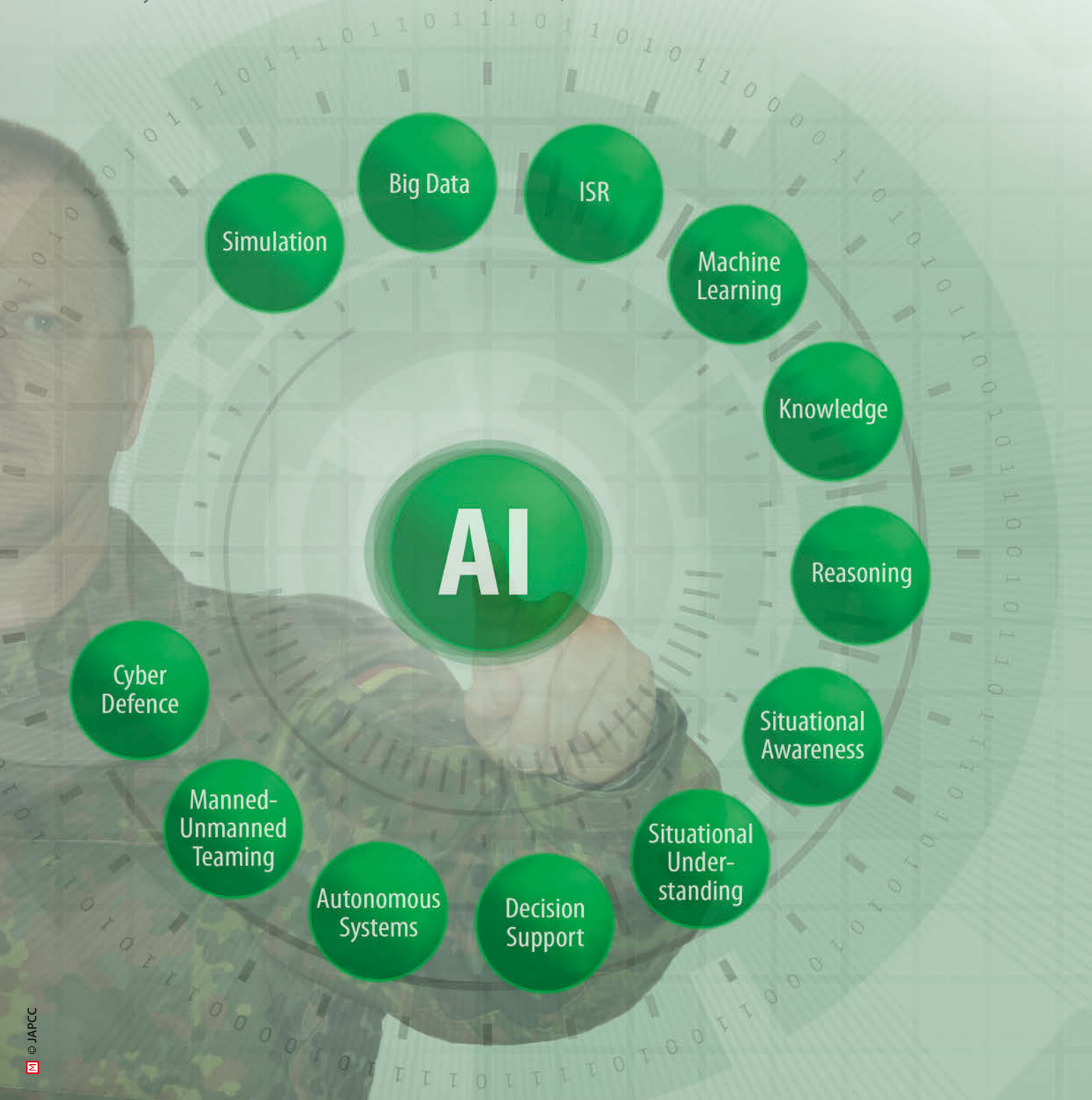


The Future Role of Artificial Intelligence

Military Opportunities and Challenges

By Andy J. Fawkes, Consultant Thinke Company Ltd

By Lieutenant Colonel Martin Menzel, DEU A, JAPCC



Introduction

Artificial Intelligence (AI) today is one of the hottest buzzwords in business and industry, and it has military applications, too. In fact, industry has developed AI as a technology over the last 60 years, and periodically it becomes mainstream news. Progress has not always been smooth, particularly in the 20th century when funding for AI research was principally public sector, primarily aimed at academic research and the military. Enthusiasm waxed and waned, as AI did not consistently deliver the desired level of capability.

However, in the 21st century we have seen industries outside the defence sector, such as large Internet providers and companies in the automotive field, make significant contributions to AI development. These developments are of significant interest as they may provide answers how to further improve unmanned systems' autonomy, and improve our ability to process vast amounts of information and data better within military command and control (C2) systems.

The purpose of this article is to provide a basic understanding of AI, its current development, and the realistic progress that can be expected for military applications, with examples related to air power, cyber, C2, training, and human-machine teaming. While legal and ethical concerns about the use of AI cannot be ignored, their details cannot be discussed here because this essay is focused on technological achievements and future concepts. However, the authors will address the question of reliability and trust that responsible commanders need to ask about such AI applications.

Artificial Intelligence – What it is and What it is Not

The concept of what defines AI has changed over time. In essence, there has always been the view that AI is intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans and other animals. In common language, the term AI is applied when a machine mimics cognitive functions attributed to human minds, such as learning and problem-solving. There are many different AI methods

used by researchers, companies, and governments, with machine learning and neural networks currently at the forefront.

As computers and advanced algorithms become increasingly capable, tasks originally considered as requiring AI are often removed from the list since the involved computer programs are not showing intelligence, but working off a predetermined and limited set of responses to a predetermined and finite set of inputs. They are not 'learning'. As of 2018, capabilities generally classified as AI include successfully understanding human speech, competing at the highest level in strategic game systems (such as Chess and Go), autonomous systems, intelligent routing in content delivery networks, and military simulations. Furthermore, industry and academia generally acknowledge significant advances in image recognition as cutting-edge technology in AI.

While such known and 'applied AI' systems are often quite powerful, it should be noted they are usually highly specialized and rigid. They use software tools limited to learning, reasoning, and problem-solving within a specific context, and are not able to adapt dynamically to novel situations. This leads to the term 'weak AI' or 'narrow AI'. Weak AI, in contrast to 'strong AI', does not attempt to perform the full range of human cognitive abilities. By contrast, strong AI or 'general AI' is the intelligence of a machine that could successfully perform any intellectual task that a human being can. In the philosophy of strong AI, there is no essential difference between the piece of software, which is the AI exactly emulating the actions of the human brain, and actions of a human being, including its power of understanding and even its consciousness.¹ In scholarly circles, however, the majority believes we are still decades away from successfully developing such a 'general AI' capability.

Military Simulation for Training and Exercise

A number of 'narrow AI' applications began to appear in the late 1970s/80s, including some for military simulation systems. For example, the US Defense

Advanced Research Projects Agency (DARPA) funded a prototype research program named Simulator Networking (SIMNET) to investigate the feasibility of creating a cost-efficient, real-time, and distributed combat simulator for armoured vehicles operators.² By 1988, a Semi-Automated Forces (SAF) or Computer-Generated Forces (CGF) capability was available to support more complex and realistic exercise scenarios with simulated flanking and supporting units that could be managed with little human resource requirement.

Meanwhile, various nations and companies developed their own SAF/CGF or constructive simulations³, the majority of which are broadly interoperable and can be connected to other Live, Virtual, and Constructive (LVC) simulation environments. NATO air power, for example, is capitalizing on such capabilities with Mission Training through Distributed Simulation (MTDS), which has demonstrated reliable connectivity and beneficial training opportunities between multiple types of aircrew simulators and training centres.⁴ In addition, since 2001, the Command & Control – Simulation Interoperation (C2SIM) data exchange standard offers existing command & control, communication, computers and intelligence (C4I) systems the potential to switch between interacting with real units and systems, including robotics and autonomous systems, and simulated forces and systems.⁵

From Remote-Controlled to Autonomous Physical Systems

Unmanned vehicle research has allowed state-of-the-art remote operations to progress significantly during recent decades, for both civil and military applications. The advance of AI, however, is now offering unprecedented opportunities to go beyond remote control and build autonomous systems demanding far less direct control by human operators. Examples of autonomous systems development include self-driving cars, trains, and delivery systems in the civil traffic and transport sector.

In the same way, the military is developing systems to conduct routine vehicle operations autonomously. For example, by 2014, the US Navy X-47B program

developed an Unmanned Combat Air Vehicle (UCAV) that had completed a significant number of aircraft carrier catapult launches, arrestments, and touch-and-go landings, with only human supervision. In April 2015, the X-47B successfully conducted the world's first fully autonomous aerial refuelling.

The conduct of combat operations by autonomous systems, though, is greatly complicated by diverse legal and ethical issues that are far too complex to discuss in detail within this essay. Moreover, military commanders need to ask themselves how much trust they want to place in what the AI-enabled autonomous system promises to be able to do. How much better is it with regard to persistence, precision, safety, and reliability, as compared to the remote human operator? When it comes to kinetic targeting on the ground, the 'human-in-the-loop' being able to intervene at any time probably should remain a requirement.

Conversely, in the field of air-to-air combat, where millisecond long timeframes for critical decisions inhibit remote UCAV operations, there has been a recent and promising leap forward. In 2016, an alternate approach funded by the US Air Force Research Laboratory (AFRL) led to the creation of 'ALPHA', an AI agent built on high-performing and efficient 'Genetic Fuzzy Trees'.⁶ During in-flight simulator tests it has constantly beaten an experienced combat pilot in a variety of air-to-air combat scenarios, which is something that previous AI-supported combat simulators never achieved.⁷ While currently a simulation tool, further development of ALPHA is aimed towards increasing physical autonomous capabilities. For example, this may allow mixed combat teams of manned and unmanned fighter airframes to operate in highly contested environments⁸, as further described below.

Human-Machine Teaming

A variation on the autonomous physical system and military operations with human-controlled vehicles is the manned-unmanned teaming (MUM-T) concept, which leaders deem to be a critical capability for future military operations in all domains. Some nations are currently testing and implementing diverse

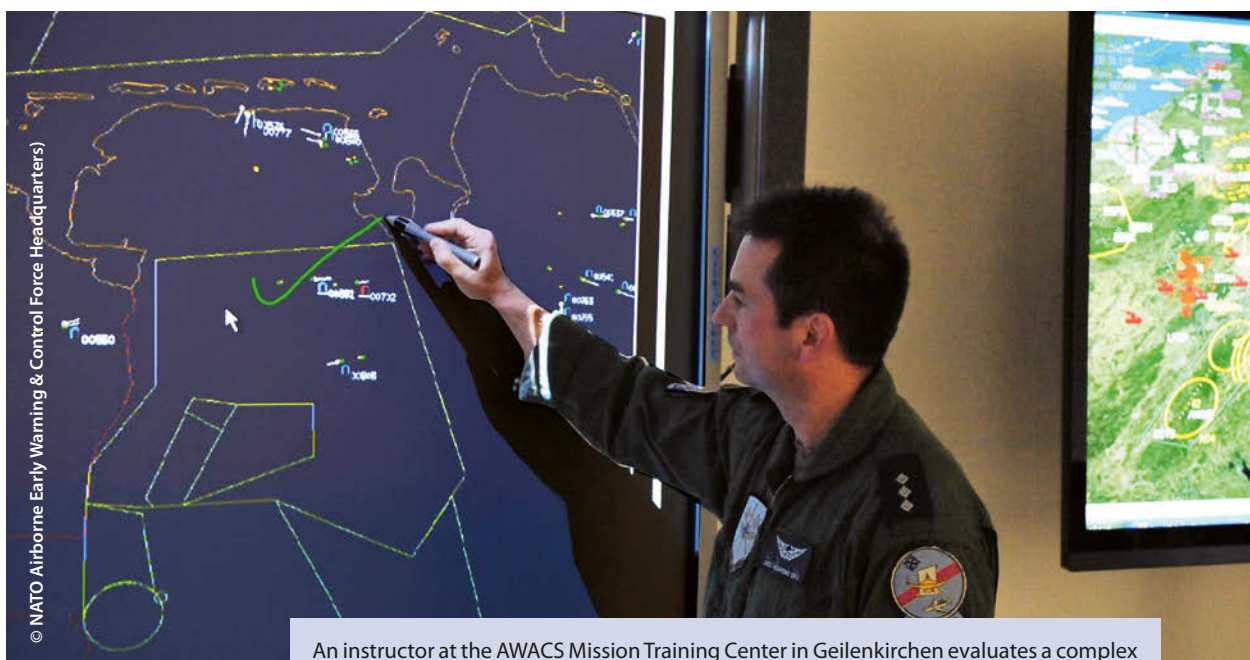
configurations to improve the following: pilots' safety, situational awareness, decision-making, and mission effectiveness in military aviation. The US Army has been conducting MUM-T for some time – most notably involving Apache helicopter pilots controlling unmanned MQ-1C Grey Eagles – and the Army will assign a broader role to MUM-T in the further development of its multi-domain battle concept.⁹

The US AFRL has been working on the *'Loyal Wingman'* model, where a manned command aircraft pairs with an unmanned off-board aircraft serving as a wingman or scout. In a 2015 live demonstration, a modified unmanned F-16 was paired with a manned F-16 in formation flight. In a 2017 experiment, the pilotless F-16 broke off from the formation, attacked simulated targets on the ground, modified its flight pattern in response to mock threats and other changing environmental conditions, and re-entered formation with the manned aircraft.¹⁰ USAF planning foresees future applications pairing a manned F-35 Joint Strike Fighter with such an unmanned wingman.

In the above test scenario, however, the unmanned F-16 conducted only semi-autonomous operations based on a set of predetermined parameters, rather than doing much thinking for itself. The next technology

waypoint with a more demanding AI requirement would be *'Flocking'*. This is distinct from the *'Loyal Wingman'* concept in that a discernible number of unmanned aircraft in a flock (typically consisting of a half-dozen to two dozen aircraft) execute more abstract commander's intent, while the command aircraft no longer exercises direct control over single aircraft in the flock. However, the command aircraft can still identify discrete elements of the formation and command discrete effects from the individual asset. A futuristic video published by AFRL in March 2018 shows an F-35A working together with six stealth UCAVs. The AFRL has also released an artist's concept of the XQ-58A *'Valkyrie'* (formerly known as the XQ-222), a multi-purpose unmanned aircraft that team members are currently developing for a project called Low Cost Attritable Aircraft Technology (LCAAT).¹¹

The third waypoint, *'Swarming'*, exceeds the complexity of flocking, so that an operator cannot know the position or individual actions of any discrete swarm element, and must command the swarm in the aggregate. In turn, the swarm elements will complete the bulk of the combat work. For example, in October 2016, the US Department of Defense demonstrated a swarm of 103 *'Perdix'* autonomous micro-drones ejected from a fighter aircraft.¹² The swarm successfully showed



An instructor at the AWACS Mission Training Center in Geilenkirchen evaluates a complex scenario provided within Mission Training through Distributed Simulation (MTDS).



© US Navy, MC2 Timothy Walter

A US Navy X-47B stealth autonomous aircraft exercises touch and go landings on the aircraft carrier George H. W. Bush.

collective decision-making, adaptive formation flying, and self-healing abilities. While not primarily an offensive tool, there are a multitude of uses for such drone swarms, including reconnaissance and surveillance, locating and pursuing targets, or conducting electronic warfare measures. Furthermore the swarm could act as expendable decoys to spoof enemy air defences by pretending to be much larger targets.¹³

Evolution in Cyber and Information Operations

The application of AI and automation to cyber systems is the most immediate arena for evolution and advantage. The cyber domain's intrinsically codified nature, the volume of data, and the ability to connect the most powerful hardware and algorithms with few constraints creates an environment where AI can rapidly evolve, and AI agents could quickly optimize to their assigned tasks. With the growing capabilities in machine learning and AI, 'hunting for weaknesses' will be automated, and critically, it will occur faster than human-controlled defences can respond.

However, AI approaches alone have thus far failed to deliver significant improvements in cybersecurity. While the industry successfully applies deep neural

networks and automated anomaly detection to find malware or suspicious behaviour, core security operator jobs such as monitoring, triage, scoping, and remediation, remain highly manual. Humans have the intuition to find a new attack technique and the creativity to investigate it, while machines are better at gathering and presenting information.

AI Support to C2 and Decision-Making

Military headquarters have largely moved from paper-based to electronic-based workflows. This, in-turn, adds information awareness but also data volume which the staff must manage. Future intelligence, surveillance, target acquisition and reconnaissance systems will generate even larger amounts of (near) real-time data that will be virtually impossible to process without automated support. At the same time, increasingly advanced, network-enabled, joint, and multi-domain capabilities will emerge, and a nation or coalition of nations will have these tools available for use in their own operations. For commanders to effectively orchestrate actions in such environments, they need situational understanding and decision-support on possible courses of action (COAs), their effects, and consequences. Improved data management and interoperability, data fusion, automated analysis support, and visualization



Artist rendering of some XQ-58A 'Valkyrie' autonomous systems, which are low-cost attritable aircraft designed to function as flock wingmen to manned aircraft in contested airspace.

technologies will all be essential to achieving manageable cognitive loads and enhanced decision-making. These critical capabilities are not only for commanders and headquarters staffs, but also for platform operators, dismounted combatants and support staff.¹⁴

Aside from traditional algorithms, simulation and AI are envisaged as tools that can enhance decision-making. However, related research and development are still in their infancy. Only recently, in 2017, the NATO Science and Technology Organization made *'Military Decision Making using the tools of Big Data and AI'* one of its principal themes. Following a call for papers, the organization collected many academic and expert views. To better define the task, some of these inputs started by breaking down John Boyd's well-known Observe-Orient-Decide-Act (OODA) loop – an abstract model generically embracing different types of military decision-making processes – and then assigned future required AI roles and functions to each of the OODA steps.¹⁵

Observe (sensing). Harvest data from a broad array of sensors, including social media analysis and other forms of structured and unstructured data collection, then verify the data and fuse it into a unified view. This requires a robust, interoperable, IT infrastructure capable of rapidly handling large amounts of data and multiple security levels.

Orient (situational understanding). Apply big data analytics and algorithms for data processing, then data presentation for timely abstraction and reasoning based on a condensed, unified view digestible by humans, but rich enough to provide the required level of detail. This should include graphical displays of the situation, resources (timelines, capabilities, and relations and dependencies of activities), and context (point of action and effects).

Decide (plan generation). Present a timely, condensed view of the situation, with probable adversary COAs and recommended own COAs including advice on potential consequences to support decision-making. To this end, it must be made possible to assess and validate the reliability of the AI to ensure predictable and explainable outcomes allowing the human to properly trust the system.

Act. As AI gets more advanced and/or time pressure increases, the human may only be requested to approve a pre-programmed action, or systems will take fully autonomous decisions. Requirements for such AI must be stringent, not only because unwanted, erroneous decisions should be prevented, but also because the human will generally be legally and ethically responsible for the actions the system takes.

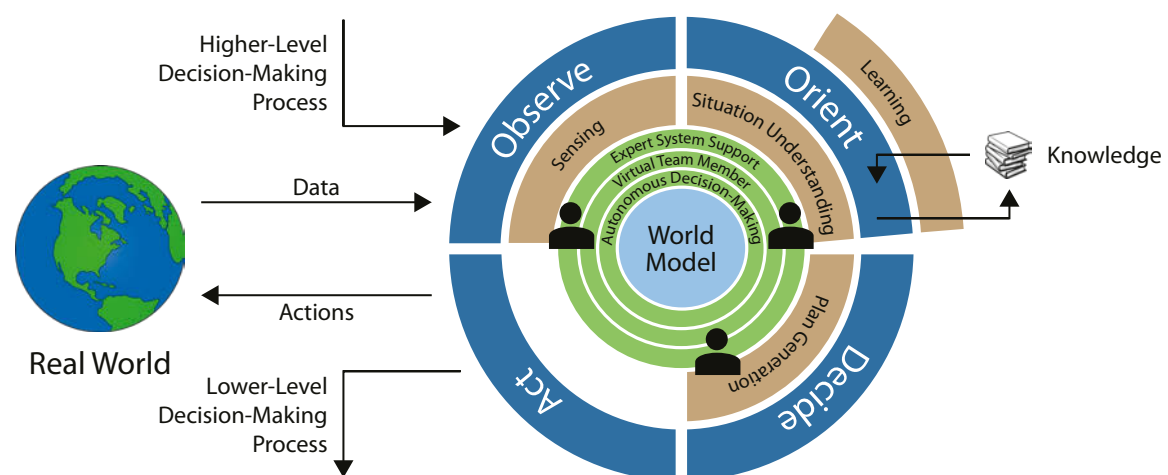


Figure 1: A system view of the OODA decision-making cycle supported by AI.

(Source: NATO Science & Technology Organization STO-MP-IST-160, graphic rebuilt at JAPCC.)

Summary and Conclusion

New AI technologies not only have potential benefits, but also shortcomings and risks that need to be assessed and mitigated as necessary. The very nature of AI – a machine that determines the best action to take and then pursues it – could make it hard to predict its behaviour. Specific character traits of narrow AI systems mean they are trained for particular tasks, whether this is playing chess or interpreting images. In warfare, however, the environment shifts rapidly due to the ‘fog and friction of war’. AI systems have to work in a context that is highly unstructured and unpredictable, and with opponents that deliberately try to disrupt or deceive them. If the setting for the application of a given AI system changes, then the AI system may be unable to adapt, thus the risk of non-reliance is increased. In context, militaries need to operate on the basis of reliability and trust. So, if human operators, whether in a static headquarters or battlefield command post, are not aware what AI will do in a given situation, it could complicate planning as well as make operations more difficult, and accidents more likely.¹⁶

The increasing array of capabilities of AI systems will not be limited by what can be done, but by what actors trust their machines to do. The more capable our

AI systems are, the greater their ability to conduct local processing and respond to more abstract, higher level commands. The more we trust the AI, the lower the level of digital connectivity demanded to maintain system control. Within this context it will be critical to develop the appropriate standards, robust assurance, certification regimes, and the effective mechanisms to demonstrate meaningful human accountability.¹⁷

That being said, there are important requirements for military AI applications that may render civilian technologies unsuitable or demand changes in implementation. In addition, further ethical and legal issues will often play an important role. Hence, defence organizations will have to make difficult choices. On the one hand, they must benefit from the rapid civil developments, while on the other hand, choose wisely where to invest to make sure that applications will be fit for military use.¹⁸

AI technology has become a crucial linchpin of the digital transformation taking place as organizations position themselves to capitalize on the ever-growing amount of data that is being generated and collected. Technology for big data and AI is currently developing at a tremendous pace, and it has major potential impacts for strategic, operational and tactical military

decision-making processes. As such, operational benefits may be vast and diverse for both the Alliance and its adversaries. However, the full potential of AI-enhanced technology cannot yet be foreseen, and time is required for capabilities to mature. ●

1. Techopedia. 'Strong Artificial Intelligence'. Online at: <https://www.techopedia.com/definition/31622/strong-artificial-intelligence-strong-ai>, accessed 26 Aug. 2018.
2. Duncan C. Miller. 'SIMNET and Beyond: A History of the Development of Distributed Simulation'.
3. Constructive simulations: these involve simulated people in simulated scenarios operating simulated equipment.
4. Jay Vizcarra. 'Preserving NATO's C2 Edge'. In Journal of the JAPCC, Edition 24. Spring/Summer 2017, p. 34–39.
5. Scott A. Carey, Martin S. Kleiner, Michael R. Hieb, Ph.D., Richard Brown. 'Standardizing Battle Management Language – A Vital Move Towards the Army Transformation'. SISO 2001 Scott A. Carey, Martin S. Kleiner, Michael R. Hieb, Ph.D., Richard Brown. 'Standardizing Battle Management Language – A Vital Move Towards the Army Transformation'. SISO 2001.
6. Fuzzy logic is a form of many-valued logic in which the truth values of variables may be between 0 (false) and 1 (true), thus featuring mechanisms to deal with imprecision and uncertainties. Current advanced fuzzy logic is able to handle many inputs with relatively low processing demands.
7. Genetic Fuzzy based Artificial Intelligence for Unmanned Combat Aerial Vehicle Control in Simulated Air Combat Missions; Journal of Defense Management; Psibernetix Inc.; Air Force Research Laboratory, USA; University of Cincinnati; 2016.

8. See Nicolas Ernest et al, 'Genetic Fuzzy based Artificial Intelligence for Unmanned Combat Aerial Vehicle Control in Simulated Air Combat Missions'. Journal of Defense Management, 2016 6.1. DOI: 10.4172/2167-0374.1000144.
9. C4ISRNET. 'Army's Multi-domain Battle Brings Manned-Unmanned Teaming to the Fore'. 31 Aug. 2017. Online at: <https://www.c4isrnet.com/unmanned/uas/2017/08/31/armys-multidomain-battle-brings-manned-unmanned-teaming-to-the-fore/>, accessed 25 Jun. 2018.
10. The Drive. 'This is What the US Air Force Wants You To Think Air Combat Will Look Like in 2030'. 23 Mar. 2018. Online at: <http://www.thedrive.com/the-war-zone/19636/this-is-what-the-us-air-force-wants-you-to-think-air-combat-will-look-like-in-2030>, accessed 11 Jul. 2018.
11. War on the Rocks. 'Loyal Wingman, Flocking, and Swarming: New Models of Distributed Airpower'. 21 Feb. 2018. Online at: <https://warontherocks.com/2018/02/loyal-wingman-flocking-swarming-new-models-distributed-airpower/>, accessed 25 Jun. 2018.
12. The Perdix have a length of 16,5 cm, a wingspan of 30 cm, weight 290 g, and can fly at maximum speed of 113 kph, with the endurance of 20 minutes.
13. Kyle Mizikamo. 'The Pentagon's Autonomous Swarming Drones Are the Most Unsettling Thing You'll See Today'. Popular Mechanics. 9 Jan. 2017. Online at: <https://www.popularmechanics.com/military/aviation/a24675/pentagon-autonomous-swarming-drones/>, accessed 17 Jul. 2018.
14. UK Ministry of Defence. 'Joint Concept Note 1/18 – Human-Machine Teaming'. May 2018. Online at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/709359/20180517-concepts_uk_human_machine_teaming_jcn_1_18.pdf
15. NATO STO. 'Big Data and Artificial Intelligence for Decision Making: Dutch Position Paper'. MP-IST-160-PP-1. 25 May 2018, p. 6.
16. Michael C. Horowitz. 'The Promise and Peril of Military Applications of Artificial Intelligence'. 23 Apr. 2018. Online at: <https://thebulletin.org/military-applications-artificial-intelligence/promise-and-peril-military-applications-artificial-intelligence>, accessed 27 Jun. 2018.
17. Ibid. 14.
18. NATO STO. 'Big Data and Artificial Intelligence for Decision Making: Dutch Position Paper'. MP-IST-160-PP-1. 25 May 2018, p. 2.



Andy J. Fawkes MSc MBA

began his career in 1979 in the UK Royal Corps of Naval Constructors, and after his training he worked on number of submarine projects and taught nuclear systems at the Royal Naval College Greenwich. Following several central MoD policy posts including HR and in the central MoD science staff he moved into the field of training and simulation in 2000. Since then he has held a number of positions including the MoD simulation policy lead, joint training systems sponsor, and the UK representative on the NATO Modelling and Simulation Group (NMSG) for 12 years, including 2 years as the Group Chair. On leaving MoD in 2012 he has been an independent consultant and regular public speaker on simulation and technology. He also provides consultancy support to Bohemia Interactive Simulations, a global provider of training simulation software and Ocean Software, which provides military air training and operations management software.



Lieutenant Colonel MBA Martin Menzel

began his military carrier in 1985, spending several years in the German Army Engineer branch, including positions as Company Commander and as Chief Instructor at the German Army NCO School. In 1999, he stepped over into the Military Intelligence branch. With a broad range of intelligence positions and functions held at Headquarters 1st German/Netherlands Corps, Joint Force Command Brunssum, SFOR, and ISAF, he became a highly experienced staff officer with regard to the conduct of military intelligence at the operational level in NATO or multi-national staff environments. From May 2014 to September 2018, Lieutenant Colonel Menzel served as the JAPCC's Subject Matter Expert for Research, Analysis and Intelligence Support, and he also was the Assistant Editor of this journal.