gp ORF

global POLICY

GP-ORF Series

The Future of War in South Asia: Innovation, Technology and Organisation

EDITED BY

Manoj Joshi
Pushan Das

Durham University

WILEY-BLACKWELL

THE FUTURE OF WAR IN SOUTH ASIA: INNOVATION, TECHNOLOGY AND ORGANISATION

Edited by
Manoj Joshi
Pushan Das

Observer Research Foundation
20 Rouse Avenue, Institutional Area
New Delhi, India 110002
contactus@orfonline.org
www.orfonline.org

ORF provides non-partisan, independent analyses on matters of security, strategy, economy, development, energy and global governance to diverse decision-makers including governments, business communities, academia and civil society. ORF's mandate is to conduct in-depth research, provide inclusive platforms, and invest in tomorrow's thought leaders today.

Editing: Preeti Lourdes John

Design and Layout: Rahil Miya Shaikh

Cover Image Source: STR/Chinese People's Liberation Army (PLA) soldiers take part in a training session at Pamir Mountains in Kashgar, in China's western Xinjiang region on August 28, 2020/Getty/Rights-managed
https://www.gettyimages.in/detail/news-photo/chinese-peoples-liberation-army-soldiers-take-part-in-a-news-photo/1228235620?adppopup=true

ISBN: 978-93-90494-38-5

Citation: Manoj Joshi and Pushan Das, eds, The Future of War in South Asia: Innovation, Technology and Organisation (New Delhi: ORF and Global Policy Journal, 2021).

Contents

Introduction: Military Transformation and the China Challenge

Pushan Das and Manoj Joshi

Indian and Chinese forces engaged in a primeval brawl in the summer of 2020 in the Galwan Valley, with the two sides using stones and nail-studded clubs, but no firearms (1). This clash claimed the lives of at least 20 Indian soldiers and four People's Liberation Army (PLA) personnel. While the Indian commander was killed, his Chinese counterpart got away with serious injuries. It was the most serious incident on the India-China border since 1975.

The leveraging of loopholes in the traditional notions of warfare to limit the potential of escalation to conventional conflict is reflective of the Chinese strategy of relying on coercion and the manipulation of risk to achieve its territorial objectives (2). The Chinese model falls into what can be referred to as Gray Zone activities where it preys upon ambiguities in international law.

With the adoption of rapidly evolving development—and in some cases, regression—of advanced warfighting technologies, the face of warfare is changing. Last year, a US Congressional Research Service note on Emerging Military Technologies listed

an overview of selected emerging military technologies in the US, China and Russia, such as lethal autonomous systems, artificial intelligence (AI), hypersonic weapons, directed energy weapons, biotechnology and quantum technology (3). As the report recounts, the face of warfare is changing with the rapidly evolving development of advanced warfighting technologies. Understanding the adoption of these technologies and the strategies to employ them will be key to countering the kinetic and geographic components of China's growing capabilities.

The security competition with China is unique and unprecedented in its complexity. The strategic challenge from China spans locales and domains. It surrounds India geographically and involves all instruments of national power. And China's recent military reforms lend it not only greater capabilities, but the command arrangements to deploy them jointly.

The PLA is undergoing far reaching reforms that have changed its organisational structures and is seeing an increasing integration of improved military equipment, targeting the goal of generating a 'world-class' military force by 2049. Terms like mechanisation, informatisation and, more recently, intelligentisation in Chinese military literature reflect some of Beijing's efforts in introducing networked platforms, sensors and weapons that can support not only better and more integrated command-and-control systems but potentially also over-the-horizon targeting at extended ranges (4).

The degree to which the integration of informationised capabilities, such as big data and AI, will influence China's approach to future warfare is unclear as its peer adversaries are adopting similar technologies. However, Maj. Gen. PK Mallick (retd.) has pointed out that India's capability to decrypt high grade cipher is non-existent, and it has an ambiguous command and control setup for cyber security operations.

In the future, the amount of data available for use will increase substantially, and how this data will be stored and processed will

be a key war winning factor. Militaries will need to be equipped to sift through and analyse terabytes of information, and this is not something humans do naturally (5). Thus, while the prospects of additional data can enhance military intelligence and operations, the inability to process an over-abundance of data will be a problem. To analyse important state capability in cyberspace, we have developed a taxonomy that focuses on enablers, including indicators of capability from the civilian sector and the armed forces.

Apart from the organisational and doctrinal shifts in the PLA, the 1 October 2019 parade marking the 70th anniversary of the founding of the People's Republic was indicative of the advances in China's defence modernisation.

Of note was China's new air systems that were displayed during the parade—the WZ-8 highspeed reconnaissance unmanned aerial vehicles and unmanned combat air vehicle (6). The first operational Chengdu J-20A fighter/ground-attack aircraft PLA Air Force (PLAAF) unit was formed in 2019, and production of the type is likely to increase over the next few years as more units are re-equipped with it. At the same time, the Shenyang J-31 multi-role combat-aircraft project continues, but at a slower pace than that of the J-20A. Justin Bronk writes that the PLAAF, and possibly the PLA Naval Air Force, will begin to field several operational unmanned combat aerial vehicle designs with significant degrees of lethal automation and broadband stealth for strike, intelligence surveillance and reconnaissance and potentially offensive counter-air operations in highly contested airspace.

In January 2020, China commissioned the first of eight Type-055s, currently under construction or already complete. The Type-055 includes several features that illustrate the progress being made by Chinese shipbuilders in incorporating complex technologies onto ships with the introduction of new capabilities in the form of an integrated mast, large-diameter vertical launching system cells, and its power generation capacity (7). Beyond the Type-055, China's output of surface

combatants remains striking, with the 19th and 20th Type 052D (Luyang III-class) destroyers launched in May 2019 and a 63rd Type-056/056A (Jiangdao I/II-class) corvette later in August 2019 (8).

Malcom Davis's chapter in the volume outlines the need for the Indian and Australian navies to have a forward presence and sufficient combat mass to counterbalance and deter the PLA Navy. There is a case to invest more in advanced autonomous systems on and under the waves, and in the air, to combat the mass being generated by China. Autonomous systems have inherent advantages in terms of lower acquisition and sustainment cost, reduced risk absent a crew, and the potential benefits of exploiting rapid innovation cycles.

The process of re-equipping the PLA Army continues, with a focus on the objectives of completing basic mechanisation and improving informatisation. Legacy equipment, such as the ZTZ-59 tank and PL-59 howitzer, is now being cycled out of frontline units, although it is unlikely that all of these weapons systems would have been replaced. The PLA Army is also dabbling in unmanned ground vehicles. It has been testing the "Desert Wolf" series of unmanned ground vehicles, which run on caterpillar tracks and are equipped with remotely controlled weapon stations (9). Maj. Gen. BS Dhanoa's (retd.) chapter on autonomous ground systems lays out the unique challenges such ground systems are likely to face in their adoption by India and in many ways other countries.

The PLA is a beneficiary of the "whole of the system" approach promoted by the civil-military fusion strategy being pushed by the Chinese leadership. At the heart of this is the understanding that technological innovation and innovative approaches in defence policy is the route towards creating a war-winning military. For the PLA, the key to victory in a conventional war lies in the dominance of space, cyberspace and the electromagnetic domains. The creation of a Strategic Support Force in December 2015 was aimed at providing the PLA with the capacity of undertaking integrated joint operations and fighting and winning informationised, if not intelligentised, wars of the

future.

Even when the Indian defence establishment recognises the need to counter PLA modernisation and adopt the operational concepts such as "informationised warfare", there exists a broader ambivalence regarding force integration among the three Indian services. Minus this integration, it is simply not possible to develop operational concepts that can enable effective combat in the cyber, electromagnetic and space domains. There is little evidence to suggest that any of the three services have adopted a capability-based approach versus the previous threat-based one. The character of war is changing—with less distinction between ground-air-sea forces, less distinction between close and deep areas, and less distinction between peace and war. Rajeswari Pillai Rajagopalan's chapter is an attention call to Beijing's increasing competencies in space and counterspace capabilities, the way it has undertaken the institutional reorganisation to strengthen the role of these capabilities, and the likely national security consequences for the region.

India's current defence spending priorities are, however, heavily weighted towards traditional means of war-fighting and conventional modes of deterrence (10). Current postures favour large-scale conflict in the form of a "two-front war", but India has an almost negligible forward presence, limited lower-end and versatile assets, and a lack of strategically mobile forces and limited capabilities to meet asymmetric threats which use a combination of defence and commercial technology. The recent conflict over Nagorno-Karabakh was a 'drone's eye view' on challenge of disruptive and accessible technology (11). Kabir Taneja writes that there is a need for the Indian military to consider the threats posed by these disruptive capabilities in the hands of non-state actors and an urgent need to develop counter measures.

The Indian military thus needs to better invest in a diverse range of dynamic forces and assets to effectively counter adversary challenges along the full spectrum of conflict, particularly

in those contests that may occur below its conventional strategic thresholds. Effective deployment, both in terms of speed and distance, is probably the greatest contemporary challenge facing the Indian military. Given the difference in the size of their economies and the head-start that China has in military modernisation, playing catch-up will be difficult, if not impossible. But smaller militaries have prevailed over larger and better equipped ones by using asymmetrical strategies. But to develop them, India needs to first have a better grasp of its current predicament.

The aim of this edited volume is to establish India's defence technology goals and strategies needed to achieve them. How can the Indian Armed Forces adapt legacy platforms and doctrines to counter emerging military technologies of the future? By identifying and highlighting the gap between the existing capabilities and the requirements of the future, the volume hopes to initiate a conversation to understand these changes with an outlook to 2030.

Endnotes

(1) Michael Peck, "China May Be Arming Its Soldiers With Medieval Halberds To Fight India," *Forbes*, September 09, 2020, https://www.forbes.com/sites/michaelpeck/2020/09/09/china-is-arming-its-soldiers-with-medieval-halberds-to-fight-india/

(2) Harsh V. Pant and Pushan Das, "China's Military Rise and the Indian Challenge," *ORF*, April 19, 2018, https://www.orfonline.org/expert-speak/china-military-rise-indian-challenge/

(3) Kelley M. Sayler, *Defense Primer: Emerging Technologies*, p. 3

(4) "Chapter One: Defence and Military Analysis," *The Military Balance* 120, no. 1 (January 1, 2020), pp. 9–20, https://doi.org/10.1080/04597222.2020.1707961

(5) "Using Big Data in Military Operations: This Is How Future Wars Will Be Fought," *Analytics India Magazine (blog)*, October 03, 2015, https://analyticsindiamag.com/using-big-data-in-military-operations-this-is-how-future-wars-will-be-fought/

(6) "More Than Missiles: China Previews Its New Way of War," *Center for Strategic & International Studies*, October 16, 2019, https://www.csis.org/analysis/more-missiles-china-previews-its-new-way-war
(7) "The US Navy's Large Surface Combatant Programme: A Project in Search of a Clear Rationale," *RUSI*, January 28, 2021, https://rusi.org/commentary/us-navy%E2%80%99s-large-surface-combatant-programme-project-search-clear-rationale
(8) "Chapter Six: Asia," *The Military Balance* 120, no. 1 (January 1, 2020), pp. 220–323, https://doi.org/10.1080/04597222.2020.1707967
(9) "China's Latest Unmanned Combat Systems to Enter Service, Aim to Win Future Wars for PLA: reports," *Global Times*, November 12, 2020, https://www.globaltimes.cn/content/1206680.shtml
(10) Pushan Das and Sushant Singh, "Today's capabilities, tomorrow's conflicts," *ORF*, February 22, 2017, https://www.orfonline.org/expert-speak/todays-capabilities-tomorrows-conflicts/
(11) Robyn Dixon, "Azerbaijan's Drones Owned the Battlefield in Nagorno-Karabakh — and Showed Future of Warfare," *The Washington Post*, November 12, 2020, https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html

Robots at War: The Future for Autonomous Systems at Sea in the Indo-Pacific

Malcolm Davis

Future naval forces will exploit a mix of traditional crewed vessels and unmanned autonomous systems that operate over, on and under the waves. These autonomous systems will be able to generate a lethal effect on the future battlespace and, as a recent report by the Congressional Research Service suggested, be "…capable of both independently identifying a target and employing an onboard weapon to engage and destroy the target without manual human control" (1). The introduction of lethal autonomous weapon systems has some significant implications for future warfare.

Firstly, the development of autonomous systems opens the prospect for re-introducing *mass* onto the future battlespace. Since the 1980s, the decisive factor in war has been gaining and sustaining a knowledge edge over an opponent to enable a qualitative advantage as the principle means to ensure victory. That remains important, but the rising unit cost of ever more capable military platforms has seen the numbers of those platforms steadily shrink, such that all but the largest

military forces are becoming increasingly boutique and brittle in a manner that raises constraints on operational readiness. In peacetime, the quest for a qualitative edge generates long acquisition cycles, and high development and sustainment costs. This generates the risk of a fiscal death spiral in capability acquisition that ultimately makes large numbers of complex and expensive platforms prohibitively expensive. Witness the fate of the US's B-2A bomber and F-22 fighter.

With autonomous systems, this trend can be potentially reversed. The key must be embracing a fast innovation cycle that avoids long-term sustainment costs. Such an approach is already being considered for the US Air Force's next generation air dominance programme under a 'digital century series' model, encompassing both crewed and autonomous platforms in a future air combat system (2,3). The same approach could be applied to other domains, including for naval warfare. If autonomous systems can be produced quickly and cheaply, then rather than seeing a small number of expensive and complex systems being acquired over a very long time at great cost, the possibility of 'swarms' of cheap, expendable and fully autonomous platforms and loitering weapons in the future battlespace might emerge, in which *quantity will have a quality of its own* (4).

Also of key importance in the development of autonomous systems is artificial intelligence (AI) to enable fully autonomous weapons and platforms, rather than systems that are remotely controlled (human 'in the loop') or given only limited autonomy ('on the loop'). This is especially important if swarming on the battlespace, including at sea, is to be a realistic option. It is simply impractical for direct human control of large numbers of unmanned systems to be viable. The accelerating pace and growing complexity of modern warfare means that AI will be essential if autonomous systems are to be effectively employed (5).

AI will emerge on delivery platforms and in the weapons themselves, allowing them to identify targets, and choose

when and how to strike without necessarily needing human intervention. This is already apparent with the development of weapons such as the AGM-158C Long-range anti-ship missile (LRASM), which can network and operate as a swarm and work out the best tactics to attack a particular target (6). With the incorporation of AI, war at 'machine speed' will generate a race to be the first major power to use AI in war comprehensively (7). There's a significant ethical and legal dilemma that emerges as a result. For western liberal democracies, a key issue in using lethal autonomous weapon systems is doing so in a manner consistent with the laws of armed conflict that define rules of engagement. For liberal democracies like Australia and India, there is debate on developing trusted autonomy in future systems and defining how far to go in allowing fully autonomous weapons and platforms.

This requirement may act as a constraint on the ability of these states to use lethal autonomous weapon systems, but authoritarian peer adversaries may not face similar constraints, and against a peer adversary equipped with autonomous weapons and willing to use them in an unconstrained manner, the military advantage might shift to our opponents.

Autonomous Weapons at Sea

The US Navy is already moving towards a mixed fleet of crewed and autonomous vessels (8). It is developing advanced capabilities such as the Sea Hunter unmanned surface vehicle (USV) and 'Orca' large unmanned underwater vehicle (XLUUV) (9). These are moving rapidly towards becoming operational systems, and they point to a future naval warfare environment where autonomous robotic systems operate alongside traditional warships and submarines. The Royal Australian Navy (RAN) is already embracing this path and has recently released its own 'remote and autonomous systems-artificial intelligence' (RAS-AI) strategy document that charts a course through 2040 to develop and incorporate such capabilities (10). Local development of the Ocius Technologies' 'Bluebottle' USV opens up prospects for hundreds of such platforms, operating

as a network to undertake surveillance tasks in a manner that can support maritime domain awareness missions and a range of military tasks (11). Although the RAN does not have specific capabilities for armed autonomous platforms being developed currently, the release of the RAS-AI strategy highlights a path to such platforms before the 2040s.

India is also pursuing unmanned underwater vehicle (UUV) capability for undersea surveillance purposes (12,13,14). China is also seeking to develop advanced UUV and USV capabilities, with UUVs on display at the recent 70th-anniversary military display (15). Analysts suggest that the Chinese HSU-001 Large Displacement UUV that was displayed at the parade is large enough to carry unattended sensors or mines, but is likely to be tasked with intelligence gathering missions near the surface. The HSU-001 is less than half the size of the US's XLUUV, and like the US's 'Snakehead' UUV, will likely be deployed from the People's Liberation Army Navy (PLAN) surface ships or a drydock on a submarine (16). On USVs, the Chinese have chosen to make an exact copy of the US Navy's Sea Hunter, which is likely to have greater displacement than the US Navy platform (17,18).

The combination of these UUV and USV platforms will contribute towards establishing a 'Great Underwater Wall' around the South China Sea (19). This will be a network of sensors positioned on the seabed, combined with mobile unmanned platforms on and below the waves, operating autonomously and utilising AI to coordinate their actions. The goal will be to prevent an adversary from deploying submarines into the region sufficiently close to China to either threaten PLAN warships, or be able to launch land-attack cruise missiles against land targets. As such, Chinese UUV and USV development needs to be seen through the context of the broader concept of anti-access and area denial, and their development and eventual deployment will be designed to further reduce the ability of the US to intervene militarily in the event of a regional crisis, perhaps over Taiwan.

With China moving forward with its own unmanned systems at sea, how states such as Australia and India can use unmanned systems to respond to the growing Chinese naval capability becomes a key issue, now and in the future.

Firstly, numbers do matter. The rapidly modernising and growing Chinese PLAN has overtaken the US Navy in numbers of battle force ships, at 350 ships and submarines, including over 130 major surface combatants, compared to the US Navy's 293 ships (20). With this larger and more modern fleet, which will continue to grow, it is likely that over time the PLAN will be able to assume a more visible and substantial presence in the 'far seas' of the Indian Ocean, as China seeks to assert its interests and presence along the twenty-first century maritime silk road.

This could see the PLAN exploiting Chinese-established commercial ports to support its naval forces, as well as a growing prospect for increasing the number of PLAN aircraft carrier battlegroups—perhaps four to six aircraft carriers being built—and a growing number of more advanced large amphibious ships that can operate combat aircraft, akin to escort carriers, which are likely to establish a presence along the maritime silk road (21).

Though the main strategic direction for the PLAN remains Taiwan and the near and middle seas within the first and second island chains, there is a clear indication that China is building power projection capabilities that will challenge the security interests of states along the Indian Ocean littoral. Responding to this larger and more assertive PLAN means regional navies must have a forward presence *and sufficient combat mass* to counterbalance and deter China from acting in a manner inimical to their interests. It makes sense to invest more in advanced autonomous systems on and under the waves and in the air to complement crewed platforms, given the inherent advantages of autonomous systems in terms of lower acquisition and sustainment cost, reduced risk absent a crew, and the potential benefits of exploiting rapid innovation cycles. But such systems must be acquired in sufficient numbers

to make their impact worthwhile. Numbers matter. And the benefits of autonomous systems will be reduced if they are not fully or mostly autonomous. Remotely piloted UUVs and USVs, limited in range, endurance and payload, make little sense, given the operational and tactical factors that are now confronting regional naval forces.

Indeed, advanced autonomous systems at sea can be launched from traditional submarines and surface ships, but they will be smaller and have a more limited range and payload. The focus of capability acquisition in autonomous systems must be on more capable fully autonomous capabilities, with the Orca UUV and Sea Hunter USV being the exemplar.

Unmanned systems still need to 'plug and play' with the rest of the fleet to be useful, so developing secure and resilient command and control in the future battlespace becomes ever more important. That could have significant implications for how major powers in the Indian Ocean region think about the use of space and 'near space' based UAV capabilities, and to mitigate the growing threat posed by Chinese counterspace capability.

In addition, the pace at which China develops its autonomous weapons capabilities should determine how quickly states like Australia and India respond. The RAN's RAS-AI Strategy has a 20-year timeline, with armed UUVs only appearing by the 2040s and USV operations emphasising non-kinetic operations until the 2040s. This relaxed pace may prove insufficient to meet the likely development of ever-more sophisticated PLAN unmanned and autonomous weapons capabilities, and is likely to slip behind what will probably be faster US development of autonomous systems such as Orca and Snakehead.

Finally, advances in AI, together with the implications of swarming networks of UUVs and USVs, and the prospects offered by quantum technologies to transform secure communications, sensing and computing functions in war, may reduce the opacity of the oceans for submarines—necessitating greater

reliance on UUVs rather than putting crewed platforms at risk. The question then becomes how 'depopulated' the future maritime battlespace will become in the coming years. It is not inconceivable that by the 2040s, much of the fighting will be done by the robots, with their human masters kept well behind harm's way.

Endnotes

(1) Kelley M. Sayler, *Emerging Military Technologies: Background and Issues for Congress*, Washington DC, Congressional Research Service, 2020, https://fas.org/sgp/crs/natsec/R46458.pdf.
(2) Valerie Insinna, "US Air Force's next-generation fighter inches forward with a new program head", *Defense News*, October 3, 2019, https://www.defensenews.com/air/2019/10/03/the-air-forces-next-generation-fighter-inches-forward-with-a-new-program-head/.
(3) Malcolm Davis, "Mystery US jet shows there's a faster path to Australia's future fighter," *The Strategist*, September 17, 2020, https://www.aspistrategist.org.au/mystery-us-jet-shows-theres-a-faster-path-to-australias-future-fighter/.
(4) Malcolm Davis, "Cheap drones versus expensive tanks: a battlefield game-changer?," *The Strategist*, October 21, 2020, https://www.aspistrategist.org.au/cheap-drones-versus-expensive-tanks-a-battlefield-game-changer/.
(5) Margarita Konaev, "With AI, We'll see faster fights, but longer wars," *War on the Rocks*, October 29, 2019, https://warontherocks.com/2019/10/with-ai-well-see-faster-fights-but-longer-wars/.
(6) Lockheed Martin, "LRASM: Long-range anti-surface cruise missile," https://www.lockheedmartin.com/en-us/products/long-range-anti-ship-missile.html.
(7) Zachary Fryer-Biggs, "Coming Soon to the Battlefield: Robots that can kill," *The Atlantic*, September 3, 2019, https://www.theatlantic.com/technology/archive/2019/09/killer-robots-and-new-era-machine-driven-warfare/597130/.
(8) Ronald O'Rourke, *Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress*, Congressional Research Service, December 23, 2020, https://fas.org/sgp/crs/weapons/R45757.pdf.
(9) Mallory Shelbourne, "Navy to use Sea Hunter in Fleet Exercises as Unmanned Systems Experimentation Continues," *USNI News*, September 30, 2020, https://news.usni.org/2020/09/30/navy-to-use-sea-hunter-in-fleet-exercises-as-unmanned-systems-experimentation-continues.

(10) Australian Naval Institute, "Chief of Navy launches the RAS-AI Strategy 2040," https://navalinstitute.com.au/chief-of-navy-launches-the-ras-ai-strategy-2040/.
(11) Ocius Technologies, "Innovative Autonomous Solutions for persistent maritime surveillance," https://ocius.com.au/.
(12) Abhijit Singh, "How India, too, is on a quest for undersea dominance, to counter the Chinese navy's growing presence," *Observer Research Foundation*, August 31, 2018, https://www.orfonline.org/research/43742-how-india-too-is-on-a-quest-for-undersea-dominance-to-counter-the-chinese-navys-growing-presence/.
(13) "Adamya AUV: India's Submarine launched Autonomous Underwater Vehicle," *Defence Update*, https://defenceupdate.in/adamya-auv-indias-submarine-launched-autonomous-underwater-vehicle/.
(14) "Indian Navy to Procure Unmanned Surface Vehicles and Autonomous Underwater Vehicles," *Defpost*, July 20, 2018, https://defpost.com/indian-navy-procure-unmanned-surface-vehicles-autonomous-underwater-vehicles/.
(15) HI Sutton, "Chinese HSU-001 LDUUV – Large Displacement Unmanned Underwater Vehicle," *Covert Shores*, October 2, 2019, http://www.hisutton.com/Chinese_LDUUV.html.
(16) David R. Strachan, "China Enters the UUV Fray," *The Diplomat*, November 22, 2019, https://thediplomat.com/2019/11/china-enters-the-uuv-fray/.
(17) HI Sutton, "New Intelligence: Chinese Copy of US Navy's Sea Hunter USV," *Naval News*, September 25, 2020, https://www.navalnews.com/naval-news/2020/09/new-intelligence-chinese-copy-of-us-navys-sea-hunter-usv/.
(18) HI Sutton, "New Evidence of China's Copy of US Navy Sea Hunter USV," *Covert Shores*, September 25, 2020, http://www.hisutton.com/Chinese-Navy-Sea-Hunter-USV.html.
(19) Jeffrey Lin and P.W. Singer, "The Great Underwater Wall of Robots: Chinese exhibit shows off Sea Drones," *Popular Science*, June 22, 2016, https://www.popsci.com/great-underwater-wall-robots-chinese-exhibit-shows-off-sea-drones/.
(20) US Department of Defense, *Military and Security Developments Involving the People's Republic of China 2020*, pp. vii.
(21) Rick Joe, "Whispers of 076, China's Drone Carrying Assault Carrier," *The Diplomat*, August 21, 2020, https://thediplomat.com/2020/08/whispers-of-076-chinas-drone-carrying-assault-carrier/.

Integrating Unmanned Platforms and Enabling Tech in India's Warfighting Doctrine

B.S. Dhanoa

The very recent conflict in Nagorno Karabakh has exposed the vulnerability of tracked weapons platforms and other unprotected ground targets to detection and engagement by unmanned aerial vehicles (UAVs) using an array of sensors and precision weapons on board (1). Such capability, earlier limited to only advanced militaries, is increasing rapidly. Today a plethora of means is on hand to military commanders to remotely deliver ordnance on target by air-, ground- and sea-borne weapons platforms. Rapid advances in detection and engagement capabilities, coupled with remotely controlled aerial loitering platforms that are difficult to detect, have made the task of striking targets in inaccessible locations relatively easier, while counters to such attacks have been slow to develop. Similar, yet slower, advances in the use of unmanned ground vehicles/platforms (UGVs) by troops have been in the offing for some time now. To paraphrase *Star Trek*, 'land is the final frontier' for the deployment and effective use of unmanned platforms. This is so as there are several unique challenges that UGVs face, the most obvious being the operating environment's complexity. Ground

vehicles operate in a cluttered and unpredictable environment containing obstacles that are unknown at any detailed level before the mission (2).

Ongoing tensions with China have highlighted the technological asymmetry between the Indian Armed Forces and our northern adversary (3). It is glaring when it comes to the fielding of high-end drones (for intelligence and reconnaissance, or targeting), leveraging of space and cyber capabilities in a theatre of interest, and an extensive use of electronic warfare means to deny the electromagnetic spectrum to the other side while protecting friendly systems. If the military does not keep a laser-like focus on the likely changes that rapid advances in computers (artificial intelligence or AI, machine learning and the ability to quickly process a vast quantum of data), robotics, wireless battlefield networks and sensor-driven weapons can—and will—bring to the coming fight, they will probably be severely handicapped on any future battlefield. While the challenges of maintaining and sustaining legacy forces consume the minds of most force planners, technology and the rapid introduction of "game-changing" weapons systems wait for none. Thus, it is necessary to have a dedicated future force team of thinkers, scientists and planners, civil as well as military, who are given executive authority to crystal gaze, broadly outline the likely contours of conflict in the coming decades, and identify possibilities of developing and integrating new technology weapons that will ensure that the military is not disadvantaged in any potential scenario. It will require a whole of government effort to be abreast of China in this field.

How does a mostly industrial-age army, with an uneven distribution of modern and high-tech weapons systems, manage to predict its future needs and ensure their development, induction and integration? It is not an easy task. In 2016, the Indian Army set up the Army Design Bureau (ADB) to plan for the upgrade of present systems and enunciate future technological needs (4). A formal interface with industry and academia has been established to get the best Indian minds and research facilities involved in military technology

development. Fundamental research by the Defence Research and Development Organisation (DRDO) and its affiliates is also closely interwoven into the process by the ADB. From this model, through a statement of future needs by different components of the army, the Indian Army hopes to project and develop future weapons systems, with unmanned platforms probably at the very top of the priority list.

A fair understanding of the complexity of developing and fielding UGVs is necessary to grasp the issues the Indian Army will face. The development of unmanned platforms is not new, yet it has taken the most brilliant minds in corporations like Tesla, Google and Microsoft to field prototypes of driverless cars, given the difficulty of safe autonomous navigation through the relatively benign yet continuously changing environment that cities present. Now imagine a military UGV operating in unknown complex terrain with different mission sets. Powerful algorithms will have to place the vehicle in a given threat posture in moments, sensing and overcoming any difficulty, while AI-driven engines will amalgamate the feeds of different surveillance sensors onboard, interpret the intelligence picture presented and activate its suite of weapons (an iteration of the OODA loop done many times over in a second). This may sound like science fiction, but it is the holy grail of convergence of disparate technologies—powerful AI engines, robotics, electro-optics, micro-sensors, 5G and satellite navigation—that have thus far only been tested in laboratories but are now being fielded in future force testbeds set up by most advanced militaries, including the US, Russia and China.

A glance at some of the ground platforms currently being field-tested may be instructive to understand their possible usage and determine an approach that India can adopt for eventual induction. Russia and the US are following proven methodologies for unmanned platforms—design, prototype, test, field. The US Army, under the Combat Capabilities Development Command, has the lead in this regard and the types of unmanned ground systems under development are legion; the most recent induction for use by the field army is

the QinetiQ Inc. and Pratt Miller Defense Robotic Combat Vehicle-Light, a purpose-built hybrid electric unmanned ground combat vehicle (5). Russia has battle-tested the Uran-9 unmanned ground combat vehicle in Syria in 2018 and formally inducted it in its ground force in 2019 (6). The Chinese have also been keeping pace with their development of unmanned ground systems and have introduced Norinco's Sharp Claw UGV, which was first unveiled at the Airshow China 2014 exhibition in Zhuhai, into the People's Liberation Army (PLA) in April 2020 (7). Each of these three UGVs can perform a variety of tasks—from intelligence, surveillance and reconnaissance (ISR) to fire support and even logistics delivery or casualty evacuation—within their operating parameters.

In India, the DRDO has developed and fielded remotely operated vehicles for several military tasks, from explosive ordnance detection and disposal to chemical, biological, radiological and nuclear reconnaissance, and these have been inducted in restricted numbers into the field army with specialist units (8). It is a small yet significant step to allow troops to gain experience with such platforms in their midst. However, any significant development of a remotely (or autonomously) operated weapons platform (micro, small, medium or heavy) has yet to see any progress outside the research environment, as is the case with the Muntra platform based on an ICV (BMP-II) or the wheeled (Honda CRV based) vehicle for use in urban terrain (9,10). UGV design and fielding of prototypes in India is almost entirely a defence research-led initiative, with some anticipation of eventual exports. The digital and support ecosystem existing in the army's field formations will be hard put to fully exploit any worthwhile capabilities of UGVs until an upgrade of the wireless network and digital battlespace needed to make UGV operations worthwhile is not fielded.

Some of the major technical challenges that scientists face in meeting military requirements for unmanned platforms, especially ground-based ones, are:

- Range of operating independently from a base is very limited, depending on terrain and the signal's fidelity in an operating space
- Successful and tactical negotiation of numerous obstacles, on the way and in a hostile area, are problematic for UGVs
- Loss of positional awareness of unmanned platforms due to jamming or spoofing of satnav signals, which are essential for onboard or remotely guided navigation
- Payloads that can be carried are limited to the vehicle configuration and its power plant type and size (from internal combustion engines to electrical motors and batteries)
- Power generation noise onboard for heavy UGVs and a requirement of frequently recharging the batteries of small and medium-sized unmanned vehicles remains an issue
- Identification of friend or foe is an ongoing hurdle for autonomous vehicles
- Frequent stoppages and breakdowns in onboard electro-optic sensor suites and weapons render such platforms inoperable at crucial junctures

The induction of UGVs, especially autonomous ones, is unlikely without the Indian Army going through a painful developmental phase. Despite the need for integral UAVs (of all sizes and types) in the military, India is yet to see these being inducted in substantial numbers and employed in an integrated manner across the spectrum of threats. The mainstay for the army has been the Searcher and Heron series of UAVs purchased from Israel, purely for ISR, while indigenous development remains on the backburner. The much-touted Rustom series, a DRDO project for ISR and combat (though which weapons are to be integrated is unclear), have had their own birthing pangs for some time now (11). On the other hand, China, and its weapons' largesse recipient Pakistan, have inducted and operated the CH series of reconnaissance and armed UAVs with growing confidence, with the PLA even integrating them into its war-fighting philosophy of the future (12,13).

The way ahead is not an easy one, but it needs to be mapped and enunciated now. India cannot be threatened by new ways

of waging war, of which it is informed endlessly but is incapable of countering with a cogent technological and doctrinal response. There are enough indicators available that unmanned systems are going to play a crucial part on the future battlefield. The threat of drone swarms overwhelming a legacy system such as an integrated missile air defence network or even an aircraft carrier at sea can no longer be ignored. India's armed forces need to do their own thinking and red teaming for such scenarios. They must give a coherent yet broad-based needs statement to the defence research establishment now, rather than have to force fit independent weapons and systems developed by the DRDO into their doctrine (which has mostly been the case so far).

In sum, the army must: look at the threats and needs of the future battlefield now, especially for unmanned systems; field an inter-agency and intra-government task force headed by a designated transformation czar; get their teams to deliberately prepare and follow up on a national and military needs paper for future systems; and integrate all the different strands of development (government and private) into a purposeful research and development project that has achievable milestones. India has the capacity, intellect, and research facilities within and outside of government to develop and field such systems faster than ever before. It should not field stand-alone systems in a piecemeal fashion if the desire is to address the forces' needs for unmanned systems in a holistic manner. If the nation's defence ecosystem needs a stimulus to hasten development, it should be intellectually driven from within and not be forced upon it because of an external threat.

Endnotes

(1) "Armenia, Azerbaijan and Russia Sign Nagorno-Karabakh Peace Deal," BBC, November 10, 2020, https://www.bbc.com/news/world-europe-54882564.

(2) National Research Council, Autonomous Vehicles in Support of Naval Operations, Washington DC, The National Academies Press, 2005, https://doi.org/10.17226/11379.

(3) Rajat Pandit, "India and China Locked in Stalemate over Troop Disengagement in Eastern Ladakh," The Times of India, November 27, 2020, https://timesofindia.indiatimes.com/india/india-and-china-locked-in-stalemate-over-troop-disengagement-in-eastern-ladakh/articleshow/79434354.cms.
(4) "Indian Army Sets up Design Bureau to Promote Production of Home-Grown Weapons: All about It," India Today, September 2, 2016, https://www.indiatoday.in/education-today/gk-current-affairs/story/army-design-bureau-338785-2016-09-02.
(5) "QinetiQ and Pratt Miller Deliver First Robotic Combat Vehicle - Light to U.S. Army," QinetiQ, November 11, 2020, https://www.qinetiq.com/en-us/news/first-robotic-combat-vehicle-light.
(6) Yury Laskin, "URAN-9 Unmanned Combat Ground Vehicle," European Security & Defence, August 9, 2019, https://euro-sd.com/2019/08/news/14287/uran-9-unmanned-combat-ground-vehicle/.
(7) Juan Ju, "Norinco's Sharp Claw I UGV in Service with Chinese Army," Janes, April 15, 2020, https://www.janes.com/defence-news/news-detail/norincos-sharp-claw-i-ugv-in-service-with-chinese-army.
(8) "Robotics," Defence Research and Development Organisation (DRDO), https://www.drdo.gov.in/robotics.
(9) Arun Mathew, "India's DRDO Unveils Muntra Unmanned Armoured Vehicle," DefPost, July 29, 2017, https://defpost.com/indias-drdo-unveils-muntra-unmanned-armoured-vehicle/.
(10) Dmitry Fediushko, "India Unveils First Multipurpose Wheeled UGV," European Defence Review Magazine, February 8, 2020, https://www.edrmagazine.eu/india-unveils-first-multipurpose-wheeled-ugv.
(11) Shishir Gupta, "DRDO's Rustom-2 Drone Takes-off, India Goes for Armed Heron," Hindustan Times, October 10, 2020, https://www.hindustantimes.com/india-news/drdo-s-rustom-2-drone-flight-tested-india-goes-for-armed-heron-uavs/story-CZ5jd9tRo6Ph2jcq2HOpmM.html.
(12) "Pakistan Bulk Buying Chinese Version Of MQ-9 'Reaper' Drones From Beijing – Reports," EurAsian Times, August 17, 2020, https://eurasiantimes.com/pakistan-bulk-buying-chinese-version-of-mq-9-reaper-drones-from-beijing-reports/.
(13) Michael S. Chase, Kristen Gunness, Lyle J. Morris, Samuel K. Berkowitz, and Benjamin Purser, Emerging Trends in China's Development of Unmanned Systems, Santa Monica, CA, RAND Corporation, 2015, https://www.rand.org/pubs/research_reports/RR990.html.

Future of Autonomous Air Platforms in the Indo-Pacific

Justin Bronk

Since 2010, China's People's Liberation Army Air Force (PLAAF) has undergone rapid modernisation and capability growth, posing an increasingly serious challenge to the established capabilities of the Japan Air Self Defence Force (JASDF), the Indian Air Force (IAF) and US Indo-Pacific Command assets. A core part of this modernisation has involved developing a range of modern, multirole fighter aircraft, modern sensors, air-launched munitions and datalinks (1). However, the active development of survivable, low-observable unmanned air systems (UAS) is one aspect of PLAAF modernisation that has typically received less attention than fast jets.

China has developed a wide range of UAS in the remotely piloted air system (RPAS) category, such as the CH-4, Wing Loong and Wing Loong II. However, RPASs such as these are generally unsuitable for state-on-state warfighting because they rely on either direct radio-line-of-sight or satellite communications up/downlinks for control in flight. Both control mechanisms are relatively easy for modern state adversaries to detect,

disrupt and/or override using electronic warfare equipment (2). As a result, UAS designed for operations in high-intensity warfighting scenarios against modern military forces are often grouped into a separate class of weapon systems—unmanned combat aerial vehicles (UCAVs). To be clear, UCAVs are different from RPAS such as the Wing Loong or MQ-9 Reaper. Unlike those systems, UCAVs are designed with very low-observable features to minimise radar and heat signatures, and fly pre-programmed sorties with a high-degree of in-flight autonomy to be able to operate in heavy-electronic warfare conditions. They offer considerable advantages compared to piloted aircraft in certain mission sets.

True UCAVs fly pre-programmed missions with operators to monitor, authorise and re-task them in flight when connectivity allows, rather than being remotely flown. As such, they require trained operators, but not pilots in the traditional sense. This is highly significant, since it reduces the requirement for airframes to train new pilots, and to provide pilots in frontline units with regular training flying hours to maintain currency. A high proportion of the expensive hours flown by fast jets is for pilot training rather than for major exercises or live operations. Without this requirement, a UCAV force will be significantly cheaper to operate and the airframes themselves could be built to lower structural fatigue life standards, saving weight and cost. High-level automation is unlikely to be sufficiently advanced to allow UCAVs to perform many of the peacetime missions currently conducted by combat aircraft—especially quick reaction alert scrambles, airspace probing and close-air support of friendly ground forces—for the foreseeable future. However, for high-intensity mission sets where rules of engagement and target identification parameters are relatively straightforward, such as suppressing enemy air defences, deep strike against fixed targets and even offensive counter-air missions in a major conflict, UCAV technology is extremely promising.

Leaked information suggests that multiple different potential UCAV programmes are supposedly being developed for the PLAAF. The first, and seemingly most mature, is the Hongdu

GJ-11. GJ stands for *gōng jī*, which roughly translates to 'attack', suggesting that penetrating strike is the intended primary role. The GJ-11 has been in flight testing since at least 2013, and a mock-up with significantly improved stealth features was shown off at the 70th-anniversary parade of the Chinese Communist Party (CCP) in 2019 (3). The airframe is a flying wing design with a single buried engine, most likely with subsonic performance and provision for internal weapons in the 2000lb class (4). Given an efficient turbofan powerplant and its low drag configuration, an operational GJ-11 will most likely have an impressive range on internal fuel—sufficient to threaten targets far from the Chinese mainland. Furthermore, the tailless flying wing shape offers the potential for broadband all-aspect stealth, far beyond current possibilities for stealth fighters such as the J-20A. This, however, requires Chinese manufacturers to solve the many engineering difficulties inherent in mounting low probability of intercept/detect sensors, heat exchangers and communications arrays within a clean operational airframe. To have a credible strike capability against defended American, Japanese or Indian targets at reach will also require the ability to fly to those targets, scan for and detect key aiming points, and release weapons within guidance parameters without real-time human control. While such levels of lethal autonomy in flight might sound extremely radical, the fact remains that modern cruise missiles, loitering munitions and anti-ship missiles have had similar autonomous navigation, target acquisition, prioritisation and attack capabilities for well over a decade. The CCP's enthusiastic development of artificial intelligence technologies in multiple defence and security fields, and determination to close the military capability gap with the US in the Indo-Pacific mean that the country is unlikely to restrict itself from developing promising, cheap and capable strike UCAVs with these capabilities on the basis of ethical or legal concerns.

In addition to the GJ-11, several other outwardly similar flying-wing or cranked kite demonstrators and mock-ups have been displayed or leaked in recent years, including the China Aerospace Science and Industry Corporation Tian Ying and China Aerospace Science and Technology Corporation CH-7 (5).

These offer additional pathways to be developed into viable low-observable strike and/or intelligence, surveillance and reconnaissance (ISR) UCAVs, with some indications that the Tian Ying in particular might be considered for operations off future catapult take-off but arrested recovery aircraft carrier designs (6). The US Navy has already shown that carrier operations are possible for this class of vehicle in trials with the Northrop Grumman X-47B cranked kite UCAV demonstrator (7). Having multiple parallel UCAV development programmes being undertaken by different aerospace manufacturers is well in line with Chinese practice across a range of other weapons systems. With few limits on funding availability, this approach maximises the likelihood of viable operational capabilities being produced, even if some fail to meet the required standards. This multiple-track development approach also increases the likelihood that at least some Chinese UCAV designs will find buyers on the export market in the Indo-Pacific and beyond, just like the CH-4 and Wing Loong series RPAS.

A wild card is the so-called 'Dark Sword' UCAV, which may or may not be an actual development programme. The UCAV was teased in a supposedly leaked photograph showing what appeared to be a demonstrator airframe or mock-up shaped for agility and supersonic flight (8). Such a design could enable a UCAV to match traditional fast jets' performance and flight characteristics more easily, suggesting that the Dark Sword could be a prototype 'loyal wingman' system intended to operate alongside piloted fast jets to provide additional weapons, sensors and tactical options in combat. However, no significant further information has been disclosed about the project, so the leaked photograph could simply have been a mock-up designed to mislead foreign intelligence services. On the other hand, loyal wingman type UCAV development programmes are underway in Australia, the US and the UK, suggesting that the Dark Sword will not be a technological outlier if it is indeed a genuine programme (9,10,11).

The clear conclusion is that, within the coming decade, the PLAAF and possibly the People's Liberation Army Naval Air

Force will begin to field several operational UCAV designs with significant degrees of lethal automation and broadband stealth for strike, ISR and potentially offensive counter-air operations in highly contested airspace. These assets are unlikely to match the flexibility and raw combat power of the latest fast jet designs but will be significantly cheaper to build and operate. They are also likely to be considerably easier to train operators for than piloted fast jets, further removing barriers to rapid force growth. Whilst countries threatened by Chinese military developments might not wish to develop armed UCAV capabilities, they will need to have credible military solutions to a PLAAF that fields them at scale.

Endnotes

(1) Justin Bronk, "Russian and Chinese Combat Air Trends: Current Capabilities and Future Threat Outlook," RUSI Whitehall Reports, October 30, 2020, https://www.rusi.org/sites/default/files/russian_and_chinese_combat_air_trends_whr_final_web_version.pdf

(2) The Iranian capture of a US Air Force RQ-170 Sentinel stealth ISR RPAS in 2011 is an excellent example of this vulnerability: John Keller, "Iran–U.S. RQ-170 incident has defense industry saying 'never again' to unmanned vehicle hacking," Military & Aerospace Electronics, May 3, 2016, https://www.militaryaerospace.com/computers/article/16715072/iranus-rq170-incident-has-defense-industry-saying-never-again-to-unmanned-vehicle-hacking

(3) Joseph Trevithick, "China Showcases Stealthier Sharp Sword Unmanned Combat Air Vehicle Configuration," The Warzone, October 1, 2019, https://www.thedrive.com/the-war-zone/30111/china-showcases-stealthier-sharp-sword-unmanned-combat-air-vehicle-configuration

(4) Andreas Rupprecht, Modern Chinese Warplanes (Houston, TX: Harpia, 2020), p. 105.

(5) Joseph Trevithick and Tyler Rogoway, "China's Biggest Airshow Offers More Evidence Of Beijing's Stealth Drone Focus," The Warzone, November 2, 2018, https://www.thedrive.com/the-war-zone/24645/chinas-biggest-airshow-offers-more-evidence-of-beijings-stealth-drone-focus

(6) Tyler Rogoway, "China's Reported Plan To Deploy Weaponless Stealth Drones On Its Carriers Make Perfect Sense," The Warzone, September 25, 2019, https://www.thedrive.com/the-war-zone/30020/china-deploying-a-weaponless-stealth-drone-on-its-carriers-makes-perfect-sense
(7) Northrop Grumman,"X-47B UCAS Makes Aviation History…Again", https://www.northropgrumman.com/what-we-do/air/x-47b-ucas/
(8) Chen Chuanren, "China Reveals a Supersonic UCAV," AIN Online, June 12, 2018, https://www.ainonline.com/aviation-news/defense/2018-06-12/china-reveals-supersonic-ucav
(9) Greg Waldron, "Boeing Australia 'loyal wingman' conducts first taxi test," Flight Global, October 22, 2020, https://www.flightglobal.com/military-uavs/boeing-australia-loyal-wingman-conducts-first-taxi-test/140738.article
(10) Garrett Reim, "US Air Force launches Skyborg competition, artificial intelligence for loyal wingman UAV," Flight Global, May 18, 2020, https://www.flightglobal.com/military-uavs/us-air-force-launches-skyborg-competition-artificial-intelligence-for-loyal-wingman-uav/138426.article
(11) Craig Hoyle, "Dstl nears decision on LANCA flight demonstration for UK," Flight Global, June 30, 2020, https://www.flightglobal.com/flight-international/dstl-nears-decision-on-lanca-flight-demonstration-for-uk/138929.article

ASATs: A Growing Response to PLA Space Capabilities

Rajeswari Pillai Rajagopalan

In March 2019, India conducted an anti-satellite (ASAT) missile test (code-named Mission Shakti), targeting a live satellite at 300 km (1,2). The test was a direct but careful response rather than a knee-jerk reaction to China's first successful ASAT test in January 2007. But this will not end here. Countries like Israel are believed to have this capability, and with growing space security competition, more countries will likely go down this path as well. From an Indian perspective, the space security threats that China presents is real and cannot be ignored. China has compelled a significant shift in India's space policy strategy, moving away from a moralistic and principled approach on outer space governance to one that is dictated by pragmatism and national security considerations. But Mission Shakti is far from adequate to produce the desired deterrent capability vis à vis China (3).

PLA's Military Space Activities a Key Driver

While China has continued with its rhetoric of peaceful uses of outer space and is pushing for treaty mechanisms such as the draft 'Treaty on the Prevention of the Placement of Weapons in Outer

Space, the Threat or Use of Force against Outer Space Objects' (PPWT), its pursuit of counterspace capabilities, including ASAT missiles, is inherently destabilising and has remained a concern for India and other major spacefaring powers. China's first successful ASAT test in 2007 has been followed by several more, termed by Beijing as 'missile defence tests' to avoid international criticism. Advanced militaries such as the US are heavily networked, with a greater dependence on space, making them vulnerable. China has been investing in counterspace capabilities to deny the US any advantage it may accrue from space use. Having studied the previous major military operations—the two Gulf Wars, Kosovo and the Afghanistan operation—China looks at the US's heavy reliance on space as a vulnerability that it can exploit during a crisis. China has concluded that the US "is inordinately dependent on its complex but exposed network of sophisticated command, control, communications and computer-based intelligence, surveillance and reconnaissance systems operating synergistically in and through space" (4). China's ASAT demonstration was an effort at developing an anti-access strategy against the US. But as the People's Liberation Army (PLA) becomes more space-reliant and networked in its military operations, Beijing's vulnerability also increases.

From an Indian perspective, Beijing's competencies in space and counterspace capabilities and the way it has undertaken the institutional reorganisation to strengthen the role of these capabilities have important national security consequences. The establishment of the PLA Strategic Support Force (PLASSF) indicates that the PLA is assigning greater roles for space, electronic warfare and cyber in military operations. The PLASSF is particularly notable for how these warfare capabilities are integrated under this single command. Over the last ten years, China has made significant investments in ASATs and electronic and cyber warfare capabilities to disrupt, damage, and deny access to space by destroying space objects consequential in military operations. The weapon systems that China has developed include direct ascent anti-satellite (DA-ASAT) weapons, high-powered lasers, co-orbital satellites, directed energy weapons, electronic jamming and spoofing, and cyber

means. Many recent studies have highlighted the growing maturity of China's counterspace capabilities and detail how the country has an entire range of weapons capable of targeting satellites from the ground up to geosynchronous orbit (GEO) (5) China's repeated ASAT tests have helped it develop the technology to such a sophisticated level that a recent report asserts that the "Chinese-ASAT capability against LEO targets is likely mature and likely operationally fielded on mobile launchers. Chinese DA-ASAT capability against deep space targets — both Medium Earth Orbit (MEO) and GEO — is likely still in the experimental or development phase" (6). China's May 2013 ASAT test was significant as it reached up to the geostationary orbit (GEO), where all the military communications, early warning and intelligence, surveillance and reconnaissance (or ISR) satellites usually orbit (7,8). China has also conducted ASAT tests using a DN-3 ASAT missile, which can go to higher orbits (9); Beijing has reportedly tested this missile system in October 2015, December 2016, August 2017 and February 2018 (10). China possibly also has a submarine-based ASAT missile, capable of hitting US satellites in GEO (11).

There have also been some notable shifts on China's counterspace capabilities front. The Center for International and Strategic Studies 2020 report on counterspace capabilities has observed that China has possibly "paused, or at least slowed" its testing of kinetic weapons (12). The authors assume that this may be either because China has mastered the technologies or because those tests bring in too much of international scrutiny. On the other hand, China appears to be devoting considerable attention to non-kinetic counterspace capabilities including rendezvous proximity operations, including a range of remote space operations. There has also been a spike in incidents of dazzling or blinding (satellites) involving lasers, electronic jamming and spoofing, all targeting space systems. China has devoted significant attention and resources to developing electronic and cyber warfare means in space as they offer some important benefits, plausible deniability being the most attractive. They are also cheaper, the entry barrier is quite low, and attribution is extremely hard. Navigation satellites such

as civilian GPS have been a favorite target as the military ones come with robust measures as protection from such attacks (13). China's means to jam and target communication satellites are also well known. Following the US drone attack on Iranian major general Qasem Soleimani in January 2020, a Chinese military analyst said that "China would be able to shoot down the drone with its air defenses and, as an added layer of defense, could conduct a "soft kill" by jamming the drone's communications and GPS" (14). China is known to have used electronic and cyber warfare means against space assets in several instances (15). Along with the capability development, China's streamlining of institutions such as through the PLASSF, combining space with other services, has been significant.

Russia's counterspace activities have not gone unnoticed either. In July 2020, the US Space Command said that Russia had "conducted a non-destructive test of a space-based anti-satellite weapon" (16). The statement detailed that Russia had released "a new object into orbit from Cosmos 2543" in the close vicinity of another Russian satellite on 15 July 2020. Russia had undertaken a similar activity in 2017 as well (17). In April 2020, Russia had also conducted an ASAT test.

Regional Responses

India is not the only country that is pursuing counterspace capabilities to develop a deterrent ability against China. Japan has also been concerned about growing space security threats from China and Russia (18,19,20,21). Both Beijing and Moscow have invested and tested several counterspace capabilities to disrupt, deny, disable and even destroy space systems. For instance, China's space robotic arm and ASAT missiles have figured in many Japanese security discussions (22). Russia's continuing ASAT tests have also been worrying Japan, and have prompted Tokyo to respond appropriately to guard its space assets. In May 2020, Japan launched a new defence space unit within the Air Self-Defense Force (ASDF), called the Space Operations Squadron, with the primary goal of protecting the country's space assets and monitoring armed attacks, and to

track space debris, satellites and meteorites to avert satellite collisions (23). The new institution will be based at the ASDF Fuchu base in Tokyo and will become operational in 2023 (24). According to experts, the establishment of the Squadron is a clear sign of the greater salience of space in Japan's overall security calculations (25). The December 2018 National Defense Program Guidelines outlined that the new institution's role will be "to ensure superiority in use of space during peacetime and armed contingencies" (26). However, the contested nature of outer space politics and use of counterspace capabilities have made Japan cautious with the guidelines seeking "to strengthen capabilities including mission assurance capability and capability to disrupt opponent's command, control, communications and information." According to former defence minister Taro Kono, the new Squadron will also actively work with the US Space Command on the external front and with the Japan Aerospace Exploration Agency on the inside (27). Japan also has plans to develop its own interceptor in the next few years to have the option to counter-attack satellites should its space assets come under attack (28).

France, another key Indian security partner, has also had to respond to the worsening security scenario in the space realm. Paris has brought in significant changes to its space policy in response to developments that are seen as compromising France's "freedom of access to and action in space" (29). The new strategy has envisioned many institutional changes, and national space governance has accordingly been reviewed and located within a Space Command under the French Air Force (30). Significantly, France is set to invest €700 million, in addition to the €3.6 billion already allotted, for military space between 2019 and 2025 to augment its surveillance and self-defence capabilities in space (31).

Outer space is witnessing an increasing destabilisation and escalatory actions including ASAT tests, cyber and electronic warfare, and even an actual kinetic weapon test in space. This means that major space powers such as the US, Japan, France and India will invest in developing a series of countermeasures to

negate the impact of Russia and China's growing counterspace capabilities. India's 2019 ASAT test may only be the beginning of the countermeasures that are required to protect the country's assets. But the major defensively-oriented Indo-Pacific space powers need to forge closer space technology partnerships to offset the negative consequences of space weaponisation.

Endnotes

(1) NDTV, "Assure World ASAT Won't Be Used Against Any Country: PM Modi," YouTube video, March 27, 2019, https://www.youtube.com/watch?v=EZzxHJ9B_d0

(2) Ministry of External Affairs Media Center, Government of India, "Frequently Asked Questions on Mission Shakti, India's Anti-Satellite Missile test conducted on 27 March 2019," March 27, 2019, https://www.mea.gov.in/press-releases.htm?dtl/31179/Frequently_Asked_Questions_on_Mission_Shakti_Indias_AntiSatellite_Missile_test_conducted_on_27_March_2019

(3) Ashley J. Tellis, "India's ASAT Test: An Incomplete Success," Carnegie Endowment for International Peace, April 15, 2019, https://carnegieendowment.org/2019/04/15/india-s-asat-test-incomplete-success-pub-78884

(4) Ashley J. Tellis, "China's Military Space Strategy," Survival, 49:3, 2007, http://dx.doi.org/10.1080/00396330701564752

(5) The US Defense Intelligence Agency's publication, Challenges to Security in Space; Project 2049 Institute's China's Space and Counterspace Capabilities and Activities; Secure World Foundation's (SWF) Global Counterspace Capabilities: An Open Source Assessment; Center for Strategic and International Studies' Space Threat Assessment 2020 and a RAND study, "The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations," authored by Kevin L. Pollpeter, Michael S. Chase and Eric Heginbotham are some of the recent works that have detailed China's space and counterspace capabilities.

(6) Brian Weeden and Victoria Samson, Global Counterspace Capabilities: An Open Source Assessment, Secure World Foundation, April 2020, https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf

(7) Zachary Keck, "China Secretly Tested an Anti-Satellite Missile," The

Diplomat, March 19, 2014, https://thediplomat.com/2014/03/china-secretly-tested-an-anti-satellite-missile/

(8) Mike Gruss, "Pentagon Says 2013 Chinese Launch May Have Tested Antisatellite Technology," Space News, May 14, 2015, https://spacenews.com/pentagon-says-2013-chinese-launch-may-have-tested-antisatellite-technology/

(9) It must be noted that while the media has tended to use the DN (Dongneng) designator, there are still unresolved questions about the actual designator for the missile or what China actually called it.

(10) Bill Gertz, "China ASAT Test Part of Growing Space War Threat," The Washington Free Beacon, February 23, 2018, http://freebeacon.com/national-security/asat-test-highlights-chinas-growing-space-warfare-capabilities/, cited in Todd Harrison, Kaitlyn Johnson and Thomas G Roberts, Space Threat Assessment 2018, Center for International and Strategic Studies (CSIS), April 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180412_Harrison_SpaceThreatAssessment_FULL_WEB.pdf?0YxNhtucgT6o6g5I7yqeBaL7CB6mBZEu

(11) Ian Easton, "The Great Game in Space: China's Evolving ASAT Weapons Programs and Their Implications for Future US Strategy," Project2049 Institute, May 2018, https://project2049.net/wp-content/uploads/2018/05/china_asat_weapons_the_great_game_in_space.pdf

(12) Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, Tyler Way and Makena Young, Space Threat Assessment 2020, Center for International and Strategic Studies (CSIS), March 2020, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200330_SpaceThreatAssessment20_WEB_FINAL1.pdf?6sNra8FsZ1LbdVj3xY867tUVu0RNHw9V

(13) Brian Weeden (@brianweeden), "Two points: 1) this is all about civil GPS signals (military signals are much more robust) 2) the DOD could have done more to prevent spoofing of civil GPS, but has not 3) Galileo, BeiDou & QZSS will all help, but not prevent it completely (see #2)," Twitter, 3:34 AM, December 18, 2018, https://twitter.com/brianweeden/status/1074787323357876229

(14) Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, Tyler Way and Makena Young, Space Threat Assessment 2020, Center for International and Strategic Studies (CSIS), March 2020, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200330_SpaceThreatAssessment20_WEB_FINAL1.pdf?6sNra8FsZ1LbdVj3xY867tUVu0RNHw9V

(15) Rajeswari Pillai Rajagopalan, "Cyber and Electronic Warfare in Outer Space," Space Dossier 3, The United Nations Institute for Disarmament Research (UNIDIR), May 2019, https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf

(16) US Space Command Public Affairs Office, "Russia conducts space-

based anti-satellite weapons test," July 23, 2020, https://www.spacecom.mil/MEDIA/NEWS-ARTICLES/Article/2285098/russia-conducts-space-based-anti-satellite-weapons-test/
(17) Nathan Strout, "Russia conducted anti-satellite test in space, says US Space Command," Defense News, July 23, 2020, https://www.defensenews.com/battlefield-tech/space/2020/07/23/russia-conducted-anti-satellite-test-in-space-says-us-space-command/
(18) Mark Stokes, Gabriel Alvarado, Emily Weinstein, and Ian Easton, "China's Space and Counterspace Capabilities and Activities," Study prepared for The U.S.-China Economic and Security Review Commission, March 30, 2020, https://www.uscc.gov/sites/default/files/2020-05/China_Space_and_Counterspace_Activities.pdf
(19) Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, Madison Bergethon and Alexandra Coultrup, Space Threat Assessment 2019, Center for Strategic and International Studies (CSIS), April 2019, https://aerospace.csis.org/wp-content/uploads/2019/04/SpaceThreatAssessment2019-compressed.pdf
(20) Brian Weeden and Victoria Samson, eds., Global Counterspace Capabilities: An Open Source Assessment, Secure World Foundation, April 2019, https://swfound.org/media/206408/swf_global_counterspace_april2019_web.pdf
(21) Defense Intelligence Agency, Challenges to Security in Space, January 2019, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf
(22) Daniel Darling, "Japanese Government Considers Launching a Satellite Interceptor," Defense & Security Monitor, August 26, 2019, https://dsm.forecastinternational.com/wordpress/2019/08/26/japanese-government-considers-launching-a-satellite-interceptor/
(23) "Japan launches new squadron to step up defense in outer space," Japan Times, May 18, 2020, https://www.japantimes.co.jp/news/2020/05/18/national/sdf-launches-space-operations-unit/#.XsUlc5MzbOQ
(24) "Japan's new space squadron takes a giant leap forward," Japan Times, June 2, 2020, https://www.japantimes.co.jp/news/2020/06/02/national/japan-space-force-self-defense-forces/
(25) Yuka Koshino, "Japan's new Space Domain Mission Unit and security in the Indo-Pacific region," Military Balance Blog, International Institute of Strategic Studies, London, May 1, 2020, https://www.iiss.org/blogs/military-balance/2020/05/japan-space-domain-mission-unit-security
(26) Ministry of Defense, Government of Japan, "National Defense Program Guidelines for FY 2019 and Beyond," December 18, 2018, https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218_e.pdf
(27) Mari Yamaguchi, "Japan launches new unit to boost defense in space,"

The Associated Press, May 18, 2020, https://www.defensenews.com/global/asia-pacific/2020/05/18/japan-launches-new-unit-to-boost-defense-in-space/

(28) Daniel Darling, "Japanese Government Considers Launching a Satellite Interceptor," Defense & Security Monitor, August 26, 2019, https://dsm.forecastinternational.com/wordpress/2019/08/26/japanese-government-considers-launching-a-satellite-interceptor/

(29) The French Ministry for the Armed Forces, Space Defence Strategy – Report of the "Space" Working Group, 2019, https://www.defense.gouv.fr/content/download/574375/9839912/Space%20Defence%20Strategy%202019_France.pdf

(30) Xavier Pasco, "A New French Space Command," Space Alert, Observer Research Foundation, Volume VII, Issue 4, October 5, 2019, https://www.orfonline.org/research/space-alert-volume-vii-issue-4-56195/

(31) Permanent Representation of France to the Conference on Disarmament, "Florence Parly unveils the French space defence strategy," https://cd-geneve.delegfrance.org/Florence-Parly-unveils-the-French-space-defence-strategy

China's Military Technology Developments and What This Means for India

Manoj Joshi

In mid-November 2020, Jin Canrong, a respected professor of international relations at Renmin University in Beijing, made a sensational claim that Chinese troops in Ladakh had forced Indian forces from two positions in the mountain chain overlooking Spanggur Tso lake by using a microwave weapon. According to a report in *The Times* (London), the microwave radiation on two hilltops occupied by the Indian forces made them vomit, forcing them to retreat. The weapons, the professor said, were used because existing agreements forbade the use of guns in the area (1).

Most observers have dismissed the story as being part of psychological operations (PsyOps), though it is not clear why someone of Jin's reputation would make such a claim. While China does possess microwave 'direct energy weapons,' most observers wondered whether they could be effective in the conditions of Ladakh. The Indian Army dismissed the report as "fake news," though it is unlikely to have confirmed the incident had it occurred (2). The fact that by the end of 2020, the Chinese were pressing the Indians to withdraw from the heights facing

them in Spanggur Tso, suggests that no such weapon was used. True or false, the claim highlights the evolving direction of Chinese policy towards operationalising disruptive and high-tech weapons systems to gain the military edge. While the focus of its endeavour is the US, India is a collateral target.

New Delhi is acutely aware of China's pursuit of such technologies. Speaking at a webinar in early November, India's Chief of Defence Staff Bipin Rawat pointed to the development of the Strategic Support Force by the People's Liberation Army (PLA) and the capabilities it was acquiring in the space, cyber and electronic domains to conduct "intelligentised" warfare (3). A week earlier, a communique issued by the Chinese Communist Party's Central Committee said that one of the main targets of the 14th Five Year Plan (2021-2025) was to develop "disruptive" technologies to close the gap with the US. According to the *South China Morning Post*, this was the first use of the term "disruptive" where previous iterations of the Plan documents had spoken of "civil military fusion" (CMF) and the modernisation of combat forces (4).

Robert Work and Greg Grant have identified five lines of effort being undertaken by China. The first has involved extensive use of industrial and technical espionage and civil military fusion to quickly acquire key capabilities. The second is to evolve capabilities aimed at destroying or disrupting the US battle network's command, control, communications and intelligence (C3I) systems. The third is the first use of an arsenal of long-range precision guided missiles capable of targeting US C3I nodes. Fourth is developing the so-called "Assassin's Mace" capabilities that can be used to shock and surprise adversaries. And fifth is using artificial intelligence (AI) to achieve military superiority (5).

While other capabilities are deployed and visible, often deliberately so, the Assassin's Mace capacities are, by definition, hidden. They belong to the Project 995 (begun in May 1990) and are the equivalent of the US stealth capabilities that were only revealed, only by their effects, in the Second Gulf War and against Serbia. This is where directed energy weapons,

space weapons, electromagnetic railguns and high-powered microwaves come in (6).

The Chinese efforts are directed towards offsetting US technological superiority, and the US has also understood the seriousness of the Chinese intent and has begun shifting gears to deal with the situation. At one level, the US is creating a more stringent export control regime to deny China emerging technologies, and at another, it is seeking to undermine the Chinese effort by refusing permission to certain categories of Chinese students wanting to study in the US. But beyond this, it is also gearing up to compete with China by outlining its own AI strategy (7,8).

Military Technology Development in China

China's 2019 White Paper on Defence had referred to new and high-tech military technologies based on IT and the "trend to develop long range precision intelligent, stealthy or unmanned weaponry and equipment." It went on to say that "war is evolving in form towards informationized warfare, and intelligent(ized) warfare is on the horizon" (9).
Recent Chinese efforts in developing military technology have focused on, first, the absorption of western technology obtained through a variety of means then digested, assimilated and re-innovated; second, enhancing the quality of conventional systems like fighter jets, warships, armoured vehicles and so on; and third, domestic innovation focusing on futuristic areas using AI, swarming, unmanned weapons systems, directed energy weapons and quantum technology.

The PLA work focuses not just on technology, but on theories and concepts related to their application. The high-power microwave weapon was tested in 2010, followed by tests of laser weapons, railguns, electromagnetic aircraft launch systems, electrical propulsion for warships, hypersonic glide vehicles like DF 17, stealth aircraft and ships. China has made significant advances in quantum science, including the use of a satellite for communications. Chinese laboratories and institutions

and the private sector have been involved in this; a quantum information science laboratory has been built in the Anhui province. "Innovation" is the new mantra and Chinese President Xi Jinping has said that "In circumstances of increasingly intense global military competition, only innovators win" (10).

Perhaps the most important focus of military modernisation in China has been on what the PLA terms "informationisation," which utilises capabilities for information operations, including cyber warfare and PsyOps. In recent times, with the emergence of AI, this has been upgraded to the concept of "intelligentised" warfare. Elsa Kania has cited several PLA science and technology leaders on the future of "hybrid intelligence" involving human and machine intelligence (11). However, many of these systems, especially those enabled by AI and machine learning, are still some distance away from deployment. Given the investment and effort being put in, it would be prudent to anticipate systems that could have a decisive impact on the tempo of operations, as well as the reach and precision of weapons.

Another disruptive area is quantum technology, with China among the early investors, beating out even the US. Like AI, quantum technology impacts a range of areas from computing and navigation to cryptography, and its transformative impact will also affect industries like health, finance and energy. The US, Russia, EU, Canada, Australia and Israel have already invested significantly in the field (12).

Military Civil Fusion

The Chinese military's 2015 White Paper had a section on the "in-depth development of civil-military integration." This understanding was basic, but by 2015, when the Chinese came up with their ten-year technology development plan under the rubric of Made in China 2025, they became more conscious of the need to strongly associate this with military technology aims as well.

The 13th Five Year Plan (2016-2020) and the linked Next Generation Artificial Intelligence Development Plan of 2017 saw an emphasis on military-civil fusion (MCF), especially in the case of AI development.

Kania says that, for now, the MCF remains a work in progress. In her view, leading Chinese tech companies are less directly engaged in supporting defence initiatives compared to their American counterparts. It is possible that some of them hide their links to continue to do international business, but she does give the example of the collaboration between the 28th institute of the China Electronics Technology Company and Baidu to set up a laboratory to research intelligent command and control. She has also listed other companies—Ziyan, which is into drones; Kuang-Chi, which is into machine learning and military metamaterials; and Yunzhou Tech, a leader in unmanned surface vessels (13).

Overall, there is now significant synergy between government, military, private sector and research and development (R&D) institutions. There is also significant investment in R&D with a clear single-minded pursuit from the highest levels.

However, as Kania and Lorand Laskal have warned, there is a problem in overestimating and even mischaracterising Chinese MCF activity. While it may be a longer term challenge for the US and its allies, "the core threat and concern is tech transfer" (14).

Organisational Arrangements

The Chinese are conscious of how much catching up they need to do to offer effective competition to the US. To this end, they have sharply ramped up spending in the science and technology sector and undertaken deep reforms in the structures and organisations that deal with military technology.

The reforms in the PLA's organisational structure promoting greater integration and jointness that began in 2013-2014 gave a fillip to the process of MCF. This only became apparent in 2016

when the document on the "Central Military Commission [CMC] Opinions on Deepening the Reform of National Defense and the Armed Forces" was released. This detailed the wide-ranging reforms in the way the PLA was organised and deployed, and the substantial reorganisation of the offices of the CMC itself. Among the most significant moves was the creation of groups within the PLA and CMC to promote military-technical innovation. These were the Central Commission for Integrated Military and Civilian Development (CMI), the CMC Science and Technology Commission and the Military Science Research Steering Committee.

The CMI is by far the most important of the three. It is chaired by Xi and has as its vice-chairs two Politburo Standing Committee members—Wang Huning and Han Zheng. The aim of this high-powered group is to signal the importance of the issue of MCF, as well as to ensure a united approach to the issues around the subject.

The CMC's Science and Technology Commission, established in 2016, is an upgrade of an older body that was embedded in the General Armaments Department and that was involved in R&D, procurement and testing of equipment for the PLA. The new commission is one of 15 new departments that report directly to the CMC.

The Military Science Research Steering Committee has been described as a secretive entity of the CMC that was revealed in July 2017. One analyst believes that it is the Chinese equivalent of the US Defence Advanced Research Projects Agency, or DARPA, which has done much to drive technological innovation in the US since it was set up in 1958. He also believes that its principal function will be to focus on the development of AI technologies, both civilian and military (15).

Around that time, China also reorganised its three top PLA academic institutes—the Academy of Military Sciences (AMS), the National Defence University and the National University of Defense Technology. The principal role of the AMS will be to

focus on scientific research and facilitate coordination between military theory and science and technology development.

Issues for India

The challenge is for India to deal with the situation where it is a collateral target. The Indian military is not unaware of the developments. Seminars and papers have been written about disruptive technologies and their implications. India has, in recent years, undertaken a systematic analysis of the technologies, including swarms, robotics, AI big data analytics and algorithmic warfare (16). The Indian military's 2013 'Technology Perspective and Capability (TPCR) Road Map' refers to AI, robotics, electromagnetic pulse weapons and unmanned underwater vehicles, among a range of other technologies. Curiously, the 2018 iteration of the same document ignores them and focuses on the more practical and conventional technologies (17,18). It is even now not clear whether the Indian military leadership grasps the challenge of CMF. As one critic has noted, "For General Rawat (the Indian Chief of Defence Staff), civil-military fusion implies the marrying of the physical assets on the commercial and military side" such as airports, the use of commercial satellites by the military and so on (19).

In 2018, the Department of Defence Production set up a task force to study the future use of AI in defence applications. It recommended five areas of focus in AI for the armed forces—lethal autonomous weapons systems, unmanned surveillance, simulated war games and training, cyber security, aerospace security, and intelligence and reconnaissance. Based on this report, a high-level Defence AI Council was set up in 2019, and plans were made for a Defence AI Projects Agency. In parallel, the NITI Aayog (India's apex planning agency), the Ministry of Electronics and Information Technology, companies like Intel and the Tata Institute of Fundamental Research have established a Model International Centre for Transformative AI in Bengaluru (20).

India has also moved to support its quantum technology effort. After neglecting this area, in 2020, New Delhi sharply boosted its budget (US$1.5 billion for five years) to support the development of quantum technologies for communications, computing, materials development and cryptography (21). But a lot of these efforts in AI or quantum technologies are still in the planning stage.

The problem for India is that its defence industrial and R&D processes continue to function in a suboptimal fashion. It has been wrestling with its defence acquisition procedure, the latest iteration of which came out this year. The bottom line for the Defence Acquisition Procedure 2020 is to promote the indigenisation of weapons and systems, given the unconscionable dependence on imports. Unless it can straighten this out, it is unlikely to have much focus on "over-the-horizon" and disruptive technologies.

The Defence Research and Development Organisation (DRDO), India's principal military R&D agency, has just about reached the process of "re-innovation" of systems through products like the Akash surface-to-air missiles, a variety of radars and electronic warfare systems. Many of its products like the Tejas Light Combat Aircraft or the Astra and Brahmos missiles depend on foreign components. But the DRDO has not yet been able to even develop an unmanned aerial vehicle that the armed forces can use.

India's problem is that, unlike China, it has not been too good in absorbing technology from abroad, acquired legally or otherwise. The intellectual property rights of most systems it imports remains with the vendor, and this inhibits efforts towards fusion. Indeed, it often finds it difficult to marry its western imported systems with those imported from Russia.

Remarkably, in AI, the DRDO was actually a pioneer in establishing a Centre for Artificial Intelligence and Robotics (CAIR) in 1986 in Bengaluru by A. Paulraj, who did pioneering work on sonars. But in 1992, he migrated to the US and became

a professor at Stanford University. CAIR has done work in a range of areas but much of it remains laboratory bound and does not see application with the armed forces.

The basic problem is the inability of policymakers and user agencies to decide just what they want and how much they are willing to spend on it. India does have resource constraints, but it has a large spread of computer science and engineering talent and a well-developed software industry. There is little doubt that if the users could provide clarity on what they need and the resources were made available, that India could make breakthroughs in AI or robotics (22).

At a basic level, the creation of these technologies depends on the resources that a country can put down. Chinese defence spending already exceeds that of India greatly. In addition, with the MCF, the PLA can synergise a lot of the money that China is investing in civilian technology development and basic research.

The weak point of the Indian system is the lack of sustained political attention to the needs of the military. By and large, things are left to the Ministry of Defence and the armed services. This is all right if the trajectory sought is unadventurous. But for something more dramatic, a whole-of-the-system effort with the support and guidance of the apex leadership is needed. This is the kind that Xi—chairman of the Chinese Communist Party, president of the People's Republic of China, chairman of the CMC and the commander-in-chief of the Joint Operations Command Center—is providing.

Endnotes

(1) Didi Tang, "China turns Ladakh battleground with India into a 'microwave oven," *The Times*, November 17, 2020, https://www.thetimes.co.uk/article/china-turns-ladakh-battleground-with-india-into-a-microwave-oven-6tlwtrtzz

(2) Writing in Forbes, David Hambling noted that the description of the symptoms does not fit the kind of known ADS weapons but could describe something called the Electromagnetic Personnel Interdiction Control (EPIC) device.

David Hambling, "India disputes claim that China routed their troops with microwave blaster," *Forbes*, November 20, 2020, https://www.forbes.com/sites/davidhambling/2020/11/20/disputed-claim-that-china-routed-indian-troops-with-microwave-blaster/?sh=78f9643324f6

(3) "Situation at LAC tense; war with China cannot be ruled out: CDS Gen Rawat," *The Tribune*, November 6, 2020, https://www.tribuneindia.com/news/nation/chinese-military-facing-unanticipated-consequences-for-misadventure-on-lac-cds-gen-rawat-166893

(4) Kristin Huang and Liu Zhen, "China-US rivalry: Beijing banking on 'disruptive technologies' for a military edge, observers say," *South China Morning Post*, November 5, 2020, https://www.scmp.com/news/china/military/article/3108463/china-us-rivalry-beijing-banking-disruptive-technologies

(5) Robert O Work and Greg Grant, *Beating the Americans at their own game: An offset strategy with Chinese characteristics*, Center for New American Security, June 6, 2019, pp. 5-6, https://www.cnas.org/publications/reports/beating-the-americans-at-their-own-game

(6) "Beating the Americans at their own game: An offset strategy with Chinese characteristics," p. 13

(7) "Executive Order on maintaining leadership in artificial intelligence," *The White House*, February 11, 2019, https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/

(8) US Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to advance our security and prosperity*, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF
(9) The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, July 2019), p. 7
(10) Cited in Elsa B Kania, "Minds at War: China's pursuit of military advantage through cognitive science and biotechnology," *Prism* Vol. 8, No.3 (2019), p. 83
(11) Kania, "Minds at War," p. 84
(12) Yonah Jeremy Bob, "Quantum apocalypse? – Super computer arms race will remake the world," *Jerusalem Post*, January 29, 2021, https://www.jpost.com/jpost-tech/quantum-apocalypse-super-computer-arms-race-will-remake-the-world-656957
(13) Elsa B Kania, "In military-civil fusion, China is learning lessons from the United States and starting to innovate," *RealClear Defense*, August 27, 2019, https://www.realcleardefense.com/articles/2019/08/27/in_military-civil_fusion_china_is_learning_lessons_from_the_united_states_and_starting_to_innovate_114699.html
(14) Elsa B. Kania and Lorand Laskai, *Myths and Realities of China's Military-Civil Fusion Strategy*, Technology and National Security, Center for a New American Security, January 2021, p.16, https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy
(15) Brian Hart, "Organisational reform a key driver of Chinese military science and technology innovation," *SAIA China Studies Review*, October 19, 2019, https://saiscsr.org/2019/10/29/csr-2019-organizational-reform-as-a-key-driver-of-chinese-military-science-and-technology-innovation/
(16) Rajat Pandit, "Indian armed forces need to invest in disruptive technologies: Gen Naravane," *Times of India*, August 25, 2020, https://timesofindia.indiatimes.com/india/indian-armed-forces-need-to-invest-in-disruptive-technologies-gen-naravane/articleshow/77744148.cms
(17) Headquarters Integrated Defence Staff, Ministry of Defence, *Technology Perspective and Capability Roadmap (TPCR)*, April 2013, https://www.mod.gov.in/sites/default/files/TPCR13.pdf
(18) Headquarters Integrated Defence Staff, Ministry of Defence, *Technology Perspective and Capability Roadmap (TPCR)*, 2018, https://www.mod.gov.in/sites/default/files/tpcr.pdf

(19) Pravin Sawhney, "2020 gave India a sharp lesson on the Chinese military. When will Indian generals take heed," *The Wire*, December 11, 2020, https://thewire.in/security/pla-china-military-india-lessons
(20) Subhashish Sarangi, "National Initiatives on Artificial Intelligence in Defence," *Strategic Perspectives*, *United Services of India,* April-June 2019, https://usiofindia.org/publication/cs3-strategic-perspectives/national-initiatives-on-artificial-intelligence-in-defence/
(21) T.V. Padma, "India bets big on quantum technology," *Nature*, February 3, 2020, https://www.nature.com/articles/d41586-020-00288-x#:~
(22) Ambuj Sahu, "Artificial intelligence in military operations: Where does India stand?" *Observer Research Foundation*, August 2, 2019, https://www.orfonline.org/expert-speak/artificial-intelligence-military-operations-where-does-india-stand-54030/

The PLA's Cyber Warfare Capabilities and India's Options

PK Mallick

China's People's Liberation Army (PLA) has understood that dominance in the information domain is the priority in modern conflict. Through the reorganisation of the PLA and the establishment of the Strategic Support Force, China has brought space, cyber, electronic warfare and psychological warfare under one umbrella to use these capabilities in a more efficient and effective manner. No other country, including the US, has done this.

China has no threat from land. Presently, its main aim is to secure Taiwan. All its modernisation, organisational changes and concepts of warfare are meant for this conflict, which will also involve the US, and has systematically developed these capabilities keeping in mind this scenario.

In the space, cyber and electronic warfare domains, China has advanced far ahead of India. With the kind of software development capabilities and human resources India possesses, it should have taken the lead in these areas, but must now play

catch up.

India has taken some baby steps by establishing the Defence Cyber Agency and Defence Space Agency, probably precursors to the Cyber and Space Command. In the fast-changing technology arena, India must move quickly and recover lost ground. But the present system of working does not give much confidence.

Psychological Operations

Currently, the Indian armed forces and strategic community blindly follow US jargons. If you want to influence the mind of people and the leaders of the adversary what terminology should be used? Is it information operation, psychological operation, strategic communications, influence operations, perception management, public information operations, public field diplomacy or other similar terms? These terms are being used interchangeably, but they are not synonyms. The Indian armed forces must coin their own common term and take appropriate actions to develop concepts, tactics, techniques and procedures.

Take, for instance, information operations. The various stake holders in this operation are—the Ministry of Home Affairs and the intelligence agencies, Ministry of Defence, Ministry of External Affairs, Ministry of Information and Broadcasting, Ministry of Electronics and Information Technology, Ministry of Communications and Ministry of Education, among others. Close coordination between these ministries will be needed to carry out information operations against an adversary. As of now, there is no central agency to coordinate and direct such a task. The integration for use of information operations is minimal within the armed forces as well.

The National Security Council Secretariat is the appropriate agency to be made responsible for information operations, given India's notoriously stove-piped bureaucracy.

Cyber Warfare

China is ranked second in the National Cyber Power Index, behind only the US, while India is ranked 21 of the 30 countries analysed (1). China is an acknowledged master in cyber espionage activities. Chinese hackers, in addition to traditional state espionage, are said to be pilfering intellectual property from every major Fortune 500 company, American research laboratories and think tanks worth trillions of dollars. Chinese hackers have taken everything, from the designs for the next F-35 fighter jet to the Google code, the US smart grid and the formulas for Coca-Cola and Benjamin Moore paint. If China can break through the reasonably good cyber network defences of these organisations, it can be assumed that Chinese malware are present in most of India's critical information infrastructures (2).

It is true that China has not shown its hand in carrying out offensive cyber operations. But the only distinction between computer network exploitation and attack is the intent of the attacker as the malware is already inside your network. The skill sets needed to penetrate a network for intelligence gathering purposes and for offensive action are the same.

Cyber Defence

Several measures have been taken to improve the cyber defence of important infrastructures. However, some reality checks are worrisome. The September 2019 cyber exploitation by North Korean cyber criminals in India's largest civil nuclear facility, the Kudankulam Nuclear Power Plant in Tamil Nadu, highlighted the vulnerabilities of Indian nuclear power plants (3). These nuclear installations do not even come under the National Critical Information Infrastructure Protection Centre and were not audited by it (4). If a cybercrime team from North Korea can penetrate India's largest nuclear facility, surely state-backed cyberattacks can cause much more damage.

Many of India's extremely sensitive and critical networks are not audited by any agency but are self-audited, including the intelligence agencies, armed forces, Defence Research and Development Organisation, defence public sector undertakings and the Ordnance Factory Board units. There is an urgent need to put these organisations under some sort of cyber audit mechanism.

War Gaming of Probable Events

Probable scenarios in a realistic environment should be war-gamed to determine the vulnerabilities in our systems and take appropriate remedial measures. For instance, say, just before a conflict in India's Northeast the power grid and railways communications network fail, adversely impacting the large-scale movement of men and material of the armed forces. War-gaming scenarios like these will help identify and plug weaknesses.

Though there has been improvement in the cyber defence of power networks, the efficacy varies. The NTPC and other public sector undertakings may be well off in cyber protection, but can the same be said about the arrangement in a state-owned hydroelectric plant that is also connected in the national power grid? A hacker could easily get into the national power grid through this poorly protected power plant and create mayhem at a time of their choosing. What can India do to prevent this incident?

Development of Crypt Analysis Capability

India does not have any high-grade decrypting capability. The introduction of 128- or 256-bits key has made code-breaking extremely difficult. However, the US's National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) already possess this capability, as do perhaps Russia and China. India must start the process of developing this capability. Cryptographers, mathematicians and analysts with the power of super computers must get together to develop this capability.

Collaboration with countries like Ukraine, Belarus, South Africa, Iran and Russia can be explored.

Forensic Labs for Embedded Hardware and Software

India is the world's biggest importer of military equipment, which have plenty of electronic hardware and software components. But no country shares its codes. There is always a chance of embedded hardware and software in these weapons platforms. What is the mechanism to check whether there is any malware in the increasingly sophisticated technology areas? What is the mechanism in the procurement of equipment procedure and supply chain management system to ensure that bugs are not present? While procuring, some legal and business clauses can be incorporated. But there is no getting away from India having its own testing facilities. This is extremely niche technology and costly, but it needs to be developed (5).

Command and Control Set-Up

There should be no ambiguity in the responsibility of organisations for cyber security. The US's NSA and Cyber Command come under the Department of Defence. In the UK, the GCHQ comes under the Foreign Ministry. In Israel, the National Cyber Bureau, directly under the prime minister, regulates activity in cyber space. In India, the National Technical Research Organisation (NTRO) has been entrusted with this responsibility, which does not come under any ministry and operates directly under the Prime Minister's Office. The interplay between the Ministry of Defence, the armed forces, the Ministry of Home Affairs and intelligence agencies (internal and external) needs to be clearly demarcated. Who will carry out offensive cyber operations in a conflict scenario? Can an intelligence agency do it, bearing in mind the rules of engagement or the laws of armed conflict?

Collaboration with friendly countries

India should actively collaborate and exchange information with friendly countries like Japan, Taiwan, Vietnam and Australia. For developing niche technology, counties like Israel, Belarus, Romania and South Africa can be approached.

Armed Forces Domain

Development of Deterrence Capability (6)

Though this is a highly classified domain, the armed forces and intelligence agencies must develop these capabilities in close cooperation. These should be tested in peace time so that they can be employed in event of a war. Projects that can be undertaken as part of capability development could include:

- How to penetrate the adversary's classified military networks
- How to isolate a built-up area electronically and in the cyber domain before carrying out any kinetic operation
- The kind of tasking to be given to Special Forces operating deep inside enemy territory. For instance, can they puncture the enemy's optical fiber cable network and obtain data?
- Develop malware in pen drives to be inserted in an enemy's classified network with the help of intelligence agencies so that information is sent back undetected at appropriate times
- Develop cyber exploits to be planted in the enemy's key military infrastructure like telephone exchanges, main servers of classified networks or radar installations, to explode electronically at an appropriate time to make them nonfunctional
- How to influence the minds of opposing operational, strategic commanders and leaders, especially of our northern neighbours

- The security of the tactical data link from India's extremely costly airborne early warning and control system to the other flying aircraft or to the bases. India must develop its own solutions for such highly classified links, and not rely on foreign technology for this
- How to overcome electronic and cyber-attacks by swarm of drones
- How to develop a malware that can be flown into an adversary's dense radar coverage, homed onto the radar beam and inserted to make the Air Defence Command and Control Systems malfunction, like in Operation ORCHARD (7)

Removal of Chinese network equipment

Earlier, there was no national policy on the use of Chinese network equipment and hardware. The audit authorities have no concern for national security and insist on the least price. Chinese companies always have the advantage of low prices. Although commanders at every level have the authority to overrule the audit observation on grounds of security and procure equipment, this is not done. This has resulted in the presence of large-scale Chinese network devices in India's many sensitive and classified networks. Efforts should be made now to take out the Chinese equipment from these networks.

Cyber capabilities at operational and tactical levels

What is our policy to provide cyber capabilities at the operational and tactical level? Due to the characteristic of target equipment and terrain features in operational and tactical battlefields, proximity to the target is essential. In the US, to carry out sophisticated cyber operations in operational and tactical battlefields, the most elite and niche technology cyber warfare experts from the NSA's Tailored Access Operations are embedded at the appropriate level in the battlefield. They carry out the tasks and fall back to the headquarters. Do our armed forces have similar arrangements with NTRO?

Cyber operations capabilities in the tactical battle area could include the following: (8)

- Collect intelligence by rapidly exploiting captured digital media
- Counter and exploit adversaries' unmanned aerial systems by exploiting data feeds
- Protect friendly unmanned aerial systems functioning in the area of operations
- Gaining access to closed networks in or near the area of operations, including extracting and injecting data
- Using electronic warfare systems as "delivery platforms for precision cyber effects"
- Exploiting new devices emerging from new trends and opportunities
- Conducting cyberspace intelligence, surveillance and reconnaissance operations
- Engaging in offensive social media operations

Electronic Warfare

China generally follows Russian concepts and equipment for electronic warfare. Russia showed its superiority in electronic warfare on the battlefields of Ukraine and Syria. In a military parade to celebrate the 70th anniversary of its founding in October 2019, China showcased its latest equipment, including for electronic warfare. Even as India procures the latest MiG 29 fighter jets and Sukhoi Su-30 MKI aircraft, it is worthwhile to consider acquiring the latest electronic warfare equipment from Russia that suits the country's requirements.

Endnotes

(1) Julia Voo, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, and Anina Schwarzenbach, *National Cyber Power Index 2020*, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2020, https://www.belfercenter.org/publication/national-cyber-power-index-2020
(2) U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, May 15, 2017, p. 72, https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF
(3) PK Mallick, *Cyber Attack on Kudankulam Nuclear Power Plant – A Wake Up Call*, Vivekananda International Foundation, December 2019, https://www.vifindia.org/paper/2019/december/18/cyber-attack-on-kudankulam-nuclear-power-plant
(4) "Cyber Attack on Kudankulam Nuclear Power Plant – A Wake Up Call"
(5) PK Mallick, *Research and Development in Cyber Domain and Indian Perspective*, Vivekananda International Foundation, September 2019, https://www.vifindia.org/paper/2019/september/05/research-and-development-in-cyber-domain-and-indian-perspective
(6) PK Mallick, *Cyber and Space Strategy for India*, Centre for Land Warfare Studies (CLAWS), https://drive.google.com/file/d/1tzcDdEENIiC9AX2nep7i1NOxaSOzKtCQ/view
(7) Caren Kaplan, "Air power's visual legacy: Operation Orchard and aerial reconnaissance imagery as ruses de guerre," *Critical Military Studies,* vol. 1, issue 1 (2015), pp. 61-78, https://www.tandfonline.com/doi/full/10.1080/23337486.2014.974949
(8) PK Mallick, *Cyber Security in India – Present Status*, Vivekananda International Foundation, October 2017, https://www.vifindia.org/issuebrief/2017/octobe/30/cyber-security-in-india-present-status

Asymmetric Warfare, Technology and Non-State Actors: What India Must Do

Kabir Taneja

While addressing a webinar on India's national security challenges and the role of air power, Air Chief Marshal R.K.S. Bhadauria, Chief of the Air Staff of the Indian Air Force, highlighted the challenges posed by rapid progression in technological innovations coupled with lower costs, leading to disruptions in how threats and warfare are now being perceived (1). The Air Chief specifically called attention to the potency of these technological disruptions in the hands of non-state actors, increasing their capabilities of achieving disproportionate effects in a conflict theatre.

He also cautioned on the use of drones by both non-state actors and small states—the latter arguably being highlighted due to the Nagorno-Karabkh conflict between Azerbeijan and Armenia in which drones played a critical role, specifically for the Azeris as the conflict zone became a parade for smaller, cheaper drones to prove their mettle (2). Meanwhile, armed with older Soviet-era equipment, the Armenians often found themselves fighting an invisible enemy. It is the non-state actors and their

incorporation of technology that has started to cause tremors in the foundations of how warfare has been viewed and broached.

Asymmetric Warfare, Counterterrorism and Counterinsurgency

The Air Chief's warning of the increasing threat of asymmetric warfare comes on the back of a slew of global and domestic developments in this field. An observable increase in small drones in and around the Line of Control in Kashmir may have finally forced the Indian security establishment to operationalise policies to counter a steady adoption of asymmetric warfare strategies, both from a state and counterterrorism level, including off-the-shelf purchases of counter-drone technologies from countries such as Israel (3,4). The use of such asymmetric tactics is not just visible in Kashmir, but also in heartland regions where the Naxal insurgency has a hold. In November 2019, it was reported that Maoists, for the first time, flew a drone above a CRPF camp in the violent Bastar region, highlighting a new phase of threat for counterinsurgency (COIN) operations to deal with on the internal security front (5,6).

However, from a counterterrorism and COIN perspective, technology such as crude armed drones (often piggybacking on quadcopters bought off any local toy store or online retailer and kitted out locally to carry crude bombs, narcotics, weapons and so on) have been operational in theatres such as Iraq and Syria, developed by terror groups like the so-called Islamic State (ISIS or Daesh). In fact, ISIS reportedly had its own small fleet of do-it-yourself (DIY) crude armed drones employed with home-made improvised explosive devices (IEDs), and the group had a system in place for operators to log in their operations, like a formalised military (7). Innovation goes beyond quadcopters, with drones outrightly built from scraps, operating both as drones with powered motors and gliders alike, showcasing an aptitude for not just 'modding' but building crude drones from scratch (8).

The use of armed crude drones can be traced back to 2016, when ISIS-linked fighters killed two Peshmerga fighters and gravely wounded two French soldiers in the Kurdistan region of northern Iraq via a booby-trapped drone (9). It is interesting to note that the crude drones have also evolved since then. The 2016 example was of a drone that crash-landed and exploded when picked up by the Peshmerga fighters after being intercepted. Since then, crude drones used by non-state actors have evolved, from both versions—that fly into targets and explode; and those that have been installed with makeshift pully systems that allows the drone to drop crude IEDs onto targets, record the same via a camera for propaganda value, and return home. These images and videos, released by ISIS's voracious online propaganda ecosystem, made it into most living rooms around the world to show how in the midst of the world's major conflict zone, the group was inventing, evolving, funding and challenging the might of the Western armed forces (10). However, since 2016, using cheap yet effective technology available off-the-shelf, and difficult to monitor or regulate, has expanded beyond ISIS. In 2018, Venezuelan President Nicolas Maduro survived an assassination attempt involving an explosive drone (11).

According to a study by New America, a US-based think tank, non-state actors ranging from Boko Haram in Nigeria and the Cartel De Jalisco Nueva Generacion in Mexico to the Taliban in Afghanistan and Hamas across the Middle East region have used drones in one way or another since 2016 (12,13). In September 2019, two major Saudi Arabian oil refineries were hit by drone attacks that were claimed by Yemen's Houthi rebels. Oddly, historically, the use of remote-control aircraft for attacks by a non-state actor can perhaps be traced back to 1993, when Japan's erstwhile extremist cult known as Aum Shinrikyo acquired a Soviet-era helicopter and planned to operate it via remote control (as a drone, in modern parlance) in a failed attempt to release toxic Sarin gas by air (14,15).

Developing Counter Measures

Deterring these new threats, specifically in the hands of terror groups and other non-state actors, has not been easy. The drones modded and used by such groups, which include models made for far simpler reasons such as photography and filmmaking, are products that are everyday items available freely at large technology retail outlets and even duty-free shops at airports. According to investigations conducted by Conflict Armament Research, India was one of the country's (along with China, Lebanon, Turkey, Uzbekistan and Kuwait) from where some of these drones were procured, most likely through online retailers. In one instance, a drone purchased in India in August 2016, and activated in the UK in October of that year, was found in Tal Afar, Iraq (16). This highlights that the time scale between purchase and use is short.

While India has tightened control on the manufacture and use of civilian drones, regulating global supply chains of finished products and components is extremely difficult. For instance, components like fuses and detonating cords manufactured by Indian companies were found in IEDs built by ISIS (17). The manufacturers revealed that they often do not know who the final buyer is, and with online markets, it is increasingly difficult to identify if a buyer is genuine or not.

Creating regulations and financial obstacles to tackle this kind of 'technology transfer' may be futile and committing to creating kinetic and tactical counter measures against these new threats by pitting technology against technology is arguably a better option to go with. Of course, the challenge always emits from the fact that technology does, and always will, outpace policy. Nonetheless, this sort of challenge has also garnered innovative responses against increasing asymmetric threats from terror groups. The French, for example, started to train eagles to take out crude drones, albeit to limited success (18).

On a more tactical and organised level, the US Army has adapted more aggressively against these threats. The US Army set up the Asymmetric Warfare Group (AWG) back in 2006 at the peak of the 'war against terror' campaigns in Afghanistan and Iraq, giving the US a headstart, at least as far as thinking beyond the box is concerned. This is not surprising considering the US military's expansive operational theatres in the Middle East and beyond, which have given it a much more realistic agenda to develop systems to ward off 'alternative' threats. The AWG studied, recognised and acted on these new threats, stripping down ISIS's drones' programme theoretically and practically, coming to innovation-based conclusions, and integrating their findings into US Army training methodologies (19).

This expansive explanation provides an insight on how to conceptualise an asymmetric threat that lies beyond threats that are obvious and bookish, and being aware of current and future 'crude-tech' innovations that could possibly be co-opted by non-state actors. Although the AWG is set to be "discontinued" by September 2021, it is a good blueprint to study for countries like India and could become another point of cooperation between Washington DC and New Delhi (20).

Conclusion

India's defence procurement, which largely relies on purchases made on the very day they need to be utilised, is currently integrating both traditional drone technologies pushed through by the recent Ladakh crisis with China and counter mechanisms to use of small drones by non-state (often supported by a state in India's case) actors via counter-drone technologies from the likes of Israel (21).

It is imperative for India to remember that fighting DIY and crude armed technologies could well be more difficult to achieve than traditional warfare. Militarising a camera drone used to make YouTube videos by an influencer is as convoluted an act as it sounds, and requires innovative thinking to tackle it granularly and strategically. The idea that drones such as the MQ-9 Reaper

be armed with Hellfire missiles and have a Hollywood-like kill list in its coffers is a pony trick that only the US can master at this point of time as far as counterterror operations are concerned. Recognising that technologies are no longer exclusive to warfare is the thought deterrence that India's national security czars should internalise. New Delhi's security thinking should move forward keeping these new mantras in mind while designing counterterror and COIN strategies for the next decade.

Endnotes

(1) "Drones in the hands of non-state actors make them more lethal: IAF chief," *The Times of India*, December 29, 2020, https://timesofindia.indiatimes.com/videos/news/drones-in-the-hands-of-non-state-actors-make-them-more-lethal-iaf-chief/videoshow/80014701.cms

(2) Alex Gatopoulos, "The Nagorno-Karabakh conflict is ushering in a new age of warfare," *Al Jazeera*, October 11, 2020, https://www.aljazeera.com/features/2020/10/11/nagorno-karabakh-conflict-ushering-in-new-age-of-warfare

(3) "Drone detected over international border in J&K: BSF," *Press Trust of India*, December 10, 2020, https://www.businesstoday.in/current/economy-politics/drone-detected-over-international-border-in-jk-bsf/story/424565.html

(4) "What are the anti-drone Israeli SMASH 2000 Plus systems the Navy has ordered?," *Times Now*, December 9, 2020, https://www.timesnownews.com/india/article/what-are-the-anti-drone-israeli-smash-2000-plus-systems-navy-has-ordered/692472

(5) "In a first, Naxals use drones over CRPF camp in Bastar," *Press Trust of India*, November 17, 2019, https://www.livemint.com/news/india/in-a-first-naxals-use-drones-over-crpf-camp-in-bastar-shoot-at-sight-order-issued/amp-11573983326488.html?__twitter_impression=true

(6) Sajid F. Shapoo, "Enticing the Maoist Guerrilla – India's COIN strategy and evolving surrender and rehabilitation policy," *Journal of South Asian Studies*, vol. 7, no. 3 (2019), pp. 95, https://esciencepress.net/journals/index.php/JSAS/issue/view/170

(7) Eric Schmitt, "Papers offer a peek at ISIS' drones, lethal and largely off the shelf," *The New York Times*, January 31, 2017, https://www.nytimes.com/2017/01/31/world/middleeast/isis-drone-documents.html
(8) Serkan Balkan, *Daesh's Drone Strategy: Technology and the Rise of Innovative Terrorism*, SETA, 2017, pp. 14, https://setav.org/en/assets/uploads/2017/08/Report88.pdf
(9) "ISIS booby-trapped drone kills troops in Iraq, officials say," *Reuters*, October 12, 2016, https://www.theguardian.com/world/2016/oct/12/exploding-drone-sent-by-isis-allies-kills-and-wounds-troops-in-iraq-report
(10) Vocativ, "ISIS propaganda video drops a bomb from a drone," YouTube video, November 4, 2017, https://www.youtube.com/watch?v=cz2jrmnm7ds&ab_channel=Vocativ
(11) "Venezuela President Maduro survives 'drone assassination attempt'," *BBC*, August 5, 2018, https://www.bbc.com/news/world-latin-america-45073385
(12) New America Foundation, "Non-State Actors with Drone Capabilities," https://www.newamerica.org/international-security/reports/world-drones/non-state-actors-with-drone-capabilities/
(13) Frud Bezhan, "Taliban PsyOps: Afghan militants weaponize commercial drones," *Gandhara*, January 29, 2020, https://gandhara.rferl.org/a/taliban-commercial-drones-attacks-afghanistan/31075672.html
(14) Ben Hubbard, Palko Karsaz and Stanley Reed, "Two major Saudi oil installations hit by drone strikes, and US blames Iran," *The New York Times*, September 14, 2019, https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html
(15) Holly Fletcher, "Profile: Aum Shinrikyo," *Council on Foreign Relations*, June 19, 2012, https://www.cfr.org/backgrounder/aum-shinrikyo
(16) Don Rassler, *The Islamic State and Drones: Supply, Scale and Future Threats*, Combatting Terrorism Center at West Point, July 2018, pp. 16, https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf
(17) Sandeep Singh and Anil Sasi, "7 Indian firms among those in Islamic State supply chain: EU study," *The Indian Express*, February 26, 2016, https://indianexpress.com/article/india/india-news-india/7-indian-firms-among-those-in-isis-supply-chain-says-eu-study/
(18) Jeff John Roberts, "France is training Eagles to kill drones," *Fortune*, February 23, 2017, https://fortune.com/2017/02/22/drones-eagles-france/#:~:text=The%20birds%20are%20natural%20drone,Aramis%2C%20Athos%2C%20and%20Porthos

(19) T.S. Allen, Kyle Brown and Jonathan Askonas, "How the Army out-innovated Islamic State's drones," *War On The Rocks*, December 21, 2020, https://warontherocks.com/2020/12/how-the-army-out-innovated-the-islamic-states-drones/
(20) Matthew Cox, "In major shift, Army to shut down Asymmetric Warfare Group and Rapid Equipping Force," *Military.com*, October 2, 2020, https://www.military.com/daily-news/2020/10/02/major-shift-army-shut-down-asymmetric-warfare-group-and-rapid-equipping-force.html
(21) Rajat Pandit, "India leases top-notch US drones for surveillance amid border row with China," *The Times of India*, November 26, 2020, https://timesofindia.indiatimes.com/india/india-leases-top-notch-us-drones-for-surveillance-amidst-border-row-with-china/articleshow/79413719.cms

About the Editors and Authors

Manoj Joshi is a Distinguished Fellow at the Observer Research Foundation.

Pushan Das is Head of Forums at the Observer Research Foundation.

Malcolm Davis is a Senior Analyst in Defence Strategy and Capability at the Australian Strategic Policy Institute.

Major General BS Dhanoa (Retd.) was in the Armoured Corps of the Indian Army. He last served at the Army War College and previously commanded an armoured brigade and an infantry division on the Western Borders.

Justin Bronk is the Research Fellow for Airpower and Technology in the Military Sciences team at Royal United Services Institute.

Rajeswari (Raji) Pillai Rajagopalan is a Distinguished Fellow and heads the Nuclear and Space Policy Initiative at the Observer Research Foundation.

Major General PK Mallick, **VSM (Retd.)** was in the Corps of Signals of the Indian Army. He holds the COAS Chair of Excellence at the Centre for Land Warfare Studies (CLAWS).

Kabir Taneja is a Fellow with Strategic Studies Programme at the Observer Research Foundation.