

Chapter 6

The AI Wave in Military Affairs: Enablers and Constraints

Michael Raska

In the 2020s, debates in strategic studies increasingly focus on the impact of emerging technologies on defense innovation and future character of warfare. The convergence of advanced novel technologies such as artificial intelligence (AI) systems, robotics, additive manufacturing (or 3D printing), quantum computing, directed energy, and other ‘disruptive’ technologies, defined under the commercial umbrella of the 4th Industrial Revolution (4IR), promises new and potentially significant opportunities for defense applications and, in turn, for increasing one’s military edge over potential rivals. Much of the current debate arguably portrays the “next-frontier” technologies as synonymous with a “discontinuous” or “disruptive” military innovation in the character and conduct of warfare - from the “industrial-age” toward “information-age warfare” and now increasingly toward “automation-age warfare” (Raska, 2021). For example, advanced sensor technologies such as hyperspectral imagery, computational photography, and compact sensor design aim to improve target detection, recognition, and tracking capabilities and overcome traditional line-of-sight interference (Freitas et al., 2018). Advanced materials such as composites, ceramics, and nanomaterials with adaptive properties will make military equipment lighter but more resistant to the environment (Burnett et al., 2018). Emerging photonics technologies, including high-power lasers and optoelectronic devices, may provide new levels of secure communications based on quantum computing and quantum cryptography (IISS, 2019).

The convergence of emerging technologies – i.e. robotics, artificial intelligence and learning machines, modular platforms with advanced sensor technologies, novel materials and protective systems, cyber defenses and technologies that blur the lines between the physical, cyber, and biological domains, is widely seen as having profound implications on the character of future warfare. For modern militaries, the application of novel machine-learning algorithms to diverse problems also promises to provide unprecedented capabilities in terms of speed of information processing, automation for a mix of manned/unmanned weapons platforms and surveillance systems, and ultimately, command and control (C2) decision-making (Horowitz, 2018; Cummings, 2017).

Notwithstanding the varying strategic contexts, however, the diffusion of these

emerging technologies is also prompting theoretical and policy-prescriptive questions similar to those posed over the past four decades: Does the diffusion of emerging technologies really signify a ‘disruptive’ shift in warfare, or is it a mere evolutionary change? If emerging technologies stipulate a disruptive change in warfare, what are defense resource allocation imperatives, including force structure and weapons procurement requirements? How can military organizations, including air forces, exploit emerging technologies to their advantage? Furthermore, how effective are emerging technologies to counter security threats and challenges of the 21st century, characterized by volatility, uncertainty, complexity, and ambiguity?

Four Decades of Disruptive Narratives

Driven largely by the quantum leaps in information technologies, the trajectory of ‘disruptive’ military innovation narratives and debates have been defined in the context of IT-driven Revolution in Military Affairs (IT-RMA), which have progressed through at least five stages: (1) the initial conceptual discovery of the Military-Technical Revolution by Soviet strategic thinkers in the early 1980s, (2) the conceptual adaptation, modification, and integration in the US strategic thought during the early 1990s, (3) the technophilic RMA debate during the mid-to-late 1990s, (4) a shift to the broader “defense transformation” and its partial empirical investigation in the early 2000s, and (5) critical reversal questioning the disruptive narrative from 2005 onwards (Gray, 2006). Since the mid-2010s, however, with the accelerating diffusion of novel technologies such as AI and autonomous systems, one could argue that a new AI-RMA – or the sixth RMA wave - has emerged (Raska, 2021).

In retrospect, however, the implementation of IT-RMA over the past four decades has also arguably followed a distinctly less than revolutionary or disruptive path, consisting of incremental, often near-continuous, improvements in existing capabilities (Ross, 2010). While major, large-scale, and simultaneous military innovation in defense technologies, organizations, and doctrines have been a rare phenomenon, military organizations have largely progressed through a *sustained* spectrum of military innovations ranging from small-scale to large-scale innovation that shaped their conduct of warfare (Goldman, 1999). While many military innovations during this era, such as concepts of Network-Centric Warfare, have matured, the ambitious narratives of impending ‘disruptive military transformation’ have nearly always surpassed available technological, organizational, and budgetary capabilities. Moreover, the varying conceptual, technological, organizational,

and operational innovations focused primarily on integrating digital information technologies into *existing* conventional platforms and systems (Raska, 2016).

For example, in the US strategic thought, the narratives of disruptive military innovation have gradually waned from 2005 onwards with operational challenges and experiences in wars in Iraq and Afghanistan. More critical voices pointed toward unfulfilled promises of ‘disruptive’ defense transformations. The rationale for ‘new way of thinking and a new way of fighting’ justifying virtually every defense initiative or proposal, signaled disorientation rather than a clear strategy (Freedman, 2006). Defense transformation sceptics also cautioned about the flawed logic in solving complex strategic challenges through technology, while discarding the adaptive capacity of potential enemies or rivals. In short, disruptive narratives of impending defense transformations have turned into an ambiguous idea, propelled by the budgetary requirements and unrealistic capability sets rather than actual strategic and operational logic (Reynolds, 2006).

Why the AI-Wave Differs?

The new ‘AI-enabled’ defense innovation wave, however, differs from the past IT-led waves in several ways. First, the diffusion of AI-enabled military innovation proceeds at a much faster pace, through multiple dimensions, notably through the accelerating geostrategic competition between great powers - the United States, China, and to a lesser degree Russia. Strategic competitions between great powers are not new; they have been deeply rooted in history – from the Athenian and Spartan grand strategies during the Peloponnesian War in the fifth century BCE, to the bipolar divide of the Cold War during the second half of the twentieth century. The character of the emerging strategic competition, however, differs from analogies of previous strategic competitions. In the 21st century, the paths and patterns of strategic competitions are more complex and diverse, reflecting multiple competitions under different or overlapping sets of rules in which long-term economic interdependencies co-exist with core strategic challenges (Lee, 2017). In a contest over future supremacy, however, technological innovation is portrayed as a central source of international influence and national power - generating economic competitiveness, political legitimacy, and military power (Mahnken, 2012). Specifically, for the first time in decades, the US faces a strategic peer competitor, China, capable of pursuing and implementing its own AI-RMA. Accordingly, the main question is not whether the AI-RMA wave is ‘the one’ that will bring about a fundamental

discontinuity in warfare, and if so, how and why? Instead, it is whether the US AI-RMA can be nullified – or at least weakened – by corresponding Chinese or Russian AI-RMAs? In other words, the margins of technological superiority are effectively narrowing, which effectively accelerates the strategic necessity for novel technologies as a source of military advantage.

Second, contrary to previous decades, which, admittedly, utilized *some* dual-use technologies to develop major weapons platforms and systems, the current AI-enabled wave differs in the magnitude and impact of the commercial-technological innovation as the source of military innovation (Raska, 2020). Large military-industrial primes are no longer the only drivers of technological innovation; instead, advanced technologies with a dual-use potential are being developed in the commercial sectors and then being ‘spun on’ to military applications. In this context, the diffusion of emerging technologies, including additive manufacturing (3D printing), nanotechnology, space and space-like capabilities, artificial intelligence, and drones, are not confined solely to the great powers (Hammes, 2016). The diffusion of AI-enabled sensors and autonomous weapon systems is also reflected in defense trajectories of select advanced small states and middle powers such as Singapore, South Korea, Israel, and others. These have now the potential to develop niche emerging technologies to advance their defense capabilities and their economic competitiveness, political influence, and status in the international arena (Barsade and Horowitz, 2018).

Third, the diffusion of autonomous and AI-enabled autonomous weapons systems, coupled with novel operational constructs and force structures, challenge the direction and character of human involvement in future warfare – in which algorithms may shape human decision-making, and future combat is envisioned in the use of Lethal Autonomous Weapons Systems (LAWS). Advanced militaries, including air forces, are experimenting with varying man-machine technologies that rely on data analytics and automation in warfare. These technologies are increasingly permeating future warfare experimentation and capability development programs (Jensen and Pashkewitz, 2019). In the US, for example, select priority research and development areas focus on the development of AI-systems and autonomous weapons in various human-machine type collaborations – i.e. AI-enabled early warning systems and command and control networks, space and electronic warfare systems, cyber capabilities, lethal autonomous weapons systems, and others.

The convergence of the three drivers - strategic competition, dual-use emerging technological innovation, and changing character of human-machine interactions

in warfare propel a new set of conditions that define the AI-RMA wave. Its diffusion trajectory inherently also poses new challenges and questions concerning strategic stability, alliance relationships, arms control, ethics and governance, and ultimately, the conduct of combat operations (Stanley-Lockman, 2021a). International normative debates on the role of AI systems in the use of force, for example, increasingly focus on the diffusion of LAWS and the ability of states to conform to principles of international humanitarian law. As technological advancements move from the realm of science fiction to technical realities, states also have different views on whether the introduction of LAWS would defy or reinforce international legal principles. Facing contending legal and ethical implications of military AI applications, military establishments increasingly recognize the need to address questions related to safety, ethics, and governance, which are crucial to building trust in new capabilities, managing risk escalation, and revitalizing arms control. Still, there is a tension between how much defense ministries and militaries focus their ethics efforts narrowly on LAWS or more broadly on the gamut of AI-enabled systems. Hence, military organizations need to track the evolving perspectives on AI and autonomy and debates on implications to the strategic and operational environment of the 2020s and beyond (Stanley-Lockman, 2021b).

Application of the AI Wave in Airpower

At the operational level, for example, the application of AI-wave can be seen in changing conceptions of airpower. Modern air forces aim to accelerate the integration of varying AI-related systems and technologies such as multi-domain combat cloud systems, which collect big-data from a variety of sources, creating a real-time operational picture, and essentially, automate and accelerate command and control (C2) processes (Robinson, 2021). For example, AI-enabled combat clouds are posed to identify targets and allocate them to the most relevant “shooters” in any domain, whether airborne, surface or underwater – which some air forces conceptualize as Joint All-Domain Command and Control (JADC2). Select air forces such are also experimenting with AI algorithms as ‘virtual backseaters’, which effectively control the aircraft’s sensors and navigation, finding adversary targets, and in doing so, reduce the aircrew’s workload (Everstine, 2020).

In this context, the key argument is that advances in AI systems – broadly programs that can sense, reason, act, and adapt, including Machine Learning (ML) systems - algorithms whose performance improves with increasing data interactions over time, and Deep Learning (DL) systems - in which multilayered neural networks learn from vast

amounts of data – have the potential “to transform air combat operations and the way airpower is conceived and used” (Davis, 2021). According to a RAND study (Lingel et al., 2020), there are currently six categories of applied AI/ML research and development that have implications for future warfare, including airpower:

- (1) Computer vision - image recognition - detecting and classifying objects in the visual world that could be used to process multisource intelligence and data fusion;
- (2) Natural language processing (NLP) - ability to successfully understand human speech and text recognition patterns, including translation, that could be used to extract intelligence from speech and text, but also monitor friendly communications and direct relevant information to alert individuals or units in need;
- (3) Expert systems or rule-based systems - collecting large amounts of data to recommend particular actions to achieve operational and tactical objectives;
- (4) Planning systems - using data to solve scheduling and resource allocation problems, which could coordinate select air, space, and cyber assets against targets and to generate recommended time-phased actions;
- (5) Machine learning systems - acquiring knowledge from data interactions with the environment, which could be used in conjunction with other categories of AI, i.e. to enable C2 systems to learn how to perform tasks when expert knowledge is not available or when optimal tactics, techniques, and procedures (TTPs) are unknown;
- (6) Robotics and autonomous systems - combining AI/ML methods from all or select preceding categories that would enable unmanned systems interactions with their environment;

These AI-related categories are applicable into nearly every aspect of airpower, potentially shaping new forms of automated warfare: from C2 decision support and planning, in which AI/ML could provide recommended options or proposals in increasingly constrained times; ISR support through data mining capabilities; logistics and predictive maintenance to ensure the safety of forces and availability of platforms and units; training and simulation; cyberspace operations to detect and counter advanced cyber-attacks; robotics and autonomous systems such as drones that are utilized across various missions from ISR to the tip of the spear missions such as suppression of enemy

air defenses and collaborative combat that integrates the varying manned and unmanned platforms in air and land strike operations. In other words, the argument here is that AI systems will be increasingly capable to streamline C2 and decision-making processes in every step of the John Boyd's Observe-Orient-Decide-Act (OODA) loop: collecting, processing, and translating data into a unified situational awareness view, while providing options for a recommended course of actions, and ultimately, helping humans to act (Fawkes and Menzel, 2018).

From Defense to Military Innovation: Ongoing Challenges

However, integrating AI systems into military platforms, systems, and organizations to transform computers from tools into problem-solving “thinking” machines will continue to present a range of complex technological, organizational, and operational challenges (Raska et al, 2021). These may include developing algorithms that will enable these systems to better adapt to changes in their environment, learn from unanticipated tactics and apply them on the battlefield. It would also call for designing ethical codes and safeguards for these thinking machines. Another challenge is that technological advances, especially in military systems, are a continuous, dynamic process; breakthroughs are always occurring, and their impact on military effectiveness and comparative advantage could be significant and hard to predict at their nascent stages. Moreover, such technologies and resulting capabilities rarely spread themselves evenly across geopolitical lines.

Most importantly, however, the critical question is how much we can trust AI systems, particularly in the areas of safety-critical systems? As Missy Cummings warns, “history is replete with examples of how similar promises of operational readiness ended in costly system failures and these cases should serve as a cautionary tale” (Cummings, 2021). Furthermore, a growing field of research focuses on how to deceive AI systems into making wrong predictions by generating false data. Both state and non-state actors may use this so-called adversarial machine learning to deceive opposing sides, using incorrect data to generate wrong conclusions, and in doing so, alter the decision-making processes. The overall strategic impact of adversarial machine learning on international security might be even more disruptive than the technology itself (Knight, 2019; Danks, 2020).

From a tactical and operational perspective, many of these complex AI systems also need to be linked together – not only technologically but organizationally and operationally. For many militaries, this is an ongoing challenge - they must be able to

effectively (in real-time) integrate AI-enabled sensor-to-shooter loops and data streams between the various services and platforms. This means effectively linking the diverse Air Force, Army, Navy, and Cyber battle management systems and data; command and control, communications and networks; ISR; electronic warfare; positioning, navigation, and timing; with precision munitions. While select AI/ML systems may mitigate some of the challenges, the same systems create another set of new problems related to ensuring trusted AI. Accordingly, one may argue that the direction and character of AI trajectories in military affairs will depend on corresponding strategic, organizational and operational agility, particularly how these technologies interact with current and emerging operational constructs and force structures.

Going forward, the level of human involvement in the future of warfare, the need to alter traditional force structures and recruitment patterns and in what domains force will be used are all matters that are being challenged by new technologies. Modern militaries are developing their own and often diverse solutions to these issues. As in the past, their effectiveness will depend on many factors that are linked to the enduring principles of *strategy* – the ends, ways, and means to “convert” available defense resources into novel military capabilities, and in doing so, create and sustain operational competencies to tackle a wide range of contingencies. The main factors for successful implementation will not be technological innovations per se, but the combined effect of sustained funding, organizational expertise (i.e. sizeable and effective R&D bases, both military and commercial) and institutional agility to implement defense innovation (Cheung, 2021). This means broadly having the people, processes and systems capable of delivering innovative solutions, while maintaining existing core capabilities that would provide viable policy options in an increasingly complex strategic environment.

Bibliography:

- Barsade, I. and Horowitz, M. 2018. Artificial intelligence beyond the superpowers. *Bulletin of the Atomic Scientists*. 16 August. Available from: <https://thebulletin.org/2018/08/the-ai-arms-race-and-the-rest-of-the-world/>
- Burnett, M. et. al. 2018. Advanced materials and manufacturing - implications for defence to 2040. *Defence Science and Technology Group Report*. Australia Department of Defence. Available from: <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-GD-1022.pdf>
- Cheung, T. 2021. A conceptual framework of defence innovation. *Journal of Strategic*

Studies, DOI: 10.1080/01402390.2021.1939689.

Cummings, M. 2017. Artificial intelligence and the future of warfare. *Chatham house research paper*. 26 January. Available from: <https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf>

Cummings, M. 2021. Rethinking the maturity of artificial intelligence in safety-critical settings. *AI Magazine*, 42(1), pp.6-15. Available from: <https://ojs.aaai.org/index.php/aimagazine/article/view/7394>

Danks, D. 2020. How adversarial attacks could destabilize military AI systems. *IEEE Spectrum*. 26 February. Available from: <https://spectrum.ieee.org/adversarial-attacks-and-ai-systems>

Davis, M. 2021. The artificial intelligence ‘backseater’ in future air combat. *ASPI Strategist*, 5 February. Available from: <https://www.aspistrategist.org.au/the-artificial-intelligence-backseater-in-future-air-combat/>

Everstine, B. 2020. U-2 flies with artificial intelligence as its co-pilot. *Air Force Magazine*, 16 December. Available from: <https://www.airforcemag.com/u-2-flies-with-artificial-intelligence-as-its-co-pilot/>

Fawkes, J. and Menzel, M. 2018. The future role of artificial intelligence - military opportunities and challenges. *The Journal of the JAPCC*, 27. pp.70-77. Available from: https://www.japcc.org/wp-content/uploads/JAPCC_J27_screen.pdf

Freedman, L. 2006. *The transformation of strategic affairs*. London: International Institute of Strategic Studies.

Freitas, S. Silva, H., Almeida, J. and Silva, E. 2018. Hyperspectral imaging for real-time unmanned aerial vehicle maritime target detection. *Journal of Intelligent and Robotic Systems*. 90, pp.551-570.

Goldman, E. 1999. Mission possible: organizational learning in peacetime. In: Trubowitz, P., Goldman, E., and Rhodes, E. *The politics of strategic adjustment: ideas, institutions, and interests*. New York: Columbia University Press, pp.233-266.

Gray, C. 2006. *Strategy and history: essays on theory and practice*. London: Routledge, pp.113-120.

Hammes, T.X. 2016. Technologies converge and power diffuses: the evolution of small, smart, and cheap weapons. *CATO Institute Policy Analysis*. 786, 27 January. Available from: <https://www.cato.org/policy-analysis/technologies-converge-power-diffuses-evolution-small-smart-cheap-weapons>

Horowitz, M. 2018. The promise and peril of military applications of artificial

- intelligence. *Bulletin of the Atomic Scientists*. 23 April. Available from: <https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/>
- International Institute for Strategic Studies. 2019. Quantum computing and defence. In: IISS. *The military balance*. London: Routledge, pp. 18-20.
- Jensen, B. and Pashkewitz, J. 2019. Mosaic warfare: small and scalable are beautiful. *War on the Rocks*. 23 December. Available from: <https://warontherocks.com/2019/12/mosaic-warfare-small-and-scalable-are-beautiful/>
- Knight, W. 2019. Military artificial intelligence can be easily and dangerously fooled. MIT Technology Review. 21 October. Available from: <https://www.technologyreview.com/2019/10/21/132277/military-artificial-intelligence-can-be-easily-and-dangerously-fooled/>
- Lee, CM.2016. *Fault lines in a rising Asia*. Washington DC: Carnegie Endowment for International Peace, pp. 119-175. Available from: <https://carnegieendowment.org/2016/04/20/fault-lines-in-rising-asia-pub-63365>
- Lingel, S. et. al. 2020. Joint all-domain command and control for modern warfare - an analytic framework for identifying and developing artificial intelligence applications. *RAND Corporation Project Air Force Report*. Available from: https://www.rand.org/pubs/research_reports/RR4408z1.html
- Mahnken, T. (ed.). 2012. *Competitive strategies for the 21st century: theory, history, and practice*. Stanford: Stanford University Press, pp.3-12.
- Raska, M. 2016. *Military innovation in small states: creating a reverse asymmetry*. New York: Routledge. Available from: <https://www.routledge.com/Military-Innovation-in-Small-States-Creating-a-Reverse-Asymmetry/Raska/p/book/9780367668617>
- Raska, M. 2020. Strategic competition for emerging military technologies: comparative paths and patterns. *Prism – Journal of Complex Operations*. 8(3), pp.64-81. Available from: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Raska_64-81.pdf
- Raska, M. 2021. The sixth RMA wave: disruption in military affairs? *Journal of Strategic Studies*. 44(4), pp.456-479.
- Raynolds, K. 2006. *Defence transformation: to what? for what?* Carlisle: Strategic Studies Institute.
- Robinson, T. 2021. The air force of 2040 – synthetically-trained, cloud-networked, space-enabled and NetZero? Royal Aeronautical Society, 10 August. Available from: <https://www.aerosociety.com/news/the-air-force-of-2040-synthetically-trained-cloud-networked-space-enabled-and-netzero/>

- Ross, A. 2010. On military innovation: toward an analytical framework. *IGCC Policy Brief*. 1, pp.14-17. Available from: <https://escholarship.org/uc/item/3d0795p8>
- Stanley-Lockman, Z. 2021(a). Responsible and ethical military AI: allies and allied perspectives. *Center for Security and Emerging Technology Issue Brief*. 25 August. Available from: <https://cset.georgetown.edu/publication/responsible-and-ethical-military-ai/>
- Stanley-Lockman, Z. 2021(b). Military AI cooperation toolbox: modernizing defense science and technology partnerships for the digital age. *Center for Security and Emerging Technology Issue Brief*. 25 August. Available from: <https://cset.georgetown.edu/publication/military-ai-cooperation-toolbox/>