RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 129 – 13 December 2022

The Future of Digital Warfare

By Michael Raska

SYNOPSIS

Cyber operations have been evolving as part of major wars and conflicts over the past three decades. However, modern militaries have struggled to align them with conventional military power. If militaries fully harness the next cyber revolution, there could be enormous implications and lessons for future warfare.

COMMENTARY

The main source of strategic advantage in the next ten years will lie in the ability of modern military organisations to fully integrate innovations in artificial intelligence (AI), cyber power and data science, cognitive science, and robotics across all levels of operations and warfare.

This process will drive the next AI-driven Revolution in Military Affairs or the AI Wave. The AI wave will fundamentally differ from the previous information technology or IT-RMAs, where cyber capabilities augmented, but did not alter, the use of force.

The AI Wave

Early signposts of the AI wave are visible in the diffusion of advanced technologies in military organisations along with conceptions of future warfare and organisational changes. The Data Analytics Centre of the Israel Defence Force Unit 8200, for example, uses machine-learning algorithms to automate threat detection and identify anomalies in large data sets.

The US military's Project Maven uses AI systems for decision support, targeting, and operational planning. They can process a large amount of data from diverse intelligence, surveillance, and reconnaissance sensors.

AI also shapes the training and simulation, including cyberspace operations, and robotics and autonomous systems such as drones in China's People's Liberation Army, including its new military research and development agency, the *Junweikejiwei*.

And the Singapore Armed Forces is focusing on the Digital and Intelligence Service to integrate SAF's military intelligence, cyber defences, electronic defence, and information operations capabilities into a full-service branch on par with the navy, air force, and the army.

The weaponisation of the AI wave and cyber will likely evolve further with the rapid interdisciplinary advances in science and technology. Data and computer sciences are increasingly merging with behavioural sciences, including psychology, neuroscience, linguistics, and anthropology, which overlap with nearly every aspect of cybersecurity.

The US Defense Advanced Research Projects Agency (DARPA), for example, has invested considerable resources into the Next-Generation Nonsurgical Neurotechnology Programme, which aims to develop brain-machine interfaces that enable control of unmanned aerial vehicles and active cyber defence systems.

Critical Infrastructure Vulnerable

In future conflicts, modern militaries will apply diverse AI-enabled cyber capabilities in targeting an adversary's critical infrastructure, such as power, transportation, satellite and communication grids.

They will also try to infiltrate competitors' networks and data centres to manipulate algorithms or to corrupt data. Growing research focuses on how to deceive AI systems into making wrong predictions by generating false data - adversarial AI. State and non-state actors will use adversarial machine learning to deceive opposing sides, corrupt data and manipulate algorithms that would generate wrong conclusions and alter the decision-making processes.

Algorithms will be increasingly used to detect disinformation and misinformation in social media, spotting smart bots and deep fakes, and biometric security vulnerabilities such as spoofing.

While these are early versions of capabilities that are likely to advance considerably between now and 2040, the actual use of AI-enabled systems reflects the pace of innovation and the urgency to incorporate the value of AI and machine learning into military operations, both of which are likely to increase as more AI-enabled capabilities are deployed.

The AI wave has already crossed important thresholds into the actual *deployment* of AI-enabled systems and capabilities in real-world military operations. The US Air Force has used AI to identify and track targets in combat, while China has been experimenting with AI-driven drone swarms deployed into near space, alongside a planned arsenal of anti-stealth drones, hypersonic spy planes and high-altitude micro-UAVs.

Australia too is working on loyal wingman capabilities, in which crewed fighter jets are

paired with a team of unmanned aerial vehicles (UAVs). Japan, for its part, is focusing on development of a range of technologies that include directed energy, AI, hypersonic missiles, longer-range air-launched missiles to execute new counterstrike missions, and technologies relevant to competing in the space and cyber domains and electromagnetic spectrum.

Rethinking Defence Planning

While the AI wave may affect select countries and militaries disproportionately, its impact on the use of force could be significant and hard to predict at nascent stages.

However, the long-term strategic impact of the AI wave in future conflicts will be sufficiently broad to require a rethinking of defence policy planning and management, including weapons development and R&D, defence budgetary processes, as well as operational and warfighting domains and concepts.

The AI wave's direction and character will be shaped by corresponding strategic, organisational, and operational agility, mainly how emerging technologies interact with current and future operational constructs and force structures.

This is evident, for example, in the challenges facing the Russian military in using its advanced military systems, including cyber capabilities, in the ongoing war in Ukraine. The Russian invasion of Ukraine has exploded many myths, perhaps none more than the myth that, over the past decade or so, Russia has successfully transformed and modernised its armed forces.

However, the conflict's developments will provide many potential lessons for future warfare, including how novel technologies will be used in future conflicts.

The mounting intensity of great power competition, the scale and pace of China's military modernisation, China's boundary-pushing behaviour, and, finally, concerns over the US security commitment to the region are all serving as catalysts for other states across the region to pursue new and enhanced military capabilities and to take on new missions.

Further changing the environment are advanced manufacturing techniques. Automated factories, robotics and AI can be combined to dramatically reduce the cost of these emerging autonomous systems. Consequently, advanced military-industrial sectors are no longer the primary drivers of technological innovation; instead, emerging technologies with dual-use potential are being developed in the commercial sectors, including those of small states and middle powers, and then being spun off to military applications.

New Defence Transformation Roadmaps

The principal challenge for implementing the AI wave in modern military organisations will be a wholesale re-engineering of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), strategy and doctrine, and, crucially, the art of warfare.

An entirely new operational environment and novel technologies will require new mindsets at every echelon of military organisations.

Militaries must also grapple with the contending legal and ethical implications of new weapons technologies and problems in encoding diverse values of safety, ethics, and governance into these systems.

For example, integrating data streams and AI systems across different military platforms, including cyber systems and organisations, will require trustworthy algorithms that will enable these systems to adapt to changes in their environment and learn from unanticipated events. It would also call for designing ethical codes and safeguards for these systems.

Ultimately, building a viable roadmap so traditional militaries can incorporate disruptive innovation paths that embrace creativity and innovation and accept massive disruptions is the military equivalent of massive 'mergers & acquisitions.'

For many militaries, it will be a hugely difficult task. But to win wars and conflicts into the 2030s and beyond, it is a task that must be met.

Michael Raska is Assistant Professor and Coordinator of the Military Transformations Programme at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg