No. 010/2022 dated 22 February 2022

The Contours of Emerging Technologies and Future Warfare

Richard Bitzinger and Michael Raska

SYNOPSIS

The Indo-Pacific is the world’s primary zone of strategic competition, involving great power clashes, artificial intelligence–driven military innovation, and potential crisis hot zones, including the Korean peninsula, Taiwan and the South China Sea. The confluence of strategic competition and diffusion of advanced military technologies enables new forms of warfare that shapes a major military change in East Asia.
East Asia has never produced so much hard power and wealth in its history, but, at the same time, its ability to harness these attributes to stabilise world order is untested. The strategic status quo in East Asia is being contested on multiple fronts: by North Korea’s rising nuclear capabilities, and China’s anti-access/area-denial (A2/AD) capabilities in key crisis hot zones, including Taiwan and the South China Sea.

Most importantly, for the first time in decades, the United States faces a strategic peer-competitor, China, capable of pursuing and implementing its own “intelligentised revolution in military affairs (RMA),” driven by artificial intelligence (AI) systems, which can potentially negate the strategic and operational advantages of the US military across geopolitical lines.

While the United States remains the sole superpower, it is no longer an indispensable power. It is no longer willing or able to be the “world’s policeman”; at the same time, it does not want others to assume the task. In particular, the United States wants to prevent China from becoming a new superpower. Nevertheless, this is probably impossible: China is likely to overtake the United States in real GDP in the 2030s and reach de facto military parity with the US military by the 2040s. In sum, by the middle of the century, China is going to be a superpower and have a voice in every major Asian and global issue.

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.

Australia, for example, 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.

The game-changing promise of AI 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.

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.
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 Forms of Hybrid Warfare**

Emerging technologies enable new forms of hybrid warfare. These include space-based hybrid operations, directed energy weapons, high-power microwaves, electronic operations (jamming, spoofing, etc.), and attacks on satellites. Another form of hybrid warfare is the concept of “war as a service” (WaaS). WaaS builds on the concept of military ecosystems and can be understood as a comprehensive politico-military concept to transfer military power in a government-to-government framework, thereby shifting the focus away from outsourcing military power to other nations or non-state actors.

Finally, there is the concept of the “weaponisation of everything”. Its strategic objective is the broad erosion of existing power and authority systems. It is proto-revolutionary in that it is designed to weaken, degrade, and destroy existing power and authority systems without a clear replacement. It is being used or likely to be used by three types of organisations: revisionist nations, particularly Russia, Iran, and China; organised criminal networks which believe that erosion of state power and authority will provide them greater operating space; and ideological movements, most likely based on new radical ideologies constructed on race, generation, or religion (to include religious opposition to technology). Most states are unprepared for this second generation of the weaponisation of everything. At issue, therefore, is whether states will be adequately innovative and resilient as they face multi-vector, often clandestine (and especially swarming), attacks on their systems of power and authority.

**Grey Zones: Challenges and Responses**

As a result of the first two developments, one should expect to see an expansion of “grey zone” operations, defined as competitions between state actors (or between state and non-state actors) that fall outside traditional concepts of conflict. Russia and China are expanding their grey-zone competitions in Ukraine and elsewhere in Central and Eastern Europe, and Japan, respectively. The goals of such operations are to reduce US power and influence in both Europe and Asia, while expanding their own geopolitical interests.

Grey-zone tactics include “elite capture” (via bribery and other corrupt practices), energy dependency and other economic pressures, strategic corruption, and disinformation campaigns. Chinese influence operations in Japan, for example, are targeted at the media (some local media outlets in Japan are partly owned by China), academia and local politicians, among others, and also are intended as part of their economic espionage campaigns. The primary goals are to (1) promote pro-China sentiment, (2) spread Communist Party of China propaganda, (3) instigate anti-Korea sentiment, and (4) instigate anti-Western sentiment.
Given recent increases in Russian and Chinese grey-zone aggression, deterrence of such aggression must include both denial and punishment. Deterrence by denial primarily consists of societal resilience, which begins with an informed public. Deterrence by punishment of grey-zone aggression builds on deterrence by denial. Examples include embargoes of luxury goods, which are prized by both Russian and Chinese elites. If the West signalled that it could suspend such exports when it decided that grey-zone aggressions had reached an intolerable level, both countries might try to stay far below that level. Because they do not know where precisely Western governments’ threshold of pain is located, the prospect of punishment would cause them to stay far below where they imagine the threshold is. The same goes for other sanctions that Western governments could employ, such as threatening to cancel visas for political, economic, and cultural elites of aggressor-nations, as well as for their families.

**Strategic Implications**

The convergence of emerging technologies and new forms of hybrid warfare presents novel strategic challenges to traditional conceptions of deterrence and defence, particularly in the context of “cross-domain deterrence and compellence” (CDD&C) challenges.

CDD&C refers to the act of deterring an action in one domain through a threat in another domain — where the domains are defined as land, under the land, at sea, under sea, in the air, in space, and in cyberspace — and may often involve the use of economic sanctions and other diplomatic, political and informational tools. In other words, emerging technologies may enable cross-domain coercion in multiple domains to influence an opponent's strategic choices.

Consequently, when contemplating how emerging technologies such as AI may further affect security and defence trajectories, defence planners and militaries have to learn to use “non-kinetic toolkits”. What types of challenges does this present for them? How will they operate in a contested environment characterised by the diffusion of sophisticated longer-range adversary capabilities and methods such as ballistic missiles, submarines, weapons of mass destruction, as well as offensive space, cyberspace, and AI-enabled warfare assets?

Overall, how nations — and in particular, their military-industrial complexes — can leverage advanced military and dual-use technologies will have a significant impact on military capabilities. Such technologies and capabilities are being distributed unequally. Some countries will possess the resources to exploit advanced military technologies — either through indigenous R&D efforts or through acquisition from foreign suppliers — and others will not; some will have the means to systems-engineer advanced commercial technologies into effective military systems (i.e., spin-off) and others will not. The main factors for success are probably funding, existing expertise (i.e., sizeable and effective R&D bases, both military and advanced commercial), and top-down commitment to such a goal. All of these factors, in turn, will probably have a significant impact on regional security and stability.
Richard BITZINGER is Visiting Senior Fellow and Michael RASKA is Assistant Professor with the Military Transformations Programme of the Institute of Defence and Strategic Studies (IDSS), RSIS.