'. *Business Insider*, 13 October 2019. https://www.businessinsider.com.au/clothes-accessories-that-outsmart-facial-recognition-tech-2019-10?r=US&IR=T.

Howson, Edward. 'Moving Forward – The Future of Cavalry Reconnaissance'. *The Cove*, 12 August 2020. https://cove.army.gov.au/article/moving-forward-the-future-cavalry-reconnaissance.

Hughes, Wayne P. and Robert Girrier. *Fleet Tactics and Naval Operations*, 3rd ed. Annapolis: Naval Institute Press, 2018.

Hurst, Jules. 'Robotic Swarms in Offensive Maneuver'. *Joint Force Quarterly* 87, 4th Quarter, (October 2017): 105–111.

Insinna, Valerie. 'Navy to Kick Off Extra Large UUV Competition This Month'. *Defense News*, 10 January 2017. https://www.defensenews.com/digital-show-dailies/surface-navy-association/2017/01/10/navy-to-kick-off-extra-large-uuv-competition-this-month/.

Javorsek, Daniel. 'Air Combat Evolution (ACE)'. *Defense Advanced Research Projects Agency*, Accessed 10 January 2021. https://www.darpa.mil/program/air-combat-evolution.

Joe, Rick. 'China's Growing High-End Military Drone Force'. *The Diplomat*, 27 November 2019. https://thediplomat.com/2019/11/chinas-growing-high-end-military-drone-force/.

Jones, Scott. 'Third Wave AI: The Coming Revolution in Artificial Intelligence'. *Medium*, 28 August 2018. https://medium.com/@scott_jones/third-wave-ai-the-coming-revolution-in-artificial-intelligence-1ffd4784b79e.

Kallenborn, Zachary. 'Swarming Sea Mines: Capital Capability?' *Center for International Maritime Security*, 29 August 2017. http://cimsec.org/swarming-sea-mines-capital-capability/33836.

Karber, Phillip and Joshua Thibeault. 'Russia's New-Generation Warfare'. *Association of the U.S. Army*, 20 May 2016. https://www.ausa.org/articles/russia%E2%80%99s-new-generation-warfare.

Kasapoglu, Can. *Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control*. Rome: NATO Defense College, November 2015. https://www.files.ethz.ch/isn/195099/rp_121.pdf.

Kasparov, Garry. 'The Chess Master and the Computer', review of *Chess Metaphors: Artificial Intelligence and the Human Mind*, by Diego Rasskin-Gutman, translated by Deborah Klosky. *The New York Review of Books*, 11 February 2010. https://www.nybooks.com/articles/2010/02/11/the-chess-master-and-the-computer/

Kaushal, Sidharth. 'The Type 055: A Glimpse into the PLAN's Developmental Trajectory'. *RUSI Defence Systems* 22, no. 1 (19 October 2020). https://rusi.org/publication/rusi-defence-systems/type-055-glimpse-plan%E2%80%99s-developmental-trajectory.

Keegan, John. *The Price of Admiralty: The Evolution of Naval Warfare*. New York: Penguin, 1988.

Keller, John. 'Not Just for the Navy: Unmanned Surface Vessels (USVs) in Wide Use for Surveillance at NOAA'. *Military & Aerospace Electronics*, 29 March 2016. https://www.militaryaerospace.com/unmanned/article/16714492/not-just-for-the-navy-unmanned-surface-vessels-usvs-in-wide-use-for-surveillance-at-noaa.

Keller, John. 'Pentagon Gets Serious about Unmanned Surface Vessels'. *Military & Aerospace Electronics*, 29 September 2020. https://www.militaryaerospace.com/unmanned/article/14184308/unmanned-surface-vessels-usv.

Kelnar, David. *The State of AI 2019: Divergence*. London: Barclays UK (BUK) Ventures, 2019. https://iec2021.aaru-confs.org/The-State-of-AI-2019-Divergence.pdf.

'Kleos Scouting Mission Smallsats Deployed'. *Satnews*, 10 November 2020. https://news.satnews.com/2020/11/10/kleos-scouting-mission-smallsats-deployed/.

Kline, Jeffrey E. 'Impacts of the Robotics Age on Naval Force Design, Effectiveness, and Acquisition'. *Naval War College Review* 70, no. 3 (Summer 2017): 77. https://digital-commons.usnwc.edu/nwc-review/vol70/iss3/5.

Konaev, Margarita and Samuel Bendett. 'Russian AI-Enabled Combat: Coming to a City Near You?' *War on the Rocks*, 31 July 2019, https://warontherocks.com/2019/07/russian-ai-enabled-combat-coming-to-a-city-near-you/.

Kongsberg. *Seaglider*. Horten: Kongsberg, May 2014. https://www.hydroid.com/sites/default/files/product_pages/Seaglider_Data_Sheet.pdf.

Kuper, Stephen. 'Japan Reveals More Details on Future Fighter Development Program'. *Defence Connect*, 9 November 2020. https://www.defenceconnect.com.au/strike-air-combat/7150-japan-reveals-more-details-on-future-fighter-development-program.

Larter, David B. '5 Things You Should Know about the US Navy's Plans for Autonomous Missile Boats'. *Defense News*, 13 January 2020. https://www.defensenews.com/digital-show-dailies/surface-navy-association/2020/01/13/heres-5-things-you-should-know-about-the-us-navys-plans-for-big-autonomous-missile-boats/.

Larter, David B. 'DARPA's Latest Mad Science Experiment: A Ship Designed to Operate Completely Without Humans'. *Defense News*, 21 January 2020. https://www.defensenews.com/naval/2020/01/21/darpas-latest-mad-science-experiment-a-ship-designed-completely-without-humans/.

Larter, David B. 'To Compete with China, an Internal Pentagon Study Looks to Pour Money into Robot Submarines'. *Defense News*, 1 June 2020. https://www.defensenews.com/naval/2020/06/01/to-compete-with-china-an-internal-pentagon-study-looks-to-pour-money-into-robot-submarines/.

Launchbury, John. 'A DARPA Perspective on Artificial Intelligence'. Defense Advanced Research Projects Agency. Accessed 9 January 2021. https://www.darpa.mil/attachments/AIFull.pdf.

Launchbury, John. 'A DARPA Perspective on Artificial Intelligence'. Defense Advanced Research Projects Agency. Streamed 15 February 2017. YouTube video, 16:11. https://www.youtube.com/watch?v=-O01G3tSYpU&list=LL5S74bRl-vBw9Fz8Gpxr6jQ&index=4537.

Layton, Peter. *Algorithmic Warfare: Applying Artificial Intelligence to Warfighting*. Canberra: Air Power Development Centre, 2018.

Layton, Peter. 'Artificial Intelligence, Big Data and Autonomous Systems Along the Belt and Road: Towards Private Security Companies with Chinese Characteristics?' *Small Wars & Insurgencies* 31, no. 4 (June 2020): 874–897.

Layton, Peter. *Fifth Generation Air Warfare*. Working paper 43. Canberra: Air Power Development Centre, 2017. https://airpower.airforce.gov.au/APDC/media/PDF-Files/Working%20Papers/WP43-Fifth-Generation-Air-Warfare.pdf.

Layton, Peter. 'Fifth Generation Surface Warfare Fleet Emerges'. *Defence Today* (September 2017): 13–18.

Layton, Peter. 'Our New Model Robot Armies'. *Small Wars Journal*, 7 August 2018. https://smallwarsjournal.com/index.php/jrnl/art/our-new-model-robot-armies.

Layton, Peter. *Prototype Warfare and the Fourth Industrial Age*. Canberra: Air Power Development Centre, 2019.

Layton, Peter. *Surfing the Digital Wave: Engineers, Logisticians and the Future Automated Airbase*. Canberra: Air Power Development Centre, 2020.

Leonhard, Robert R. *Fighting by Minutes: Time and the Art of War*, 2nd ed. N.P.: CreateSpace Independent Publishing Platform, 2017.

Levick, Ewen. 'Ocius Launches Latest USV'. *ADM: Australian Defence Magazine*, 27 August 2020. https://www.australiandefence.com.au/news/ocius-launches-latest-usv.

Lingel, Sherrill, Jeff Hagen, Eric Hastings, Mary Lee, Matthew Sargent, Matthew Walsh, Li Ang Zhang and David Blancett. *Joint All-Domain Command and Control for Modern Warfare: An Analytic Framework for Identifying and Developing Artificial Intelligence Applications*. Santa Monica: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR4408z1.html.

Liquid Robotics. 'The Digital Ocean: How Systems Can Work Together to Solve Our Planet's Biggest Challenges'. Last modified 2016. http://cdn2.hubspot.net/hubfs/287872/LR_DigitalOcean_eBook.pdf.

Liquid Robotics. 'Liquid Robotics Case Study: Monitoring Marine Protected Areas'. Last modified 2017. https://cdn2.hubspot.net/hubfs/287872/website-downloads/lr-cs-Pitcairn-mda_FINAL_web.pdf.

Liquid Robotics. 'The Wave Glider: Transform How You Understand the Ocean'. Last modified 2017. https://www.seismic.com.au/assets/pdf/Liquid-Robotics-WG_DataSheet-1-2_web.pdf.

Lomas, Natasha. 'Another AI Chatbot Shown Spouting Offensive Views'. *Tech Crunch*, 25 October 2017. https://techcrunch.com/2017/10/24/another-ai-chatbot-shown-spouting-offensive-views/.

MacFarland, Sean B. *Non-Linear Operations: A New Doctrine for a New Era*. Fort Leavenworth: United States Army Command and General Staff College, School of Advanced Military Studies, 1994. https://apps.dtic.mil/dtic/tr/fulltext/u2/a284137.pdf

MacKay, Niall. 'Lanchester Combat Models'. *Mathematics Today* 42 (2006). https://pure.york.ac.uk/portal/en/publications/lanchester-combat-models(cdc24eeb-4fc6-44ca-9153-972edbd9a154)/export.html.

Majumdar, Dave. 'Stealth vs. Electronic Attack'. *USNI News*, 21 April 2014. https://news.usni.org/2014/04/21/stealth-vs-electronic-attack.

Markotkin, Nikolai and Elena Chernenko. 'Developing Artificial Intelligence in Russia: Objectives and Reality'. Carnegie Moscow Center. Last modified 8 May 2020. https://carnegie.ru/commentary/82422.

Martinez, Dave, Nick Malyska, Bill Streilein, Rajmonda Caceres, William Campbell, Charlie Dagli, Vijay Gadepally, et al. *Artificial Intelligence: Short History, Present Developments, and Future Outlook*. Boston: Massachusetts Institute of Technology, January 2019. https://www.ll.mit.edu/sites/default/files/publication/doc/2019-09/Artificial%20Intelligence%20Short%20History%2C%20Present%20Developments%2C%20and%20Future%20Outlook%20-%20Final%20Report%20-%20Martinez.pdf.

Mason, Jeff and Susan Heavey. 'Trump Says He Aborted Retaliatory Strike to Spare Iranian Lives'. *Reuters*, 20 June 2019. https://www.reuters.com/article/us-mideast-iran-usa-idUSKCN1TL07P.

Maayan, Gilad David. 'The IoT Rundown for 2020: Stats, Risks and Solutions', *Security Today*, 13 January 2020. https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?p=1

McLaughlin, Andrew. 'First RAAF Loyal Wingman Unmanned Combat System Rolled Out'. *ADBR*, 5 May 2020. https://adbr.com.au/first-raaf-loyal-wingman-unmanned-combat-system-rolled-out/.

Meilinger, Phillip S. 'Giulio Douhet and the Origins of Airpower Theory'. In *The Paths of Heaven The Evolution of Airpower Theory*, edited by Phillip S. Meilinger, 1–40. USAF Maxwell Air Force Base: Air University Press, 1997.

Merkel, Angela. 'Speech by Federal Chancellor at the World Economic Forum Annual Meeting in Davos on 24 Jan 2018'. The Federal Government, 2018. Transcript, https://www.bundesregierung.de/Content/EN/Reden/2018/2018-01-24-bk-merkel-davos_en.html.

Milne, Sandy. 'Bluebottle USVs Green-Lit for Autonomous Operation'. *Defence Connect*, 8 July 2020. https://www.defenceconnect.com.au/strike-air-combat/6414-bluebottle-usvs-green-lighted-for-autonomous-operation.

Mizokami, Kyle. 'Russia's "Hunter" Is Unlike Anything in America's Arsenal'. *Popular Mechanics*, 10 August 2020. https://www.popularmechanics.com/military/aviation/a33548209/russia-hunter-combat-drone/.

Mizokami, Kyle. 'This Robot Tank Is the Future of Armored Warfare'. *Popular Mechanics*, 23 June 2020. https://www.popularmechanics.com/military/weapons/a32947926/type-x-robot-combat-vehicle/.

MMC Ventures. *The AI Playbook: The Step-by-Step Guide to Taking Advantage of AI in Your Business*. London: Barclays UK (BUK) Ventures, 2019. https://www.ai-playbook.com/.

Murray, Williamson and Allan R. Millett (eds.). *Military Innovation in the Interwar Period*. Cambridge: Cambridge University Press, 1998.

Naveh, Shimon. *In Pursuit of Military Excellence: The Evolution of Operational Theory*. London: Frank Cass, 1997.

Ocean Aero. *Ocean Aero Autonomous Underwater and Surface Vehicles*. San Diego: Ocean Aero, 2020. http://ems-ocean.com/catalogue2/Ocean%20Aero/OA%20AUSVs%202.19.pdf.

Office of the Secretary of Defense. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*. Washington: Office of the Secretary of Defense, 2020. https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF.

Opall-Rome, Barbara. 'Israel Air Force Says Seized Iranian Drone Is a Knockoff of US Sentinel'. *Defense News*, 12 February 2018. https://www.defensenews.com/global/mideast-africa/2018/02/12/israel-air-force-says-seized-iranian-drone-is-a-knockoff-of-us-sentinel/.

'Oshkosh Defense Delivers Autonomous Vehicles'. *Nation Shield: Military and Strategic Journal*, 2 February 2020. http://nationshield.ae/index.php/home/details/reports/oshkosh-defense-delivers-autonomous-vehicles/en#.X5JSdlMzZTZ.

Otis, Glenn K. 'Ascendancy of Fires: The Evolution of the Combined Arms Team'. *Field Artillery*, (June 1995): 17–19.

Panetta, Kasey. '5 Trends Drive the Gartner Hype Cycle for Emerging Technologies'. *Gartner*, 18 August 2020. https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020/.

Papernot, Nicolas, Patrick McDaniel, Somesh Jha, Matt Fredrikson, Z. Berkay Celik and Ananthram Swami. 'The Limitations of Deep Learning in Adversarial Settings'. *IEEE European Symposium on Security and Privacy (EuroS&P),* IEEE 2016, Saarbrucken, Germany, 21–24 March 2016. https://arxiv.org/pdf/1511.07528.pdf.

Pardo, John R. 'Parallel Warfare: Its Nature and Application'. In *Challenge and Response: Anticipating US Military Security Concerns*. Edited by Karl P. Magyar, 313–334. USAF Maxwell Air Force Base: Air University Press, August 1994.

Peck, Michael. 'Iran Gifts ScanEagle Copy to Russia'. *C4ISRNET*, 2 November 2015. https://www.c4isrnet.com/unmanned/uas/2015/11/02/iran-gifts-scaneagle-copy-to-russia/.

Perez, Sarah. 'Microsoft Silences Its New A.I. Bot Tay, After Twitter Users Teach It Racism [Updated]'. *Tech Crunch*, 25 March 2016. https://techcrunch.com/2016/03/24/microsoft-silences-its-new-a-i-bot-tay-after-twitter-users-teach-it-racism/.

Polyakova, Alina. '*Weapons of the weak: Russia and AI-driven asymmetric warfare', part of 'A Blueprint for the Future of AI' series,* Artificial Intelligence and Emerging Technology Initiative, Brookings, 15 November 2018. https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/

Rasser, Martijn, Rebecca Arcesati, Shin Oya, Ainikki Riikonen and Monika Bochert. *Common Code: An Alliance Framework for Democratic Technology Policy*. Washington: Center for a New American Security, October 2020.

Reim, Garrett. 'US Air Force Launches Skyborg Competition, Artificial Intelligence for Loyal Wingman UAV'. *Flight Global*, 19 May 2020. https://www.flightglobal.com/military-uavs/us-air-force-launches-skyborg-competition-artificial-intelligence-for-loyal-wingman-uav/138426.article.

Rogoway, Tyler. 'China Gives Drone Back—But Why Did They Grab It in The First Place?' *The Drive*, 20 December 2016. https://www.thedrive.com/the-war-zone/6604/china-gives-drone-back-but-why-did-they-grab-it-in-the-first-place.

Royal Australian Navy. *RAS-AI Strategy 2040*. Canberra: Royal Australian Navy, October 2020. https://www.navy.gov.au/sites/default/files/documents/RAN_WIN_RASAI_Strategy_2040f2_hi.pdf.

Schrauf, Stefan and Philipp Berttram. *Industry 4.0: How Digitization Makes the Supply Chain More Efficient, Agile, and Customer-Focused.* Strategy&. Munich: PwC Network, 7 September 2016. https://www.strategyand.pwc.com/gx/en/insights/digitization-more-efficient.html#Download.

'SEA Provides Leading ASW Sensor System for Australian Autonomous Surveillance Capability Trial'. *EDR Online*, 15 October 2020. https://www.edrmagazine.eu/sea-provides-leading-asw-sensor-system-for-australian-autonomous-surveillance-capability-trial.

Semiconductor Industry Association. *2020 State of the U.S. Semiconductor Industry.* Washington: SIA Semiconductor Industry Association, 2020. https://www.semiconductors.org/wp-content/uploads/2020/06/2020-SIA-State-of-the-Industry-Report.pdf.

Shameen, Assif. 'Tech: Why the US-China Chip War is Heating Up'. *The Edge Malaysia Weekly*, 25 September 2020. https://www.theedgemarkets.com/article/tech-why-uschina-chip-war-heating.

Shaneman, Shane. 'The AI Stack: A Blueprint for Developing & Deploying AI'. National Defense Industrial Association SO/LIC Symposium 2019, 3 February 2019. https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2019/solic/Shaneman.pdf.

Sharma, Nabin and Michael Blumenstein. 'SharkSpotter Combines AI and Drone Technology to Spot Sharks and Aid Swimmers on Australian Beaches'. *The Conversation*, 28 September 2018. https://theconversation.com/sharkspotter-combines-ai-and-drone-technology-to-spot-sharks-and-aid-swimmers-on-australian-beaches-92667.

Shaw, Robert L. *Fighter Combat: Tactics and Maneuvering*. Annapolis: Naval Institute Press, 1985.

Shead, Sam. 'Researchers: Are We on the Cusp of an "AI Winter"?' *BBC News*, 11 January 2020. https://www.bbc.com/news/technology-51064369.

Shelbourne, Mallory. 'DARPA Testing the Limits of Unmanned Ships in New NOMARS Program'. *USNI News*, 2 November 2020. https://news.usni.org/2020/10/27/darpa-testing-the-limits-of-unmanned-ships-in-new-nomars-program.

Silver, David and Demis Hassabis. 'AlphaGo Zero: Starting from Scratch'. *DeepMind* (blog), 18 October 2017. https://deepmind.com/blog/article/alphago-zero-starting-scratch.

Singh, Mandip. *Learning from Russia, How China Used Russian Models and Experiences to Modernize the PLA*. Berlin: Mercator Institute for China Studies, 23 September 2020. https://merics.org/en/report/learning-russia-how-china-used-russian-models-and-experiences-modernize-pla.

Skinner, Dan. 'The Integrated Digital Soldier System: Close Combat in the 21st Century'. *The Cove*, 6 August 2019. https://cove.army.gov.au/sites/default/files/the_integrated_digital_soldier_concept_v1.pdf.

Sokol, Joshua. 'Why Artificial Intelligence Like AlphaZero Has Trouble with the Real World'. *Quanta Magazine*, 21 February 2018. https://www.quantamagazine.org/why-alphazeros-artificial-intelligence-has-trouble-with-the-real-world-20180221/.

Spelman, Mark Bruce Weinelt, Peter Lacy, Anand Shah, Mehran Gul, William Hoffman and Reema Siyam, et al. *Digital Transformation Initiative: Unlocking $100 Trillion for Business and Society from Digital Transformation*. *Executive Summary*. Cologny: World Economic Forum in collaboration with Accenture, January 2017. https://www.accenture.com/_acnmedia/accenture/conversion-assets/wef/pdf/accenture-dti-executive-summary.pdf.

Spencer, Michael. *Pseudosatellites Disrupting Air Power Impermanence*. Canberra: Air Power Development Centre, 2019.

Stewart, Duncan, Jeff Loucks, Mark Casey and Craig Wigginton. 'Bringing AI to the Device: Edge AI Chips Come into Their Own'. *Deloitte Insights*, 9 December 2019. https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2020/ai-chips.html.

Stoner, Robert H. 'R2D2 with Attitude: The Story of the Phalanx Close-In Weapons'. NavWeaps. Last modified 30 October 2009. http://www.navweaps.com/index_tech/tech-103.php.

Strout, Nathan. 'How the Army Plans to Use Space and Artificial Intelligence to Hit Deep Targets Quickly'. *Defense News*, 5 August 2020. https://www.defensenews.com/digital-show-dailies/smd/2020/08/05/how-the-army-plans-to-use-space-and-artificial-intelligence-to-hit-deep-targets-quickly/.

Sutton, H. I. 'Iran Rebuilds U.S. Navy Global Hawk UAV It Shot Down'. *Forbes*, 14 July 2020. https://www.forbes.com/sites/hisutton/2020/07/14/shot-down-us-navy-global-hawk-reconstructed-by-iran/#15d3cc187fd1.

Talend. 'What is Data Fabric?' Accessed 9 January 2021. https://www.talend.com/resources/what-is-data-fabric/.

Thomas, Timothy L. *Russian Military Thought: Concepts and Elements*. McLean: The MITRE Corporation, August 2019. https://www.mitre.org/publications/technical-papers/russian-military-thought-concepts-and-elements.

Thomas, Timothy, *The Chinese Way of War: How Has it Changed?.* Public Release Case Number 20-1450. McLean: The MITRE Corporation, June 2020. https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-books/332777/download

Trajtenberg, Manuel. *AI as the Next GPT: A Political-Economy Perspective*. NBER Working Paper No. 24245. Cambridge: National Bureau of Economic Research, January 2018.

Trevithick, Joseph. 'Here's Who's in the Running to Build the Royal Air Force's First Loyal Wingman Drones'. *The Drive*, 30 June 2020. https://www.thedrive.com/the-war-zone/34498/united-kingdom-will-decide-soon-who-will-build-its-first-loyal-wingman-drones.

Trevithick, Joseph. 'Navy Establishes First Squadron to Operate Its Carrier-Based MQ-25 Stingray Tanker Drones'. *The Drive*, 1 October 2020. https://www.thedrive.com/the-war-zone/36859/navy-establishes-first-squadron-to-operate-its-carrier-based-mq-25-stingray-tanker-drones.

Trevithick, Joseph. 'Navy's Sea Hunter Drone Ship Is Getting a New Owner, New Abilities, and a Sister'. *The Drive*, 6 February 2018. https://www.thedrive.com/the-war-zone/18264/navys-sea-hunter-drone-ship-is-getting-a-new-owner-new-abilities-and-a-sister.

Trevithick, Joseph. 'This Containerized Launcher for the XQ-58A Valkyrie Combat Drone Could Be a Game Changer'. *The Drive*, 16 October 2019. https://www.thedrive.com/the-war-zone/30474/this-containerized-launcher-for-the-xq-58a-valkyrie-combat-drone-could-be-a-game-changer.

Trevithick, Joseph. 'Watch Russia's S-70 Unmanned Combat Air Vehicle Fly With an Su-57 for the First Time'. *The Drive*, 27 September 2019. https://www.thedrive.com/the-war-zone/30053/watch-russias-s-70-unmanned-combat-air-vehicle-fly-with-an-su-57-for-the-first-time.

Trevithick, Joseph and Tyler Rogoway. 'Mysterious Wave Glider Spotted Off Florida Keys Had Electronic Intel Gathering System (Updated)'. *The Drive*, 29 June 2020. https://www.thedrive.com/the-war-zone/34485/mysterious-wave-glider-vessel-spotted-off-florida-keys-has-electronic-intel-gathering-system.

Trimble, Steve and Lee Hudson. 'U.S. Army Flexes New Land-Based, Anti-Ship Capabilities'. *Aviation Week*, 20 October 2020. https://aviationweek.com/defense-space/missile-defense-weapons/us-army-flexes-new-land-based-anti-ship-capabilities.

Tucker, Patrick. 'An AI Just Beat a Human F-16 Pilot in a Dogfight – Again'. *Defense One*, 20 August 2020. https://www.defenseone.com/technology/2020/08/ai-just-beat-human-f-16-pilot-dogfight-again/167872/.

A. M. Turing, 'Computing Machinery and Intelligence', *Mind* 59, no. 236 (October, 1950): 433-460.

Underwood, Kimberly. 'A Lack of Major Movement Toward Human-Machine Teaming'. *Signal*, 2 September 2020. https://www.afcea.org/content/lack-major-movement-toward-human-machine-teaming.

U.S. Army. *The U.S. Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1. Fort Eustis: U.S. Army Training and Doctrine Command, 6 December 2018.

U.S. Army Research Laboratory. 'Internet of Battlefield Things'. Accessed 10 January 2021. https://www.arl.army.mil/business/collaborative-alliances/current-cras/iobt-cra/.

'U.S. Navy Selects Lockheed Martin to Deliver Large Unmanned Surface Vessel Study'. *Navy Recognition*, 18 September 2020. https://www.navyrecognition.com/index.php/news/defence-news/2020/september/9005-u-s-navy-selects-lockheed-martin-to-deliver-large-unmanned-surface-vessel-study.html.

Vincent, Brandi. ‘DARPA Wants Help Developing a “Sea Train” of Unmanned Warships’. *Nextgov*, 9 January 2020. https://www.nextgov.com/emerging-tech/2020/01/darpa-wants-help-developing-sea-train-unmanned-warships/162342/.

Wallace, Cory W., George M. Morris, Scott Stephens and Shawn D. Pardee. ‘Army Modernization in Next-Generation Vehicles Will Change the Battlefield’. *Armour: Mounted Maneuver Journal* CXXXIII, no. 2 (Spring 2020): 8–13.

Wan, Alvin. ‘What Explainable AI Fails to Explain (and How We Fix That)’. *Towards Data Science*, 17 April 2020. https://towardsdatascience.com/what-explainable-ai-fails-to-explain-and-how-we-fix-that-1e35e37bee07.

Warden, John A. III. *The Air Campaign: Planning for Combat*. Washington: National Defense University Press, 1988.

Waterston, John. ‘Ocean of Things’. Defense Advanced Research Projects Agency, Accessed 9 January 2021. https://www.darpa.mil/program/ocean-of-things.

Watling, Jack. *The Future of Fires: Maximising the UK’s Tactical and Operational Firepower*. London: Royal United Services Institute for Defence and Security Studies, November 2019.

Welch, Michael. ‘The Science of War: A Discussion of J. F. C. Fuller’s Shattering of British Continuity’. *Journal of the Society for Army Historical Research* 79, no. 320 (Winter 2001): 320–334.

Werner, Ben. ‘VIDEO: Houthi Forces Capture U.S. Navy Unmanned Underwater Vehicle Off Yemen’. *USNI News*, 3 January 2018. https://news.usni.org/2018/01/03/houthi-rebels-find-likely-u-s-navy-unmanned-underwater-vehicle.

Wesley, Eric J. and Robert H. Simpson. *Expanding the Battlefield: An Important Fundamental of Multi-Domain Operations*. Land Warfare Paper 131. Arlington: Association of the United States Army, April 2020.

Westwood, Chris. *5th Generation Air Battle Management*. Canberra: Air Power Development Centre, 2020.

Williamson, William. ‘From Battleship to Chess’. *USNI Proceedings*, 146/7/1,409, July 2020. https://www.usni.org/magazines/proceedings/2020/july/battleship-chess.

Work, Robert O., Chris Dougherty and Paul Scharre. ‘Transcript from a Virtual Panel Discussion on Emerging Concepts in Joint Command and Control’. *Center for a New American Security*, Last updated 20 May 2020. https://www.cnas.org/publications/transcript/transcript-from-emerging-concepts-in-joint-command-and-control.

Work, Robert O., Paul Scharre, Martijn Rasser, Megan Lamberth, Ainikki Riikonen, Dr Lynne Parker and Olivia Zetter. ‘Transcript from U.S. AI Strategy Event: “The American AI Century: A Blueprint for Action” ’. *Center for a New American Security*. Last modified 17 January 2020. https://www.cnas.org/publications/transcript/american-ai-century.

Yeadon, Steven A. ‘A New Combined-Arms Approach for the Armored Brigade Combat Team’. *Armour: Mounted Maneuver Journal* CXXXIII, no.3, (Summer 2020): 14–21.

Joint Studies Paper Series

About the series

Over the last three decades, each of the three Australian Services has established a centre of excellence to conduct academic research and development in relation to their core functions. These centres have made excellent contributions to the literature on military activities in the maritime, land, air and space domains. To date, however, the Australian Defence Force (ADF) has had no equivalent outlet for academic research and development relating to the conduct of joint military activities.

The Joint Studies Paper Series will help to fill this gap. A collaborative venture between Australian Defence Force Headquarters, Defence Science and Technology Group and the Australian Defence College, the series will help to shape future joint best practice within the ADF through the promulgation of research about the past, present and future of joint military activities.

Papers in the series are available in hard copy and online. They can be downloaded free of charge from: http://www.defence.gov.au/ADC/publications/Joint_Studies.asp.

Papers in the series

No. 1 **Australia's Joint Approach: Past, Present and Future**
Tim McKenna and Tim McKay

No. 2 **The Four Aspects of Joint: A Model for Comparatively Evaluating Jointness within Armed Forces**
Aaron P. Jackson

No. 3 **Design Thinking: Applications for the Australian Defence Force**
Aaron P. Jackson (ed.)

No. 4 **Fighting Artificial Intelligence Battles: Operational Concepts for Future AI-Enabled Wars**
Peter Layton

Call for submissions

The Joint Studies Paper Series welcomes unsolicited submissions on a range of topics related to joint military activities. Ideally, papers should be linked to the Australian experience of joint military activities or should contain information that will be of interest to the ADF; however, papers examining other joint topics may be considered depending on their focus and content. For example, papers exploring topics in the following areas will be of particular interest to the series:

- joint force design and experimentation
- joint capability development, management and integration
- fundamental inputs to capability
- joint professional military education and training
- joint doctrine, theory and concepts (including future concepts)
- joint and organisational culture (including cultural change management)
- joint planning, design thinking and evaluation
- historical aspects of the joint military concept.

Papers submitted for consideration should be longer than a journal article but shorter than a book – between 10,000 and 70,000 words (inclusive of notes) is ideal. References should be included in Notes and Bibliography form and individual citations should be formatted in accordance with the Chicago Manual of Style. For further style guidance, please see the Australian Government Style Manual at https://www.stylemanual.gov.au.

Potential contributors are strongly encouraged to contact the editor to discuss their paper idea prior to submission of the paper itself. The editor can be contacted at: cdr.publications@defence.gov.au.

In recent years, militaries around the world have recognised the need to rapidly increase investments in artificial intelligence (AI) technologies and examine the potential ways it may be employed in future warfighting. Over time, AI will likely infuse most military equipment and enable the battlespace. Yet, there is still much to be determined in terms of the application and management of AI as a military capability.

AI machine learning has enormous potential for enhancing efficiency, quickly identifying patterns and detecting items within very large data troves. But, AI also has known weaknesses and lacks robustness and, to be effective, it must still be carefully teamed with humans.

In this paper, Dr Peter Layton considers these issues and proposes operational level defensive and offensive concepts for an AI-enabled battlespace. He then explores how these concepts may be applied to the traditional sea, land and air domains. The intent is to stimulate discussion and new ways of thinking about how AI may be employed in the future and how to begin preparing for that future now.

__Dr Peter Layton__ is a Visiting Fellow at the Griffith Asia Institute, Griffith University, a Royal United Services Institute Associate Fellow and a RAAF Reserve Group Captain.

DPS:DEC020-20