global POLICY

GP-ORF Series

Future Warfare and Technology: Issues and Strategies

Editor

Rajeswari Pillai Rajagopalan

Durham University

WILEY

FUTURE WARFARE AND TECHNOLOGY: ISSUES AND STRATEGIES

Edited by
Rajeswari Pillai Rajagopalan

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 and Production: Preeti Lourdes John

Cover Design: Rahil Miya Shaikh

Layout: Simijaison Designs

ISBN: 978-93-90494-14-9

Citation: Rajeswari Pillai Rajagopalan, ed, Future Warfare and Technology: Issues and Strategies, (New Delhi: ORF and Global Policy Journal, 2022).

Contents

Implications Perspectives

Introduction

Rajeswari Pillai Rajagopalan

The purpose of war has remained constant since time immemorial. Prussian general and military theorist Carl von Clausewitz famously stated, "War is merely a wrestling match on an extensive scale, an act of violence intended to compel our opponent to fulfil our will". Nevertheless, the ways and means to achieve such goals have transformed through the course of history, spurred mainly by evolution in the technological realm. There have been attempts to capture and categorise these changes through different analytical frameworks, but the influence of technology and geopolitics forms a deadly mix, making future warfare far more complex.

With global and Asian balance of power in a state of strategic flux, competition, rivalry, and conflict—whether violent or otherwise—are again taking centre stage. Further, driven by technological innovation and with the advent of emerging and critical technologies, there are also possible changes in tactics, strategies, and mediums of war. The growing importance of cyber warfare, weaponisation of space, warfare by proxy and influence operations, and misinformation campaigns denote that modes of warfighting are changing. Future battlefields might be unrecognisable with the growth and advancements in technologies such as artificial intelligence (AI), quantum, cyber, space, and biotechnology.

Militaries around the world, policymakers, and strategists are confronted with enormous challenges driven by this transformation. Issues such as attribution and deniability pose additional challenges in arriving at suitable policy responses and dispensing justice of, in, and post-war. Further, these challenges are expected to become more complex as states aim to devise new ways of leveraging technological change to wage war.

Governments worldwide have had to understand and adapt as well as come up with appropriate response measures in recognition of the changing nature of warfare. This compendium aims to understand what future warfare might look like, what are the different theatres and domains where the wars will be fought, and the role of critical and emerging technologies in aiding the goals of future warfare. The essays included in this volume have been written by expert authors from across the globe on a variety of themes, including autonomous weapons and AI; cyber weapons; space and counter-space technologies;

biotechnology and biowarfare; data analytics and behavioural science; the role of nuclear weapons; quantum technologies; the interplay between different domains or technologies involving space, cyber or nuclear; and the impact of quantum technologies on cyber, space, and nuclear security.

Key questions examined in the volume include the who, what, where, when and how of future warfare, and the implications.

Air Vice Marshal Arjun Subramaniam examines the broad contours of conventional war and the future of joint operations with an infusion of emerging and critical technologies. He argues that even as India embraces these technologies, for the Indian armed forces to manage the challenges of a two-front security conundrum over the next decade against the backdrop of a fragile and unstable global and regional security environment, its leadership needs to remain doctrinally nimble, resource-conscious, technologically- savvy, and flexible enough to remain grounded in India-specific operational realities. While many strategists in recent years have given up on the idea of states fighting a traditional conventional war, Sameer Patil argues that high-intensity warfare has returned, as can be evidenced through several contemporary conflicts, including the Russian invasion of Ukraine, developments across the Taiwan Straits, India-China conflict, or the South China Sea. Patil discusses how major militaries worldwide are having to adapt to this, with the addition of disruptive technologies and how that distinguishes the present high-intensity warfare from its previous incarnations. With the intensification of great power politics, high-intensity warfare, and the acceleration of the US-China technology competition, sanctions are also making a comeback. Kazuto Suzuki explores the importance, usefulness, and effectiveness of sanctions, especially by looking at the current US, European Union (EU), and Japanese sanctions on Russia for its invasion of Ukraine. Suzuki also brings in the limitations of its effectiveness by considering the current situation. The EU importing 40 percent of Russian oil and gas is bringing into question the effectiveness of the sanctions on Russia. That the EU does not present a united front on this issue further demonstrates the limited efficacy of sanctions in today's interdependent world.

Next, Wilfred Wan and Nivedita Raju examine how different technologies intersect with each other to impact strategic stability. The authors highlight how the defining trait of hybridity, which is the interplay across domains, affects the strategic context, considering ramifications for nuclear deterrence, related risks, and arms control and disarmament. Maj. Gen. Amarjit Singh assesses the future of warfare in the context of grey zone operations, which have become extremely prevalent in the last few years. However, Singh is quick to point out that the advent of the new generation of warfare does not make obsolete the lessons of earlier generations. In fact, even in the current Ukraine conflict, one can see all the generations of warfare simultaneously except for the first-generation of warfare. In this context of changing warfare patterns, Ashok GV examines a crucial question of attribution in cyberattacks against space objects to determine the impact, if any, of international space law on the subject of attribution and the consequential questions of state responsibility. Gen. Raj Shukla explores the theme of changing warfare, and the evolution of warfare and the salience of the technology dynamic in the current generation of warfare. He argues that the embrace of technology along with agile doctrinal adaptation and organisational restructuring is what is needed if militaries are to exercise "a sharp, calibrated edge over competitors and adversaries alike". Further, he tries to answer important questions of how national security institutions and global militaries should prepare for the future; what are the necessary attributes of a future-ready military, and finally—and possibly most importantly—how we design and nurture an ecosystem that will facilitate our capacity to address better the challenges that

come along with the new paradigm of digital combat. Looking at the trends in warfare, Lt. Gen. Ravindra Singh Panwar outlines some key issues related to AI, autonomy, and human control. While AI-based applications can bring enormous benefits in the civilian sector, AI-enabled weapon systems are concerning because of their dangers to human lives. The essay also outlines the host of legal and ethical issues associated with AI, thereby underlining the need for global regulations that could suitably address the threats posed by these systems.

Next, Manpreet Sethi examines the continued role of nuclear weapons in future wars despite the changing nature of warfare. She asks pertinent questions like whether the risks of actual use of nuclear weapons will increase due to new doctrinal or technological developments or if the weapons will continue to have a restraining impact on wars in general. She argues that the answers to such questions can never be definite but adds that two doctrinal and three technological developments related to nuclear weapons will likely impact future wars. Bart Hogeveen examines a key new form of warfare—cyber warfare—and the emerging cybersecurity landscape in the Indo-Pacific. Hogeveen does this by outlining the changing contours of cybersecurity in the regional security context, listing the growing military cyber warfare capabilities and establishing cyber-specific defence institutions that have sprung in the Indo-Pacific, all of which are indicative of the securitised cyber domain. To mitigate the risks and threats from such activities and capability development, Hogeveen makes a case for global dialogues and engagements involving the multiple stakeholders engaged in this domain, including political leaders, officials, civil society advocates, technicians, and industry. This will develop a 'common operational picture', which is essential for developing appropriate policy interventions that has adequate oversight, checks and balances.

Noëlle Van der Waag-Cowling examines the intangible nature and the secrecy around the development and existence of cyber weapons that adds to the difficulties associated with their potential and usage in the changing context of warfare. Beginning with conceptual perspectives on cyber weapons, she provides an overview of cyber operations in armed conflict, the limitations and affordances of cyber weapons, and the proliferation of cyber offensive capabilities. The essay concludes with an examination of cyber weapons and international law, especially the various global efforts that have been in play but also the limitations of developing global cyber arms control measures. Next, Michal Křelina looks at another novel development—quantum technology. The author points out that quantum technology is variously described as a disruptive or an emerging technology of strategic significance, especially in the context of China, providing Beijing with "a decisive advantage in future peacetime and wartime competition alike". Like many other emerging technologies, quantum technologies are dual use in nature, with both civilian and military applications. Krelina provides a careful perspective of how and what impact of these technologies may have on future conflicts and war. The author does this by outlining the various military applications of quantum technologies, including the application of quantum computing in cyber operations that can break the current asymmetric encryptions, quantum-enhanced machine learning for intelligence, surveillance and reconnaissance (ISR) and situational awareness, faster and better wargame simulations (leading to better decision-making), optimisation of military logistics and supply chain for missions, and enhanced analysis of radio-frequency spectrum. But to avert any unpleasant surprises, Krelina argues for the need to generate greater awareness of the technology and its direct and indirect consequences.

Next, Shambhavi Naik assesses another important technology—biotechnology—in the context of changing warfare. Naik provides both tactical and strategic implications of biotechnology and biowarfare in future warfare. While bioweapons have been considered a weapon of mass destruction, the global community has shunned these weapons. But the emergence of new technologies and a fractured international political situation have pushed for the development of "targetable bioweapons" that may be developed and "used without attribution". Such a scenario, the author argues, calls for a review of existing international mechanisms such as the Biological Weapons Convention.

The next two essays look at the outer space domain in the context of changing warfare. Outer space was immune from terrestrial politics and had maintained sanctity for several decades, but that is not the case anymore. Malcolm Davis argues that space has never been a global common for peaceful purposes alone, as the rhetoric generally suggests. Davis argues that space has been militarised since the beginning of the space age, with both the US and erstwhile Soviet Union using satellites for gathering ISR data, satellite communications, and for strategic functions including nuclear command, communications, and control, and missile early warning services. The role of space has only expanded manifold over the last few decades, and the threat of counterspace technologies is real. Nevertheless, with a divided global space community, Davis argues that "the best solution to meeting the threat posed by adversary counterspace capabilities is to promote a dual-track solution by enhancing and strengthening space law and regulation to establish new norms of responsible behaviour in space and working to get all major space powers to agree to these new arrangements – together with investment in resilient space capabilities and a means to ensure effective space control that strengthens space deterrence". The pursuit of space deterrence and resilience appears to be inevitable, but it will likely make space a lot more fragile. The second space-related essay by Almudena Azcárate Ortega examines the critical importance of space and the current threats to space systems. This brings out the urgency in dealing with them or facing the reality of space being "a new theatre of conflict, with devastating consequences for humankind". Azcárate Ortega argues that the existing space legal regime has several inadequacies, including "a permissive and open-ended language, which has allowed the emergence of different interpretations when it comes to the use and exploration of space". She argues that arriving at a common understanding of what connotes space security is possibly difficult "because of the complexity of space systems, the multiple uses and users of space system, and the lack of space-specific regulations that focus on space security". Despite the bleakness of the situation in space, she ends the essay on an optimistic note with the current work undertaken by the UN Open-Ended Working Group (on space security norms and principles.

Kubo Mačák and Laurent Gisel explore cyber operations in armed conflicts from an implications and international humanitarian law (IHL) perspective. The authors make a strong case for the applications of IHL principles and rules to cyber operations, citing the reports of the recent UN Open-Ended Working Group and the UN Group of Governmental Experts, but they are also mindful of the challenges that come along with it through issues including the notion of attack, and the importance attached to civilian electronic data protection. Jyun-Yi Lee examines the role of technology in China's hybrid warfare against Taiwan, stating that "the threat posed by the interplay of China's lawfare and technological warfare to Taiwan has been growing". Lee identifies technology use in four scenarios to make warfare more effective while creating legal uncertainties. The final essay in the volume by Samyak Rai Leekha, Rajeswari Pillai Rajagopalan, and Pulkit Mohan looks at the implications of some critical and emerging technologies, including space, cyber, nuclear, and AI and automation. The authors take us through

the major developments in each of these technologies, especially as it relates to military and security contexts. Despite many past and ongoing efforts, geopolitical developments, including the changing balance of power dynamics, have impeded the development of consensus on the global governance of these technologies.

The *Future Warfare and Technologies: Issues and Strategies*, a collection of 18 essays, explores the challenging path ahead in terms of technological interface with emerging trends in warfare. There are issues of uneven technological development trajectories, which have influenced global governance debates on critical and emerging technologies, the insufficiencies and vagueness of existing governance measures, and the integration of many of these technologies in conventional military operations, all of which are examined in a nuanced manner. This volume is merely an attempt at unpacking some of the critical technologies in the context of changing warfare.

I also want to thank my colleagues Samyak Rai Leekha and Pulkit Mohan for their assistance with this volume. My thanks also goes to Preeti Lourdes John for her meticulous copy editing and bringing the volume to a reality.

General Strategic Perspectives

The Future of Joint Operations in a Technology Intensive Battlefield: An Indian Perspective

Arjun Subramaniam

"…the "holy trinity" of digital engineering, agile software development and open system architectures…must be adopted fully to drive down costs and enable rapid development."

Air Commodore K A Muthana (1)

From the conflicts in Syria, Afghanistan and Yemen, and between Azerbaijan and Armenia, India and China, and now Russia and Ukraine, thick clouds of doctrinal and operational ambiguity have emerged to challenge joint military planners across the world. Among these are dilemmas that relate to the changing character of war. These include the fusion and concurrent coexistence of several genres of conflict within the same battlespace, the all-pervasive impact of technology across the spectrum of conflict, and the blurring of transition lines between what constitutes a traditional conflict and the increasingly common phenomenon of "all measures short of war" (2). Air Chief Marshal Vivek Chaudhari, India's current air chief, succinctly listed the key characteristics of future battlefields from an Indian standpoint as being "cluttered, congested, complex and contested" (3).

Despite the suboptimal political outcomes in recent decades resulting from the US-led force application in Iraq and Afghanistan, large and powerful states such as Russia do not seem to have learned military lessons from history. Consequently, they have been bogged down in conflicts because of not thinking through the possible consequences of force application strategies and their linkages with possible geopolitical outcomes.

Amidst this chaos, spectacular technological advances have occurred over the past few decades. These advances have forced joint military planners to take stock of existing doctrines, review force structures, and embark on transformation strategies to leverage the force multiplier and enabling capabilities of several attractive technologies across the spectrum of conflict.

This essay will highlight the impact of several enabling technologies on a joint battlefield environment as experienced and envisaged in the Indian context from a current and medium-term perspective. It will also paint a possible adversarial landscape and situate future operational scenarios from a joint warfighting perspective with the technological paradigm occupying centre stage. Following this, it will highlight some emerging technologies that could enhance the readiness of the Indian military to deliver the necessary strategic and operational effects in future battlespaces. Finally, it will offer a cautionary practitioner's perspective based on ground realities about the magnetism of technology as a panacea for all operational problems.

Conflict Landscape

India may at times be tempted to overplay the collusive continental threat along the nearly 5,000-km contested frontiers with its principal adversaries (China and Pakistan), but there is little doubt that the clear zones of conflict exist along the Line of Actual Control (LAC) with China and the Line of Control (LoC) with Pakistan.

Going by the conflicts and clashes along these frontiers over the last two decades, the worst-case scenario for India will be two or three localised high-intensity skirmishes at high altitudes along the LAC with China and a diversionary feint by Pakistan along the LoC to split the Indian response. In such a situation, commonly called a 'two-front scenario' by Indian military analysts, the onus of opening a maritime front will rest with India. This proposition merits serious discussion as it goes against the grain of the Indian strategic DNA of taking the lead in expanding a conflict. Consequently, India's strategic temptation will be to soak in the pressure along its continental fronts with a reactive and resilient operational air-land strategy that lies within its comfort zone. This strategy could reinforce failures from the past.

Unlike in the past, these localised conflicts will see a quantum increase in efforts by all protagonists, particularly the side that seeks to achieve the initial surprise, to shape the battlespaces with overwhelming cyberattacks to blind both offensive and defensive networks. When complemented by effective and coordinated firepower that causes significant and early combat attrition and shock, a 'first-mover advantage' is likely to be created that can be leveraged in a short and swift conflict. However, should it be prolonged like the current Russia-Ukraine conflict or the Kargil War, there will be other challenges to consider, such as the sustenance of networks, logistics chains and troop morale, all of which have technology enablers as key propellants. Any crystal-gazing into the future must also factor in an escalation in the maritime domain, particularly if the continental front faces significant pressure. This would call for an increasingly sophisticated approach to joint operations that is driven by a technology-enabled politico-military leadership.

Technology-Enabled Joint Operations

While there is a tendency to superimpose operational templates from several recent clashes on scenarios India is likely to face, these must be calibrated by recognising technology's pivotal role at all stages in a potential conflict involving joint forces. For instance, the success of unmanned aerial platforms in the Armenia-Azerbaijan and Russia-Ukraine battles is instructive in understanding these platforms' immense potential in surveillance, tactical reconnaissance, targeting, and offensive missions. However, their effectiveness in a contested and symmetrical aerial environment is yet to be tested. On a different plane, however, is the highly relevant and timely warning of the consequences of a poorly networked joint operating and logistics environment, as experienced by the Russians in their stalled offensive towards Kyiv in the ongoing war in Ukraine (4). For ease of understanding and placing technology in various buckets during the likely phases of operations, attributes such as flexibility, interoperability, and interchangeability must emerge as the edifice on which strategies, doctrines, and operational plans are developed.

Situational awareness and shaping battlespaces

Multidomain narrative building and situational awareness with an emphasis on net assessment are vital in shaping effective Indian responses in the face of rapidly evolving and unknown security threats across the spectrum of conflict (5). The above process is no more than a sophisticated technologically-enabled scenario-building and threat-mitigation process that gained traction during the Cold War when both the US and Soviet Union were constantly evaluating and processing each other's capabilities. The importance of net assessment in contemporary conflict dynamics is reflected by the renewed importance of this competency in countries like the UK through the appointment of accomplished academics and intellectuals to critical positions (6).

In contemporary times, strategic and operational situational awareness will largely depend on defensive and offensive cyber capabilities, information dominance and persistent stare space situational awareness (SSA), which translates into the creation of maritime, high-altitude, and electronic operational mosaics (7). This would then drive the ability to deploy quick response joint capabilities across multiple operating domains. With an eye on China, India's principal security challenge in the foreseeable future, much needs to be done in all three areas.

Although several strategic commentators have suggested a 'leapfrogging' approach to reduce the widening asymmetry in the areas mentioned above, definitive strategies to convert ideas and intent into processes and products are still a work in progress. Though developing indigenous capability in the cyber and space domains through the *Atmanirbhar Bharat* (self-sufficient India) initiative is laudable, medium-term responses will only be possible with significant support from India's strategic partners, particularly the US, France, and Israel.

While some joint operational structures do exist in India in the form of organisations such as the Defence Space Agency (DSA) (8), the fusion of defensive and offensive cyber operations is still a work in progress within the Indian armed forces. In contrast, China's People's Liberation Army (PLA) created a Strategic Support Force to coordinate all offensive and defensive operations in the space and cyber

domains. The launch of airships by the Chinese Academy of Sciences to altitudes higher than Mount Everest in May 2022 is part of China's Earth Summit Mission that examines the impact of westerly winds on the ozone layer over Tibet. These airships, much like aerostats ('lighter-than-air' aircraft), have the potential to carry surveillance and other electronic payloads and can easily be deployed in large numbers across the Tibetan Plateau to enhance situational awareness to extraordinary levels of persistent stare and monitoring capabilities (9).

Any assessment of the India-China paradigm in the post-2014 period through these lenses must be accompanied by an acknowledgement that moving from a posture of strategic diffidence, as demonstrated by India vis-à-vis China since the 1990s, to one of strategic confidence, even with a more assertive Indian government in power, will be incremental due to the huge capability gap that exists between the two powers (10). India has arguably adopted a robust response to the increasing Chinese assertiveness since the 2017 Doklam standoff, but reports of possible 'salami slicing' across the LAC, stray cyberattacks on critical Indian infrastructure, and change in the profile of PLA troops across Tibet should have pushed India to try and proactively shape a possible battlespace across the LAC, albeit from a position of disadvantage (11). Clearly, the lack of adequate aerial and space-based surveillance assets impeded the creation of an operational mosaic that could be acted upon decisively by joint commanders.

The signing of several foundational technology and logistics sharing agreements between India and the US, including the Basic Exchange and Cooperation Agreement (BECA) on geospatial intelligence, is just one way to improve interoperability and interchangeability between the countries' militaries (12). The signing of BECA in October 2020, mere months after the Galway clash, indicates a recalibration of ties with China since it offers India significant value in several areas, including SSA and precise targeting intelligence, where its own capabilities have been limited.

Networks, logistics and sustenance

Had India demonstrated better situational awareness and synergy before the Galwan clash, the Indian Air Force (IAF) could have undoubtedly responded sooner, both in the kinetic and non-kinetic domains, to facilitate a logistics and force induction, and to position offensive assets to preempt the events that led to a change in the status quo in Eastern Ladakh. Before the Galwan crisis, warfighting in Eastern Ladakh was cocooned in a time warp, with the PLA seizing the first-mover advantage over the Indian Army by creating a network-enabled infrastructure and logistics system to support operations across large swathes of the LAC. There was, however, a propensity on both sides to remain within a comfort zone that resulted in massing troops opposite one another across the LAC and anticipating a land-centric and infantry dominated rather than a technology-enabled manoeuvre battle when conflict broke out. This approach largely dominated the thinking of operational commanders on both sides (13).

The months preceding the transgressions by frontline PLA formations into Eastern Ladakh saw a massive build-up of a PLA logistics chain in Western Tibet to support a large exercise conducted by the Chinese across Tibet, which also saw the employment of new light tanks and 155mm howitzers. India's response to this was largely reactive as it cranked up a joint response on multiple fronts only after the brutal skirmish at Galwan left many soldiers dead and wounded on both sides. While the politico-diplomatic dimension of this response is beyond the purview of this essay, India's military response was notable. It took the PLA by surprise with its swiftness and fervour. At the heart of this response was a

decisive move by the Indian Army to reconfigure its deployment of forces in Eastern Ladakh by giving them more offensive teeth in the form of armour and the latest artillery acquisitions and the Indian government's open-ended clearance to employ air power in all its dimensions over Eastern Ladakh for the first time since independence (14).

Consequently, the volume of airlifts into Eastern Ladakh between mid-May to mid-August 2020 and then through the winter of 2020 was unprecedented. This was possible because of the transformation of the air mobility assets of the IAF with the induction of the C-17 heavy lift, the C-130 J Special Forces and medium-lift platforms, and the Chinook heavy lift helicopters. The IAF station in Chandigarh emerged as the hub of the logistics build-up, the first assertive Indian move on the Eastern Ladakh chessboard.

A critical look at this operation reveals that the response and build-up was a joint one that resulted from a crisis and was not initially built around an integrated supply chain and logistics network with standard protocols and networks. As tensions with China persist, Air Chief Marshal Chaudhari maintains that the greatest lessons the armed forces learned from the combined challenge of responding to the PLA incursions and the Covid-19 pandemic were those related to integrated logistics, stocking, and replenishment in a network-centric environment (15). It is possible that in any future conflict along the LAC, managing logistics and maintaining troop morale and effectiveness in hostile terrain and weather conditions will play a crucial role in determining outcomes. The speed with which China is building bridges across the Pangong Tso in Ladakh with heavy-duty and high-tech construction machinery and providing proper combat gear to its troops bears testimony to this fact (16).

Joint maritime options

Amid the Eastern Ladakh crisis, India's strategic community has realised that some air power and maritime measures are available, particularly in the Indian Ocean Region (IOR), among the several counter-coercive options that can be deployed in response to Chinese aggression along the LAC. These include India's active participation in the Quadrilateral Security Dialogue; a recognition that the Andaman Nicobar Islands offer immense potential as a springboard for several kinds of operations, including recce, surveillance, strike, and amphibious operations; and the relative operational advantage enjoyed by the Indian Navy west of the Malacca Straits.

This makes it imperative for India to develop joint maritime options that go beyond maritime diplomacy. Several Indian practitioners of sea power, including Rear Admiral Raja Menon and Vice Admiral Anil Chopra, suggest that it is time for Indian sea power to seriously contest the PLA Navy's attempts to make inroads into the IOR (17).

The trajectory of maritime conflict in the post-Second World War era suggests the implausibility of large fleet versus fleet engagements on the high seas due to the heightened vulnerability of large and expensive surface platforms. However, the risk to the global economy poses the greatest challenge for any power while contemplating coercive strategies at sea. Considering this conundrum, some practitioners of sea power argue that sub-surface deterrence in the form of building adequate submarine capability is the way forward. However, notwithstanding the vulnerability of surface platforms like the aircraft carrier, it remains a critical element of power projection, and it will be a tough call for India's strategic planners not to consider the three-carrier force in the decades ahead to match the expansion of the PLA Navy.

Until that happens, India has no option but to leverage the experience and capabilities of the IAF over the maritime domain, particularly in offensive roles, by exploiting platforms such as the SU-30 MKI and the Rafale. However, the depleting strength of fighter squadrons in the IAF will challenge its ability to impact the maritime and continental fronts simultaneously.

Should there be active hostilities along the LAC and LoC, some viable options include active surveillance and shadowing operations by exploiting the Indian Navy's large fleet of P-8 I Long Range Maritime Patrol aircraft, freedom-of-navigation patrols, and even seizing enemy merchant ships. The combined aviation assets of the Indian Navy and the IAF are a significant force multiplier and must be leveraged synergistically for decisive impact (18). The usefulness of deterrence at sea and the power projection potential of large fleets and several low-scale coercive possibilities make joint sea power a potent instrument that needs nurturing, particularly amid great power competition and several subsidiary competitions in an increasingly multipolar world order.

Joint attrition strategies

Inflicting disproportionate attrition with shock and surprise on powerful and numerically superior adversaries is a time-tested strategy. In the modern era, this strategy has often been the focus of 'asymmetric' warfighting across the spectrum of conflict. India is no stranger to such strategies, with Pakistan testing such tactics against it with some degree of success over the last seven decades.

Barring the proactive joint strategy applied during the 'Lightning Campaign' in present-day Bangladesh in 1971, the Indian military has since independence primarily relied on reactive deterrence, resilience, and a never-say-die spirit to respond to national security crises, particularly along its contested frontiers. Faced now with a considerably stronger adversary with a defence budget four times that of its own and a growing technological asymmetry in every realm of military technology, the Indian military must now think about developing, wargaming and testing innovative strategies. The aim should be to cause disproportionate attrition on the PLA in 'limited war' scenarios at high altitudes and possibly in the maritime domain.

In the absence of any real competitive advantage in force structures, the success of such a strategy rests on the Indian armed forces' ability to jointly and innovatively leverage the existing cutting-edge technologies and platforms it possesses. These must then be deployed against specific adversary pressure points to create operational cycles for sustainable outcome-based targeting inside the adversary's OODA Loop (a decision-making acronym for 'observe, orient, decide, act'). The heart of such a strategy will rest on an air power-led offensive philosophy supported by highly accurate and near real-time satellite-based intelligence that would enable precision targeting. Without a 24X7 capability in this realm, the importance of collaborative efforts cannot be lost on Indian military planners. The signing of BECA soon after the Galwan clash highlights the seriousness India accords to the military threat from China after decades of hoping for 'business as usual' with the Chinese despite the multiple stressors along the LAC.

What would be the main constituents of an effective 'attrition causing' strategy (not to be confused with commonly understood First World War-type attrition strategies that rely on mass and friction)? Preemptive, proactive, and preventive approaches offer the best possibilities for causing impactful

attrition that could disproportionately affect the likely political outcomes in the India-China context. These could be a possible response to a traditional 'salami slicing' move by the PLA with an expectation of a muted and delayed response from India.

With escalation dynamics being a crucial facet of any strategy in the backdrop of conventional war between nuclear-armed adversaries, it would be advisable to initially calibrate attrition strategies to remain at the shallow tactical level by exploiting technology and precision to ensure that firepower is used for effect rather than widespread destruction.

A proactive strategy—with a combination of drone swarms, long-range precision fires from fifth-generation fighter platforms such as the Rafale and SU-30 MKIs, well-directed artillery and surface fires, and multiple raids by stealthily inserted Special Forces—has the potential to cause significant initial attrition and surprise the PLA. However, such a strategy must be accompanied by sufficient resilience and absorption of massive retaliatory fires from the PLA Rocket Force and PLA Air Force (PLAAF). While this would be the ideal attrition-causing strategy for a weaker adversary to employ, it is unlikely to be a typical Indian response to a grave provocation along the LAC. Consequently, in the eventuality of the PLA initiating a limited conflict, an alternate strategy will need to rely on technology to ensure the survivability of the bases, networks and sensors associated with the offensive capabilities discussed previously (19). Absorb, recover, respond, and attrite will be the operational sequencing in such a strategy.

Creating, training, and deploying such quick response capabilities are entirely within reach and will depend on the seriousness with which India walks the road of 'jointness' and 'transformation'. Reliable reports from practitioners who witnessed the entire sequence of the Indian military response to the PLA's creeping actions in Eastern Ladakh in 2020 indicate that a vital positive takeaway has been India's politico-military willingness to think and act offensively, even if it has not translated into visible and optimal results on the ground.

Offensive air power will be pivotal in driving early military successes in any conflict between India and its adversaries, irrespective of the terrain involved. Taking a cue from the incredible progress made in developing and deploying unmanned combat aerial vehicles by the PLAAF (20), India is prioritising expanding its own inventory of UAS and has accelerated several indigenous programmes. Additionally, it has supplemented its current inventory of Israeli-made platforms like the Heron and Searcher with the US-built Sea Guardian offensive drones (21). Indian advances in operationalising long-range weapons (such as the extended-range Brahmos) and several long-range air-air and air-ground missiles (such as the Astra-1, Astra-2 and the New Generation Anti-Radiation Missile) are praiseworthy and indicate the right focus to gain the 'first-mover' advantage (22).

Technology Challenges

To leverage the potential of several disruptive and emerging technologies—such as artificial intelligence (AI), Internet of military things (IoMT), combat clouds, a fusion of networks, and UAS—transformation in the Indian military must progress beyond the current superficial initiatives that seemingly revolve around theatreisation and single-service jostling for a larger share of the defence budget. For instance,

Air Commodore Kalianda A. Muthana, a distinguished former IAF test pilot, has highlighted the need to embrace an indigenous technology regime that ensures the ubiquitous and seamless connectivity of all sensors and shooters into what is known as a combat cloud (23).

An AI-enabled battlespace was one of the initial capabilities sought from the Defence Communication Network (DCN) deployed in 2016 (24). Ensuring the resilience of this network by continuously maintaining and updating hardware and software infrastructure would be vital. The hardware would include a constellation of satellites in different orbits, high-altitude pseudo satellites, terrestrial elements and manned/unmanned aircraft that can be launched quickly to cover gaps should the need arise. The newly formed Defence Space Agency has much ground to cover in this realm (25). Cyber deterrence must be part of such plans as the world moves well beyond only physical attacks. This is best achieved by building offensive capabilities and demonstrating it occasionally, as the Chinese allegedly executed on the Mumbai power grid. Among the several challenges faced by the Indian military will be integrating the operations of the Defence Space Agency and the Defence Cyber Agency.

After setting up the combat cloud, the next step will be to equip sensor/shooter elements with software-defined radios (SDRs) compatible with datalinks, thereby creating an IoMT (26). Currently, only IAF aircraft are equipped with SDR (27). Ideally, compatible SDRs must become standard equipment on all weapons platforms of the Indian armed forces' Only then can India achieve ubiquitous and seamless connectivity, thus enabling maximum compression of the sensor-to-shooter loop.

It is often easy to forget an essential element in IoMT—weapons. Suitable weapons must be considered an intrinsic part of the carrier platform during the design stage. All smart weapons must have a compatible datalink and become part of the IoMT. There must be a top-down flow of directives mandating the equipping of all weapon systems with compatible datalinks for them to play their role in IoMT. How sophisticated and resilient the IoMT is for the DCN to decide. Operationalising the IoMT involves conception, wargaming, and implementation (28).

The military leadership and combat personnel in the armed forces need to understand AI's strengths and limitations. This includes distinguishing between artificial narrow intelligence (ANI), which is the performance of tasks, and artificial general intelligence (AGI), which is the performance of jobs. While much progress has been made on AGI, wherein the AI tries to compete with the human brain, it is still many years away (29). At the same time, while developing and planning usable ANI resources, technological experts must be included in the programme groups to translate a war fighter's requirements into functioning AI-enabled operational deliverables. However, with a diverse arsenal of imported and indigenously manufactured 'smart' weapons, ensuring the compatibility of their data links with the larger combat cloud will be a massive challenge for India.

Global concerns over the use of space for offensive military applications have gained momentum in recent years, given the advances made by Russia and China in hypersonic weapons (30). But India is well-set to leverage the success of the Brahmos-1 Missile and engineer the Brahmos-2 as a hypersonic weapon that is expected to reach speeds of Mach 8 and hit targets at 600 kms and more (31)

Conclusion

Budgeting and resource allocation are among the prime challenges in this narrative. India's defence acquisition procedure evolves often; the last release was in September 2020, with an update in April 2022 (32). In the research and development (R&D) space, the formation of the Innovation for Defence Excellence) organisation and establishment of the Technology Development Fund are commendable steps. Air Commodore Muthana, however, argues that these only cater to small-ticket R&D items in the private sector but that there is a lack of courage to invest in larger areas. He also suggests that India create a Department of Defense Technology to monitor programmes like the Advanced Medium Combat Aircraft (AMCA) and other big-ticket items in future military technology programmes. This monitoring agency should ideally include military personnel and experts in various technical fields laterally inducted from within India and elsewhere. The sensitive and secretive nature of the institution is not currently critical since the country is in the nascent stage of developing its technological prowess. What would need to remain in the closed domain is the level of its adoption by the military, its deployment, and its operational philosophy (33).

India's armed forces will need to navigate the challenges of a two-front security conundrum in a volatile global and regional security environment for the next decade (34). To achieve this, its leadership must be doctrinally nimble, resource-conscious, technologically savvy, and flexible enough to remain grounded in India-specific operational realities.

Endnotes

(1) Air Commodore K. A. Muthana, "Fighting Future Wars: A Roadmap for Adoption of Disruptive Technologies In the Indian Context,'" *Council for Strategic and Defense Research*, Special Issue No. II; Policy Paper, December 2021, https://csdronline.org/upload/user/CSDR_KA_Muthana_An_Aerial_Prac_Perspective.pdf.

(2) Thomas J. Wright, *All Measures Short of War: The Contest for the 21st Century & the Future of American Power,* (New Haven, Connecticut: Yale University Press, 2017).

(3) Nitin Gokhale interviews Air Chief Marshal V.R. Chaudhari, 12 May 2022, https://www.youtube.com/watch?v=Kg1kFLIeFZI

(4) Ann Marie Dailey, "What's behind Russia's Logistical mess in Ukraine," *Atlantic Council*, 21 March 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/whats-behind-russias-logistical-mess-in-ukraine-a-us-army-engineer-looks-at-the-tactical-level/.

(5) Maj Gen B K Sharma (Retd), "Net Assessment of China's Strategic Forays in India's neighbourhood," *Bharat Shakti*, 03 May 2019, https://bharatshakti.in/net-assessment-of-chinas-strategic-forays-in-indias-neighbourhood/.

(6) Government of UK Press Release, *Announcement of new Director appointed to the Secretary of State's Office for Net Assesment and Challenge (SONAC)*, 06 May 2022, https://www.gov.uk/government/news/announcement-of-new-director-appointed-to-the-secretary-of-states-office-for-net-assessment-and-challenge-sonac

(7) Park Si-soo, "US, India agree to cooperate on space situational awareness", *SpaceNews*, 12 April 2022, https://spacenews.com/us-india-agree-to-cooperate-on-space-situational-awareness/.

(8) Robert Farley, "Managing the Military problem of Space: The Case of India," *The Diplomat,* 19 April 2021, https://thediplomat.com/2021/04/managing-the-military-problem-of-space-the-case-of-india/.

(9) "China flies airship at record altitude, higher than Mount Everest," *India Today*, 16 May 2022, https://www.indiatoday.in/science/story/china-flies-airship-at-record-altitude-higher-than-mount-everest-1949998-2022-05-16?utm_source=rss.

(10) Lieutenant General Hooda interviewed by Ananth Krishnan, "The LAC Crisis has been a wake-up call in how we deal with China says former Northern Command Chief," *The Hindu,* 08 May 2022, https://www.thehindu.com/opinion/interview/the-lac-crisis-has-been-a-wake-up-call-in-how-we-deal-with-china-says-former-northern-command-chief-lt-gen-ds-hooda/article65394688.ece.

(11) Snehesh Phillip, "Army Bets on Technology & not more troops in Eastern command to deal with China," *The Print,* 19 October, 2021, https://theprint.in/defence/army-bets-on-technology-not-more-troops-on-ground-in-eastern-command-to-deal-with-china/752788/.

(12) "India and US sign BECA,'" *The Hindu*, 28 October 2020, https://www.thehindu.com/news/international/india-and-us-have-signed-beca/article32962324.ece. Also see, https://www.defensenews.com/space/2020/10/28/india-us-sign-intel-sharing-agreement-amid-tension-with-neighboring-china/.

(13) Arjun Subramaniam, "Can Counter-Coercion work against a belligerent China," *ORF Expert Speak*, 24 July 2020, https://www.orfonline.org/expert-speak/can-counter-coercion-work-belligerent-china/; Arjun Subramaniam, "Air Power in Joint Operations in a Limited Conflict Against China," *ORF Issue Brief 374,* 26 June 2020, https://www.orfonline.org/research/air-power-in-joint-operations-68547/.

(14) Lt Gen Deependra Singh Hooda (retired), "Establishing Military Deterrence Against China," *Delhi Policy Group*, 06 September 2021, https://www.delhipolicygroup.org/publication/policy-briefs/establishing-military-deterrence-against-china.html. Also see Arjun Subramaniam, "IAF has enhanced India's deterrent and coercive posture in Ladakh," *Indian Express,* 23 November 2020, https://indianexpress.com/article/opinion/columns/power-in-the-air-7061634/.

(15) Nitin Gokhale interview with Air Chief Marshal Chaudhari

(16) Press Trust of India Report from Beijing, "Chinese soldiers in eastern Ladakh provided high-tech gear to manage winter," *The Indian Express,'* 29 October 2020, https://indianexpress.com/article/india/chinese-soldiers-in-eastern-ladakh-provided-high-tech-gear-to-manage-heavy-winter-military/.

(17) Raja Menon, "Reorienting Indian Military Grand Strategy: From Territoriality to Offensive Oceanic in the Indo-Pacific," Unpublished paper that argues for a more offensive Indian naval posture in the Indo-Pacific. The author was one of the practitioner-scholars to comment on the paper by Rear Admiral Raja Menon, one of India's leading scholars on the application of sea power.

(18) Air Marshal Diptendu Choudhury, "Expanding Role of PLAAF in China's Security Strategy," *Strategic Analysis, Vol 44*, Issue 6, (2020), pp. 521-541. The author argues that the only way in which India can counter the growing clout of China in the IOR is by leveraging the joint capabilities of the IAF and IN.

(19) Air Marshal VK Bhatia (Retd), "IAF to build NextGen Blast pens at Strategic Eastern Air Bases," *India Strategic,* February 2019, https://www.indiastrategic.in/iaf-to-build-nextgen-blast-pens-at-strategic-eastern-air-bases/.

(20) Rick Joe, "China's Growing High-End Drone Force," *The Diplomat,* 27 November 2019, https://thediplomat.com/2019/11/chinas-growing-high-end-military-drone-force/.

(21) Raghav Bhikchandani, "Heron, Searcher, Sea Guardian, SWITCH – the many UAVs that make up India's Drone Arsenal," *The Print,* 6 August 2021, https://theprint.in/defence/heron-searcher-sea-guardian-switch-the-many-uavs-that-make-up-indias-drone-arsenal/709670/; Snehesh Phillip, "As stand-off with China continues, India-made drones for LAC surveillance," *The Print,* 24 January 2022, https://theprint.in/india/as-stand-off-with-china-continues-army-orders-more-india-made-drones-for-lac-surveillance/811619/.

(22) Rajat Pandit, "From missiles to glide bombs, India set to test several advanced weapon systems," *Times of India,* 7 May 2020, https://timesofindia.indiatimes.com/india/india-all-set-to-test-several-homemade-weapon-systems/articleshow/91394150.cms.

(23) Air Commodore K. A. Muthana, "Fighting Future Wars: A Roadmap for Adoption of Disruptive Technologies In the Indian Context," *Council for Strategic and Defense Research*, December 2021, https://csdronline.org/upload/user/CSDR_KA_Muthana_An_Aerial_Prac_Perspective.pdf.

(24) "HCL Infosystems implements first-ever converged communication network between Indian Army, Navy and Air force," https://www.hclinfosystems.in/case-study-dcn/

(25) "HAL takes a leap of technology, to develop unmanned pseudo satellite that can fly unmanned for upto 3 months," *Times Now Digital*, 04 February 2020, https://www.timesnownews.com/india/article/hal-takes-a-leap-of-technology-to-develop-unmanned-pseudo-satellite-that-can-fly-unmanned-for-upto-3-months/715932.

(26) Air Commodore Muthana, 'Fighting Future Wars'

(27) Air Commodore Muthana, 'Fighting Future Wars'

(28) Air Commodore Muthana, 'Fighting Future Wars'

(29) Air Commodore Muthana, 'Fighting Future Wars'

(30) William Schneider, "China and Russia's hypersonic weaponry threatens US early warning system," *Financial Times*, 26 February 2022, https://www.ft.com/content/7d566088-7d25-4fde-9b02-311f86eb845e.

(31) Nitin J Ticku, "India's Hypersonic Missile: As DRDO Goes Vertical, US Speculates Indian Navy could go hypersonic by 2025-28," *Eurasian Times*, 15 December 2021, https://eurasiantimes.com/indias-hypersonic-missile-drdo-indian-navy-could-go-hypersonic/.

(32) Indian Ministry of Defense, *Defence Procurement Procedure*, https://www.mod.gov.in/dod/defence-procurement-procedure-dap

(33) Air Commodore Muthana, 'Fighting Future Wars'

(34) Sushant Singh, "The Challenge of a Two-front War: India's China-Pakistan Dilemma," *Stimson Center: Crisis and Consequences in Souther Asia Project,* 2021, https://www.stimson.org/2021/the-challenge-of-a-two-front-war-indias-china-pakistan-dilemma/

Blast from the Past: Return of High-Intensity Warfare?

Sameer Patil

In the international system, war is considered a systemic change-effecting device. It arguably represents "one of the most consequential events in human history", almost always with a high death toll (1). While many abhor war, it remains a ubiquitous and recurrent phenomenon. From the realist theory perspective, the condition of 'anarchy'—the absence of a common sovereign, an overarching authority, or a 'world government'— leads to conflict among nations as they must compete for security, political influence, material capabilities, and other scarce resources that are necessary for their survival (2). States cannot transcend this condition of anarchy.

In the post-Cold War era, many strategic experts argued that the global focus had shifted from high-intensity warfare and inter-state wars to low-intensity conflict and intra-state or civil wars. Some countries grappling with ethnic divisions, insurgencies, and separatist movements suddenly witnessed a surge in internal conflicts and clashes after 1991. The Bosnian civil war that began in 1992 and the Rwandan genocide in 1994 seemed to confirm this trend (3). For others, the September 2001 terrorist attacks in the US and the subsequent 'global war on terror' shifted the West's focus from adversarial regimes to transnational terrorist groups and terrorist safe havens (4). In response to these developments, certain countries changed their strategic doctrines, force postures, and military capabilities.

However, a scan of the strategic canvas and geopolitical developments at the dawn of the third decade of the twenty-first century reveals that we are amidst a shift, a fundamental break from the post-Cold War decades. From Russia's invasion of Ukraine and its disputes with the North Atlantic Treaty Organization, to China's territorial belligerence vis-à-vis its neighbours, and to the persistent simmering hostilities between traditional adversaries, these developments suggest that the world is heading towards an extended period of major-power competition. These developments have possibly acted as a catalyst for a return to high-intensity warfare.

This essay discusses the return of high-intensity warfare and how major militaries worldwide are gearing up for it. In addition, it examines the role of disruptive technologies and other military capabilities,

which distinguishes the present high-intensity warfare from its previous incarnations. Finally, the essay argues that the emerging great-power relations may lead several militaries worldwide to prepare for high-intensity warfare. Nevertheless, potential future conflicts will see a combination of high- and low-intensity warfare elements, as illustrated by the concepts of 'hybrid warfare', 'grey zone tactics', or 'campaign between wars'.

From the "Most Peaceable Era" to the "Age of Unpeace"

The end of the Cold War began a new era in international relations. Many experts argued that the onset of globalisation and the increasing economic interdependence brought a period of peace. War was seen as a threat to the global circulation of capital. So, the incentives for violence reduced dramatically.

In 1989, American political scientist John Mueller argued that a notion had developed about the obsolescence of war between major powers (5). Mueller attributed four reasons for this: lessons taught by the two world wars to avoid repetition at any cost; the advent of nuclear weapons; the elimination of a significant source of conflict with the decline of Communist ideology in the 1980s; and the belief that war is counterproductive in achieving prosperity and economic growth. Hence, great powers had rejected war as "unwise" and "a thoroughly bad and repulsive idea". More than two decades later, Canadian cognitive psychologist Steven Pinker echoed Mueller's sentiments when he claimed that humankind might be living in the "most peaceable era" ever (6). Looking at historical trends, Pinker argued that violence has declined over the past half-millennium and that no aspect of life is untouched by this "retreat from violence".

On another track, the September 2001 terrorist attacks quickly changed the military approach of the US and its allies. As the 2002 US National Security Strategy declared, "The United States of America is fighting a war against terrorists of global reach. The enemy is not a single political regime, person, religion, or ideology. The enemy is terrorism—premeditated, politically motivated violence perpetrated against innocents (7)." With this, fighting al-Qaeda and conducting counterterrorism became a major priority for the West, while conventional high-intensity conflict quickly lost its relevance as militaries re-assessed and reconfigured their force postures and deployments (8). However, in retrospect, this shift proved to be a transient phase. Two decades later, after al-Qaeda and later the Islamic State terrorist group were decimated through sustained counterterrorism and counterinsurgency operations, strategic competition between the West and its adversaries regained salience. Yet, the fundamental dynamics of security competition between the major powers had not altered.

Even as the world was getting closer and integrated, the fundamental security dynamics and sources of conflict were also being reinforced. As British political scientist Mark Leonard argued, "the connections that knit the world together" also drove it apart (9). Reminiscent of American political scientist Samuel Huntington's theory of a 'clash of civilisations', hyper-connectivity and hyper-interdependence unleashed disagreements and conflicts. These factors quickly paved the way for the "age of unpeace", primarily manifested through the evolving great power competition.

View from the Militaries

Rising tensions and competition between great powers are paving the way for high-intensity warfare, also described by some US military officials as a "near-peer conflict" (10). Some military historians, such as Victor Davis Hanson, have also used the terminology "tomorrow's war" to denote the enormity of destruction that the hostilities between major powers would cause (11).

Since the last decade, the world has seen widening tensions between US and China on the one hand, and Russia and the West on the other. Besides, competition and conflict have dominated every part of the world—from the Indo-Pacific to Europe, and from the Persian Gulf to the horn of Africa. In a sense, the Russian invasion of Ukraine in February 2022 is just a manifestation of these growing geopolitical rivalries.

Western militaries, which had been retooled to fight terrorist groups and low-intensity conflicts, only paid attention to the phenomenon of high-intensity warfare much later. In addition, this was also a recognition that the prevalence of these low-intensity conflicts had diverted attention from the training and preparation for future high-intensity warfare. For instance, the US National Defense Strategy of 2018 noted: "Today, we are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding. We are facing increased global disorder, characterized by decline in the long-standing rules-based international order—creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic competition, not terrorism, is now the primary concern in the US national security" (12). This was a watershed moment by turning the US away from the two-decades-long counterterrorism and counterinsurgency efforts in Afghanistan, Iraq, and Syria to pursue conventional military superiority vis-à-vis Russia and China (13).

This shift to high-intensity warfare was even more pronounced for the European militaries, which have witnessed the longest period of relative peace and stability since the Second World War. For years, France, just like the US, had focused on counterterrorism operations in the Sahel region of Africa. But in a significant reorientation of its military focus in 2021, the French military advanced the '*hypothèse d'engagement majeur*' (hypothesis of major engagement) to denote its conception of high-intensity warfare (14). The French defence ministry's Strategic Update of 2021 acknowledged the "resurgence of strategic and military competition" by Russia or China (15). It noted that multiple geopolitical developments, including heightened great power competition and emboldened regional powers, have created "tougher operating environments and the multiplication of fields of confrontation". As a result, the possibility of "a direct confrontation between major powers can no longer be ignored", and the French military will prepare for "scenarios of engagement in a major conflict." The UK also recognised this trend. In December 2021, its chief of defence staff had noted the need to "deter and defend against state-based opponents" (16).

For the West's adversaries, however, the possibility of high-intensity warfare and inter-state conflict always existed. For example, China's 2015 Military Strategy noted that in the foreseeable future, "a world war is unlikely, and the international situation is expected to remain generally peaceful" (17). However, it added that there are "new threats from hegemonism, power politics and neo-interventionism", and therefore, the world still faces both "immediate and potential threats of local wars." Likewise, Russia's

2015 Military Doctrine highlighted the main military threat to the country as "drastic aggravation of the military-political situation (interstate relations) and creation of conditions for using military force (18)." Therefore, to deter and prevent military conflict, Russia will assess "military and political situation at global and regional levels", and "the state of interstate relations in the military-political".

Evidently, Russia and China focused on high-intensity war, while the Western militaries anticipated this shift much later. As one expert put it, "The interventions in Afghanistan, Iraq, and even Mali in the case of France are today analyzed by Western political and military leaders as strategic distractions that have caused their armies to lose the reflexes of high-intensity combat and have allowed Russia and China to strengthen their capacity to cause harm, in their immediate neighborhood and beyond" (19).

Notably, China had studied the US military campaigns since the 1990-91 Gulf War and absorbed lessons from them in its military reforms to build the capabilities needed for high-intensity warfare.

Capabilities and Technologies for High-intensity Warfare

Today's high-intensity warfare undeniably denotes old-fashioned state-to-state warfare. But it is not an exact return to the 'trench and tank warfare' of the twentieth century. Instead, modern high-intensity warfare is differentiated from its earlier versions by the critical role disruptive technologies play in shaping contemporary military strategies and battlefield tactics. Moreover, there are now new spectrums of war, such as space, information, and cyber, which imply that states must develop full-spectrum capabilities to meet the challenge of their near-peer adversary. Different militaries have taken diverse routes to prepare for this inter-state warfare. Some, like the UK, are cutting down their troop strength and acquiring more tech platforms, such as unmanned systems, whereas others, like France, have not cut down on troops and are buying more conventional equipment (20), (21). The French approach appears to prepare for the worst-case scenario, i.e., when technology fails, it will be human courage and ingenuity that will matter the most on the battlefield.

That said, major powers worldwide are pursuing disruptive technologies with greater vigour and deploying them to bolster their military capabilities. These include artificial intelligence (AI), blockchain, autonomous systems, quantum computing, advanced sensors, swarming drones, and other unmanned aerial systems—technologies and systems that can keep up with the rapidly evolving battlefield situations and, therefore, give better situational awareness of the threat environment and remove troops from harm's way. It is no surprise that these technologies are alluring, and militaries are eager to deploy them on the ground to gain an advantage over their near-peer adversaries. Precursor systems enabled by these technologies include the US's AI-enabled submarine prototype, Russia's unmanned ground patrol vehicle, and Israel's Iron Dome missile defence system (22).

Since the end of the Cold War, Western militaries have been preoccupied with low-intensity warfare that required an entirely distinctive posture than one needed to confront a near-peer adversary. Consequently, the conventional military superiority that the Western militaries maintained in air defence, heavy armour, and electronic warfare capabilities stagnated, and its adversaries took the lead. A 2021 study by the French Institute of International Relations noted that between 1999 and 2014, European militaries allowed their tank fleet to dwindle by 66 percent, their fighter jet fleet by 45 percent, and their naval

fleet by 25 percent (23). During the same period, Russia and China massively expanded their defence spending to modernise their equipment. For instance, between 2000 and 2019, Russian military expenditure increased by 175 percent (24). Compared with the European countries, Russia's military spending in 2019 was US$ 65.1 billion, about 30 percent more than the individual defence budgets of France, Germany, and the UK.

As expected, this shrinking of the European militaries has affected their defence preparedness for high-intensity warfare. Resultantly, much of the recent effort has been to rebuild their military capability and upgrade existing equipment principally. Pierre Morcos and Colin Wall note that in the last two decades since the September 2001 attacks, European navies tasked with counterinsurgency duties had been reconfigured to prepare for several low-end missions, such as a fight against illegal trafficking, search and rescue, counterpiracy, or disaster relief (25). However, in recent years, they have reprioritised conventional capabilities. Now, they are spending money to buy more major surface combat ships, amphibious vessels, and submarines, and enhance their capacity for logistics, surveillance, and long-range strike. This approach is combined with heavy investments in information warfare and cyber capabilities.

The same impetus has fuelled the US military modernisation efforts in recent years (26). It is pursuing high-end conventional capabilities and weapons like air and missile defences, strategic airlift and mid-air refuelling capabilities, long-range artillery, long-range bombers, attack and reconnaissance aircraft, anti-ship weapons, hypersonic weapons, electronic warfare capabilities, and command-and-control networks. The aim is to ensure that the US can bring adequate firepower to a "high-intensity" battlefield against China and Russia (27). Eventually, the US wants to achieve what Secretary of Defense Lloyd J. Austin termed "integrated deterrence", spanning multiple domains across services and a range of capabilities (28).

A key element of preparing for this high-intensity warfare is training exercises that will ready the defence forces to simulate potential battle scenarios and organise accordingly. The Western militaries have carried out several exercises, such as the Polaris naval exercises in the Mediterranean Sea and the BALTOPS exercise in the Baltic Sea, replicating naval battles (29), (30). The manoeuvres of these exercises and emphasis on maritime operations reflect the participating nations' concern over similar potential high-intensity combat in the waters of the Indo-Pacific and the Atlantic Ocean, and their preference for fighting these battles with reliable allies. Likewise, the US Army and Marines have practised firing artillery from landing craft and transport docks to prepare troops for amphibious battles in the Pacific (31). Such drills have also helped to test logistical support and supply provisions for forces.

China, too, has pursued the same conventional capabilities, albeit with more determination. Its military reforms of 2015 have enabled the People's Liberation Army (PLA) to consolidate its forces and introduce new structures for 'integration' and 'informatisation'. For instance, as part of the reforms, the PLA created two new services: Strategic Support Force (SSF) and the Joint Logistics Support Force (JLSF). The SSF serves as the PLA's cyber, space, and electronic warfare branch, whereas the JLSF manages general and joint logistics support, including transport (32), (33).

The Russian invasion of Ukraine, in that sense, has served as a good example of how twenty-first-century high-intensity warfare can pan out. Russia's use of cyber and information warfare capabilities, simultaneous deployment of its conventional forces and its operational woes due to a lack of effective joint or combined arms operations have demonstrated the importance of jointness for high-intensity warfare.

Technological advancement in previously unknown domains of cyber and space, and pursuit of new high-end conventional capabilities have undoubtedly altered the nature of warfare. However, one feature that will remain common with twentieth-century inter-state warfare is the protractedness of the conflict—as seen by the fighting in Ukraine, where neither victory nor loss appears to be immediate tangible outcomes for Russia or Ukraine. And this will happen despite the wide capability gaps between the fighting militaries. Again, as demonstrated by Ukraine vis-à-vis Russia, some form of external support (formal alliance or informal assistance) will keep propping up the weaker adversary. This extended length of the conflict and the resulting stalemate will test the mettle of belligerents.

High-intensity Warfare or Hybrid Warfare?

It is clear that major militaries are preparing for high-intensity warfare by strengthening their conventional capabilities and pursuing innovations in disruptive technologies. Moreover, given the nature of contemporary great power relations, countries perceive high-intensity warfare as the most significant national security risk. Nonetheless, the nature of emerging threats today suggests that the world will see more hybrid warfare involving high and low-intensity warfare elements, rather than conventional inter-state warfare.

Hybrid warfare includes tactics like economic coercion, the use of proxies, disinformation and propaganda, and cyber warfare (34). The interdependence brought upon by globalisation has offered several new fronts for hybrid warfare, like cyberattacks and sanctions, to hit back at adversaries beyond the physical battlefield. Countries prefer using these tactics because they allow the pursuit of geopolitical objectives against their adversaries and stop just below the threshold of full-blown conventional military hostilities. Russia has optimised this type of warfare in Ukraine and Europe by raising 'malign influence networks', deploying private military companies and engaging in malicious cyber activity (35). Likewise, China has regularly used grey zone tactics against Taiwan and in the South China Sea. Given Russia and China's highly successful application of these tactics, countries will find hybrid warfare more advantageous. Hence, they will look for means and opportunities to use such tactics and rile their adversaries. The common use of disinformation and propaganda by several countries during crisis situations is one example of how hybrid warfare has become pervasive. This will undoubtedly change how militaries will be utilised (36).

A template like hybrid warfare is Israel's 'campaign between wars' strategy, also known as "the war between the wars". It combines many elements of hybrid warfare with Israel's modus vivendi of proactive, intelligence-based offensive actions (37). The chief aim of this strategy is to constantly weaken the adversary's conventional force accretion to thwart its strategic efforts (38).

In India's case, hybrid warfare has been a reality for many decades in the form of Pakistan's use of cross-border terrorism as a state instrument. This has allowed Pakistan to break through India's conventional superiority. In addition, it is now using cyberspace to breach Indian computer networks and engage in anti-India propaganda. So, even as India confronts China and Pakistan in the context of high-intensity conflict, the Indian military's joint doctrine recognises that future wars are likely to be "nonlinear", "unpredictable and hybrid" (39).

There is a recognition of this reality among the Western military planners too. France's Chief of Defense Staff General Thierry Burkhard underlined in his 2021 Strategic Vision his ambition for the French military to "win the war before the war (40)." Aligning with this assessment is the UK's Defence Command Paper, which conceded that, "The threats of today are different from those we are used to. Our adversaries no longer only seek to challenge us in open, large-scale warfare, but instead seek to use activities below the threshold of open war" (41).

Conclusion

The classic security dilemma and the consequent persistence of traditional rivalries have created a schism in contemporary international relations. It is reinforced by China's relentless pursuit of technology and military domination, the Russian invasion of Ukraine, and the West's swift and harsh retaliation through economic and technology sanctions. There are many other emerging domains of conflict, such as environmental issues and supranational Big Tech (42). Nevertheless, fractious great power dynamics will be the single most dominant factor in shaping national security policies and defence strategies of countries worldwide. This alone will ensure the relevance of high-intensity warfare and militaries' contingency planning. However, the path towards this warfare will be laden with various hybrid warfare instruments, which wsill blur the distinction between war and peace.

Endnotes

(1) Andreas Wimmer, "War," *Annual Review of Sociology* 40 (2014): 173.

(2) Marc Trachtenberg, "The Question of Realism", *Security Studies* 13, no. 1 (2003): 156-194.

(3) Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era*, (Stanford, California: Stanford University Press, 2001), pp. 104.

(4) Kanti P. Bajpai, *Roots of Terrorism*, (New Delhi, Penguin Books, 2002).

(5) John Mueller, *Retreat from Doomsday: The Obsolescence of Major War*, (New York: Basic Books, 1989), pp. 217.

(6) Steven Pinker, *The Better Angels of Our Nature: Why Violence has Declined*, (New York: Viking, 2011), pp. xx-xxi.

(7) The White House, President George W. Bush, "The National Security Strategy," September 2002, https://georgewbush-whitehouse.archives.gov/nsc/nss/2002/.

(8) Pierre Morcos and Colin Wall, "Are European navies ready for high-intensity warfare?," *War on the Rocks,* January 31, 2022, https://warontherocks.com/2022/01/are-european-navies-ready-for-high-intensity-warfare/.

(9) Mark Leonard, *The Age of Unpeace: How Connectivity Causes Conflict*, (London: Bantam Press, 2021).

(10) US Department of Defense, "Near-Peer Threats at Highest Point Since Cold War, DOD Official Says," March 10, 2020, https://www.defense.gov/News/News-Stories/Article/Article/2107397/near-peer-threats-at-highest-point-since-cold-war-dod-official-says/.

(11) Victor Davis Hanson, "Tomorrow's Wars," *City Journal,* Winter 2010, https://www.city-journal.org/html/tomorrow%E2%80%99s-wars-13258.html.

(12) US Department of Defense, "Summary of the 2018 National Defense Strategy of the United States of America", https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

(13) Billy Fabian, "Back to the Future: Transforming the U.S. Army for High-Intensity Warfare in the 21st Century," *Center for a New American Security*, November 19, 2020, https://www.cnas.org/publications/commentary/back-to-the-future-transforming-the-u-s-army-for-high-intensity-warfare-in-the-21st-century.

(14) Raphaël Briant , Jean-Baptiste Florant, and Michel Pesqueur, "The mass in the French armies: a challenge for high intensity," *French Institute of International Relations*, Strategic focus no. 105, June 2021, https://www.ifri.org/sites/default/files/atoms/files/briant_florant_pesqueur_masse_2021.pdf.

(15) Ministère des Armées, Government of France, "Strategic Update 2021," https://s.rfi.fr/media/display/e19540ea-b16e-11eb-b464-005056bff430/210300%20France%20defense%20strategic-update%202021.pdf.

(16) Ministry of Defence, Government of UK, "Chief of the Defence Staff Speech to the Royal United Services Institute," December 7, 2021, https://www.gov.uk/government/speeches/chief-of-the-defence-staff-speech-to-the-royal-united-services-institute.

(17) The State Council of the People's Republic of China, "China's Military Strategy," May 27, 2015, http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

(18) Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, "The Military Doctrine of the Russian Federation," June 29, 2015, http://rusemb.org.uk/press/2029.

(19) Alexandra de Hoop Scheffer, "Collective Defense is Now at the Forefront of NATO," *German Marshall Fund of the United States*, April 7, 2022, https://www.gmfus.org/news/collective-defense-now-forefront-nato.

(20) Ministry of Defence, Government of UK, "Defence in a competitive age," March 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974661/CP411_-Defence_Command_Plan.pdf.

(21) Stephanie Pezard, Michael Shurkin, and David Ochmanek, "A Strong Ally Stretched Thin: An Overview of France's Defense Capabilities from a Burdensharing Perspective," *RAND Corporation*, 2021, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA200/RRA231-1/RAND_RRA231-1.pdf.

(22) Sameer Patil, "The Future of War in the Age of Disruptive Technologies," *Observer Research Foundation,* April 26, 2022, https://www.orfonline.org/expert-speak/the-future-of-war-in-the-age-of-disruptive-technologies/.

(23) Briant, Florant, and Pesqueur, "The mass in the French armies: a challenge for high intensity," pp. 11.

(24) Siemon T. Wezeman, "Russia's military spending: Frequently asked questions," SIPRI, April 27, 2020, https://www.sipri.org/commentary/topical-backgrounder/2020/russias-military-spending-frequently-asked-questions.

(25) Morcos and Wall, "Are European navies ready for high-intensity warfare?"

(26) US Department of Defense, "As Prepared Remarks by Secretary of Defense Mark T. Esper at the Munich Security Conference," February 15, 2020, https://www.defense.gov/News/Speeches/Speech/Article/2085577/as-prepared-remarks-by-secretary-of-defense-mark-t-esper-at-the-munich-security/.

(27) Marcus Weisgerber, "Army Secretary Reveals Weapons Wishlist for War with China & Russia," *Defense One*, April 16, 2019, https://www.defenseone.com/business/2019/04/army-secretary-reveals-weapons-wishlist-war-china-russia/156347/.

(28) C. Todd Lopez, "Defense Secretary Says 'Integrated Deterrence' Is Cornerstone of U.S. Defense," Department of Defense News, April 30, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2592149/defense-secretary-says-integrated-deterrence-is-cornerstone-of-us-defense/.

(29) Xavier Vavasseur, "Here Is The Ship List For POLARIS 21: France's High Intensity Combat Exercise," *Naval News*, November 19, 2021, https://www.navalnews.com/naval-news/2021/11/here-is-the-ship-list-for-polaris-21-frances-high-intensity-combat-exercise/.

(30) Magnus Nordenman, "At BALTOPS, It's Back to Prepping for High-End Warfare," *Defense One*, June 14, 2017, https://www.defenseone.com/ideas/2017/06/baltops-its-back-prepping-high-end-warfare/138669/.

(31) David Axe, "High-Intensity Warfare Is Back and America Practicing for the Next Big Conflict," *The National Interest*, January 27, 2020, https://nationalinterest.org/blog/buzz/high-intensity-warfare-back-and-america-practicing-next-big-conflict-117491.

(32) Adam Ni and Bates Gill, "The People's Liberation Army Strategic Support Force: Update 2019," *The Jamestown Foundation*, May 29, 2019, https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/.

(33) Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *The Cyber Defense Review* 3, no. 1 (2018): 105–22.

(34) Andrew Dowse and Sascha-Dominik Dov Bachmann, "Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone'?", *The Conversation*, June 17, 2019, https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841.

(35) Todd Harrison and Nicholas Harrington, "Bad Idea: Conflating Great Power Competition with High-Intensity Conflict", *Center for Strategic and International Studies*, December 15, 2020, https://defense360.csis.org/bad-idea-conflating-great-power-competition-with-high-intensity-conflict/.

(36) Akshat Upadhyay, "Fighting Future Wars: Preparing India for Conflicts in the 21st Century", *Observer Research Foundation*, Issue Brief No. 525, March 2022, https://www.orfonline.org/wp-content/uploads/2022/03/ORF_IssueBrief_525_FutureWars.pdf.

(37) Gadi Eisenkot and Gabi Siboni, "The Campaign Between Wars: How Israel Rethought Its Strategy to Counter Iran's Malign Regional Influence", *The Washington Institute for Near East Policy*, September 4, 2019, https://www.washingtoninstitute.org/policy-analysis/campaign-between-wars-how-israel-rethought-its-strategy-counter-irans-malign.

(38) Yaakov Lappin, "Israel's Intelligence "Factory"", *BESA Center for Strategic Studies*, April 16, 2018, https://besacenter.org/israel-intelligence-factory/.

(39) Headquarters Integrated Defence Staff, Ministry of Defence, Government of India, "Joint Doctrine Indian Armed Forces", 2nd Edition, April 2017, pp. 10.

(40) Ministère des Armées, Government of France, "Strategic Vision of the Chief of Defense Staff," October 2021, https://www.defense.gouv.fr/sites/default/files/ema/211022_EMACOM_Strategic-Vision_UK_Vdef_HQ%20%283%29.pdf.

(41) Ministry of Defence, Government of UK, "The Defence Command Paper sets out the future for our armed forces," March 23, 2021, https://www.gov.uk/government/news/the-defence-command-paper-sets-out-the-future-for-our-armed-forces.

(42) Lydia Kostopoulos, "The Emerging Domains of Conflict in the 21st Century," Observer Research Foundation, Issue Brief No. 551, June 2022, https://www.orfonline.org/research/the-emerging-domains-of-conflict-in-the-21st-century/.

Can Economic Sanctions Replace Forces in Modern Warfare?

Kazuto Suzuki

Before Russia invaded Ukraine in February 2022, the US and NATO countries denied deploying troops in Ukraine and chose to avoid engaging in direct warfare with Russia, but they declared that they would impose massive economic sanctions if Russia invaded, thereby seeking to deter Moscow. As it turned out, Russia did not fear the economic sanctions, invaded Ukraine, and the fighting continues. In response, the US, the European Union (EU), and Japan have implemented broad economic sanctions against Russia (1), but this has not stopped Russia's military aggression.

Understanding Economic Sanctions

First, for economic sanctions to have any effect, a certain degree of economic interdependence must be established. Economic sanctions will not have an effect unless some "pain" is caused by politically severing such relations. During the Cold War, trade relations existed between the East and West, but they were not so interdependent that the economy could not survive if trade relations were severed. After the end of the Cold War, both Russia and China joined the World Trade Organization and became part of the free trade system. As a result, China's low production costs, high quality of labour, and infrastructure developed under the socialist system allowed it to acquire the role of the 'world's factory', and Western countries began to invest in China and integrate it into the global supply chain. On the other hand, Russia, armed with its rich underground resources, developed natural gas and oil pipelines to European countries, exported rare metals (such as palladium), and became a major resource power in the global economy. Thus, even countries with different regimes united under a free trade regime that promoted economic dependence, and the increased interdependence created the conditions for economic sanctions to be more effective.

It is important to note, however, that the implementation of economic sanctions in a state of interdependence means that the "pain" will be felt not only by the sanctioned country but also by the sanctioning country. Economic sanctions are those that restrict economic activities for political purposes. The most effective sanction against Russia is the suspension of natural gas imports from the country, which can place an economic burden on it by depriving it of foreign currency income. At the same time, European countries that depend on natural gas from Russia will see their economic and social activities severely restricted by the implementation of the sanctions. Significant restrictions on their economic and social activities, risk-facing electricity shortages, and other problems caused by natural gas shortages will become evident (2). The higher the degree of interdependence, the more effective the economic sanctions will be, but, at the same time, countries must be prepared for the risk of hurting themselves and the impact on their own economic activities and national policies. The problem has not surfaced because most sanctions have targeted relatively small economies (i.e., countries with asymmetrical interdependence), such as North Korea and Iran, but sanctions targeting economies of the size of Russia have revealed the difficulty of targeting countries with symmetrical interdependence. The difficulty of targeting countries with symmetrical interdependencies in sanctions targeting economies of the size of Russia became apparent.

Second, the effectiveness of economic sanctions may be limited because of political calculations in the target country. Economic sanctions produce their effects by placing an economic burden on the target country, making it difficult for the policy to continue, forcing policymakers to change their judgement, and increasing public pressure by making life difficult for the people. However, economic sanctions will not be effective if policymakers have a strong will and believe there are more benefits to continuing the policy than any economic burden that can be placed on them. For example, in the case of North Korea's nuclear development, Kim Jong-un, who has a dictatorial authority to make policy decisions, recognises that the development and possession of nuclear weapons is the most important issue for his country's survival and has not stopped nuclear development even amid widespread economic hardship. Although economic sanctions should make it impossible for North Korea to obtain the necessary materials for nuclear development, it has been able to obtain these materials and continue its policy by developing on its own, smuggling, and other means of evading sanctions. Also, although it should not be able to obtain the funds necessary for nuclear development, it is believed to be happening through means such as the theft of cryptocurrency in cyberspace (3). Economic sanctions will not be very effective if loopholes can be exploited.

Public opinion can greatly influence these formulas because economic sanctions inevitably affect the lives of citizens and impose restrictions on economic activity, with public discontent building up. However, in the case of authoritarian or dictatorial political regimes, such public discontent is often violently suppressed. In this respect, economic sanctions are more likely to have an effect when people can express their dissatisfaction in the form of elections, which in turn influence policymakers. For instance, the 2015 Iran nuclear deal was reached in large part because of the 2013 presidential election, which saw the election of Hassan Rouhani, a moderate who pledged to lift economic sanctions.

Third, economic sanctions must have some strategic objective. In other words, economic sanctions cannot be effective unless the purpose for which they are imposed is clearly communicated. In this regard, economic sanctions against Iran were set with the objective of halting its nuclear development, but since Iran never withdrew from the Treaty on the Non-Proliferation of Nuclear Weapons and positioned its

nuclear development as a "peaceful purpose" as a matter of course, the burden of economic sanctions became greater. However, the Iran nuclear agreement did not curb Iran's conventional weapons hegemony in the Middle East region, or reduce its influence over Iraq, Lebanon, and Yemen, and it has continued to pose a threat to Israel, which were among other strategic goals that were different from those of nuclear development, which led the Trump administration in the US to withdraw from the agreement and unilaterally reimpose sanctions. These sanctions are currently far from achieving their strategic goals, but this is partly due to the fact that they have not placed enough of an economic burden on Iran to exceed its resolve. Another problem is the many loopholes in the US unilateral withdrawal from the nuclear agreement and sanctions, as many countries are not cooperating with the sanctions due to a lack of legitimacy.

Economic Warfare in the Case of Russian Sanctions

Sanctions against Russia are broader and stronger than any imposed before by the US and the EU. However, from the perspective of effectiveness and if they can achieve strategic goals, they are not thorough sanctions even though they will likely have some effect.

European countries with deep interdependence on Russia were reluctant to impose energy-related sanctions because the sudden imposition of oil and natural gas embargoes would have a major impact on the economies and civilian lives within the European region. On the other hand, the US, which is less dependent on Russia, sought to implement energy sanctions first. At the same time, the G7 sought to demonstrate a united international position, but the US prioritised not giving Russia an opening to negotiate individually with other countries, which would disrupt the unity of the G7 and loosen the effects of the sanctions. The US also kept in step with the European countries and did not strongly pursue energy sanctions (the US suspended imports of Russian crude oil as part of its own sanctions).

However, Russia did succeed in limiting the sanctions to Western countries, while emphasising relations with Middle Eastern and African countries (with which it cooperates in the form of resource and grain exports, arms exports, and the provision of services by private military companies), as well as with China and India, whose behaviour is distinctly different from that of the G7. Therefore, it should be noted that the implementation of sanctions against Russia is limited to Western countries, while economic relations between Russia and the rest of the world continue.

To implement effective economic sanctions against Russia, it is important to stop fossil fuels such as coal, oil, and natural gas, which account for nearly half of Russia's exports, and unless the EU, Russia's largest trading partner and accounting for over 40 percent of energy exports from that country (4), stops its imports, the effect will be limited. It is often argued that even if Russia sanctions are implemented, China and India will not participate in the sanctions, creating a 'loophole' and making them less effective, but even though China is Russia's second-largest trading partner after the EU, it accounts for only 15 percent of Russian exports, and India only 1 percent (5). Even if the EU were to reduce its imports of Russian crude oil by 90 percent by the end of 2022, it would be difficult for China and India to take on all of the crude oil destined for Europe, making it a relatively small loophole.

More importantly, when the European Commission proposed a ban on Russian crude oil imports, Hungary, a landlocked country that procures Russian crude oil through pipelines, strongly opposed the proposal, and it took four weeks to reach an agreement. The Hungarian government has not hidden its anti-EU stance, claiming that the single market rules imposed by Brussels infringe on its national interests. This can also be seen as a result of Russian President Vladimir Putin's attempt to take advantage of the bickering among the EU member states to strengthen relations with Hungarian Prime Minister Viktor Orbán, thereby preventing coordination within the EU. In other words, it is difficult to implement effective economic sanctions when there is no consensus within the G7 and the EU.

This intra-EU disharmony is even more pronounced with sanctions over natural gas. For Germany and Central and Eastern European countries that depend on natural gas imports from Russia, sanctioning natural gas will have a major impact on economic activity and the lives of citizens, as they would not only lack fuel for their main source of power generation, but would also be unable to obtain the gas they need for heating and cooking. According to some estimates, Germany's participation in natural gas sanctions would result in a loss of about €220 billion (6). In the case of crude oil, storage is relatively easy, and more than two-thirds of Russian crude oil is transported by sea, so there are hopes that imports can be shifted to the Middle East and other oil-producing countries, but this is not the case with natural gas. Most natural gas is transported by pipeline, and if it were to be transported by sea, facilities would be needed to cool and liquefy the natural gas, transport it by tanker, and then vaporise it again. Large-scale facilities would also be needed to store stockpiles, and these would have to be newly constructed. In addition, there is a big difference between the cost of transporting natural gas by pipeline and the cost of transporting liquefied natural gas (LNG). Even if Russian natural gas were to be replaced by LNG, the cost would have to be recovered by raising gas prices, which would inevitably affect economic activities and the lives of citizens.

This European dependence on Russian fossil fuels means that, as a result, Europe will continue to buy fossil fuels from Russia, which suggests that it will continue to provide foreign currency to Russia. Gazprom, a Russian gas exporter, has also stopped supplying gas to Poland, Bulgaria, the Netherlands, and other countries ostensibly because they did not pay in rubles, but in reality, they were the victims of Russian retaliation (7). This dependence on Russia and the pressure exerted by Moscow to 'weaponise' its gas supply has resulted in the EU losing its footing and sanctions against Russia have not been thoroughly enforced. In other words, the 'loophole' in the Russia sanctions is not in China or India, but in Europe itself, and in this sense, the sanctions have the character of a 'doughnut' with a hole in the middle.

Sanctions against Russia by Western countries have been swiftly decided and aligned by Western countries, but they are imperfectly implemented because they are sanctions with little damage to themselves. These 'bottom-up' economic sanctions, designed to do as much as possible, have a major problem. The message is not clear as to what kind of behavioural change is required of Russia because of the sanctions. Economic sanctions must properly communicate strategic objectives. However, sanctions by the West are intended to sanction Russia because they cannot enter a war without a clear exit strategy in their minds.

If the strategic goal is to bring Russia's invasion of Ukraine to a ceasefire through economic sanctions, and for Russia to abandon the territory it has acquired and withdraw its troops, the current economic

sanctions are still not enough. It is not clear what Putin's war aims are, but at least he seems to have given up on his initial goal of a blitzkrieg attack on the capital, Kiev, and the collapse of the Zelenskyy regime, but he has concentrated his forces in eastern Ukraine and is aiming for full control of the Luhanshik and Donetsk oblasts of the Donbass region as well as two Southern oblasts of Zaporizhzhia and Kherson. As far as these strategic goals are redefined and the war is continued even at great cost, Putin's political will is firm, and even if economic sanctions make people's lives more difficult, he will not perceive it as an economic burden that would stop the war. If the strategic goal of the Western powers is to force withdrawal of Russian forces, they will need to step in with stronger sanctions, to the point of a natural gas embargo, even if it hurts themselves.

If the strategic goal is overthrowing the Putin regime, then the only way to achieve this will be through expressing dissatisfaction with the regime by the Russian people and an anti-regime movement, which will be difficult to induce through economic sanctions. Even if there is a buildup of discontent among the population, it is difficult to expect the anti-regime movement to gain momentum, given that dissident activists have been killed one after another in unnatural accidents or by chemical injections. In addition, although Russia is capable of regime change through elections, polls there cannot be said to be fair, and various forms of electoral fraud are said to take place (8) despite the involvement of international monitoring agencies. In such an environment, it is difficult to imagine that the impoverishment of people's lives due to economic sanctions will bring about regime change. Similarly, although sanctions have been imposed on oligarchs (newly emerging conglomerates) who support the Putin administration and their assets have been frozen, there is no indication at this point that they are going to bring down Putin, and such regime change cannot be expected.

What, then, is the goal of the economic sanctions by Western powers? Presumably, it is aimed at raising the cost of war and taking away the ability to continue the war. As long as Europe, China, India, and other countries buy oil and natural gas, Russia will have the money to continue the war, but more than that, the war will be costly. In addition, sanctions have forced Russian crude oil to be sold at a considerable discount, with the price of Urals crude oil, mainly Russian crude oil, being almost US$40 cheaper than North Sea Brent and other oil products. Furthermore, the menu of economic sanctions includes a ban on issuing Russian government bonds denominated in foreign currencies, making it difficult to issue war bonds to finance war expenditures. Given these circumstances, it is unlikely that the economic sanctions are aimed at an immediate ceasefire, withdrawal of troops, or regime change, but are likely to increase the cost of continuing the war in the hope that at some point Russia will run out of funds to continue the war and the population and Russian military will refuse to continue fighting. In addition, it is believed that the sanctions against Russia include product restrictions centered on semiconductors and other high-tech products, which will make it more difficult to obtain parts and other items needed for weapons production, and funds, thereby depriving Russia of the ability to continue the war.

Consequences of Sanctions

The economic sanctions against Russia are being implemented by the G7 countries, mainly because Russia has invoked its veto power in the UN Security Council, making it impossible for the UN to take any measures. The G7 countries are aligning themselves as Western countries to put pressure on Russia and make it difficult for the war to continue. Although economic sanctions affect not only the targeted

countries but also the business activities and the lives of the people of the implementing countries, they have been implemented with public support as a punishment for Russia's use of force in violation of international law to save the Ukrainian people.

However, these economic sanctions will not yield immediate results. Therefore, they will continue as long as the war continues, and even if a ceasefire is reached, it will be difficult to lift the sanctions unless Russia's occupation of Ukrainian land in violation of international humanitarian law (including by pro-Russian forces) is resolved. Since the purpose of the sanctions is not clearly stated, it is not even clear under what circumstances the sanctions should be lifted. As a result, there is a possibility that the sanctions will continue to be imposed without any opportunity for them to be lifted.

However, it will take a considerable time to achieve this because it will require the development of LNG storage and vaporisation facilities, and other related infrastructure. Germany has procured five vessels with facilities to vaporise LNG, but this is only temporary (9). If sanctions are to be effective in earnest, it will be important to reduce dependence on Russia even more than before.

However, the concern here is 'sanctions fatigue'. As long as the sanctions remain in place, the countries enforcing them will hurt themselves and will feel economic repercussions. Already, rising costs due to high oil prices are affecting people's lives, and global grain prices are also rising because Russia's Black Sea Fleet has stopped exports from Ukraine. These higher prices for raw materials necessary for daily life will make people's lives harder, and business with Russia will thin out, making it impossible for some companies to continue doing business. This will cause people to become dissatisfied even in countries where sanctions are in place, which will make it more difficult for Western countries to manage their regimes and result in a decline in support for them. If this happens, it is possible that at some point there will be a move to lift sanctions, even if fighting continues in Ukraine. In addition, there will be a disruption in the alignment among the Western countries, and Russia will probably try to take advantage of this by selling oil and natural gas at a discount to draw them into the Russian viewpoint. In addition, various disinformation and propaganda originating from Russia will be injected through social networking services to create a backlash within the Western regimes.

The Russian invasion of Ukraine is an event that is contrary to international law and must not be overlooked. The use of force by Russia, not to mention the Bucha massacre in June 2022, is violent and inhumane, and these acts must not be allowed to continue. Although Western nations will not deploy troops to Ukraine to engage Russian forces in direct combat, it is nevertheless important to make all efforts to deprive Russia of its ability to continue fighting by continuing to impose economic sanctions to make it easier for Ukrainian forces to fight. However, if the West stops the economic sanctions because of high energy prices and the damages to their economy, this will create an advantage for Russia, which may further intensify its attacks on Ukraine. To end this war, it is necessary to strengthen economic sanctions further, for governments to continue to explain the significance of economic sanctions to their citizens to make them aware of why and for what purpose these are being imposed to avoid a 'sanctions fatigue'.

Finally, the West and the world should prepare for future economic warfare. This is exactly why the Japanese Diet (parliament) passed the Law on Promoting Economic Security in May 2022. The law

provides opportunities for the government to intervene in commercial activities if there is a case of overdependence on foreign supplies. In times economic warfare, dependence—such as Europe's dependence on Russian oil and gas—is a weakness. Strengthening economic security and improving supply chain resilience is a form of armament, and building industrial and technological capabilities to make the country indispensable in supply chains is a protection of national interests.

Endnotes

(1) US Department of State, Department of the Treasury and Department of Commerce, *US Treasury-Commerce Alert: Impact of Sanctions and Export Controls on Russia's Military-Industrial Complex*, 2022, https://home.treasury.gov/system/files/126/20221014_russia_alert.pdf; European Council, *EU restrictive measures against Russia over Ukraine (since 2014)*, https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/; Centre for Information on Trade Security Council, *CISTEC service on sanctions on Russia <Japanese only>*, https://www.cistec.or.jp/service/russia.html

(2) Mark Flanagan, Alfred Kammer, Andrea Pescatori , and Martin Stuermer, "How a Russian Natural Gas Cutoff Could Weigh on Europe's Economies," *IMF Blog*, July 19, 2022, https://www.imf.org/en/Blogs/Articles/2022/07/19/blog-how-a-russias-natural-gas-cutoff-could-weigh-on-european-economies

(3) Choe Sang-Hun and David Yaffe-Bellany, "How North Korea Used Crypto to Hack Its Way Through the Pandemic," *New York Times*, July 1, 2022, https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html

(4) "In focus: Reducing the EU's dependence on imported fossil fuels," *European Commission*, 20 April 2022. https://ec.europa.eu/info/news/focus-reducing-eus-dependence-imported-fossil-fuels-2022-apr-20_en

(5) "How much oil, gas and coal India imports from Russia," *The Times of India*, Feb 17, 2022, http://timesofindia.indiatimes.com/articleshow/89631248.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

(6) "Joint Economic Forecast: From Pandemic to Energy Crisis: Economy and Politics under Stress," *Kiel Institute for the World Economy*, April 13, 2022, https://www.ifw-kiel.de/publications/media-information/2022/joint-economic-forecast-12022-from-pandemic-to-energy-crisis-economy-and-politics-under-permanent-stress/

(7) America Hernandez and Zia Weise, "Dutch and Danish gas buyers warn of Russian shutoff," *Politico*, May 30, 2022, https://www.politico.eu/article/netherlands-and-denmark-gas-buyers-warn-of-russia-shutoff-kremlin-gazprom/

(8) Rodion Skovoroda and Tomila V Lankina, "Fabricating votes for Putin: New tests of fraud and electoral manipulations from Russia," *Post-Soviet Affairs* (2016), pp. 1-24, https://eprints.lse.ac.uk/67182/1/Lankiina_Fabricating%20votes.pdf

(9) Federal Ministry for Economic Affairs and Climate Action, Government of Germany, September 1, 2022, https://www.bmwk.de/Redaktion/EN/Pressemitteilungen/2022/09/20220901-bmwk-charters-fifth-floating-lng-terminal-while-infrastructure.html

Strategic Instability Across Domains

Wilfred Wan and Nivedita Raju

Much has been said about the changing nature of warfare in the twenty-first century and the battlefields of the future. Initially, the discussion was geared towards conflict with actors who had become newly prominent on the international stage in the post-Cold War era, notably rogue states and terrorist groups. This narrative gained ground in the aftermath of the 11 September 2001 terrorist attacks in the US. Interrelated notions of asymmetric, unconventional, and unrestricted warfare—not necessarily new concepts—were acknowledged to have greater relevance against the backdrop of the altered international order and soon "dominating the lexicons of military and security forces," as well as security studies and international relations scholarship (1).

The common theme across these concepts centred on an expansive image of warfare and its combatants. Conflict itself encompassed new domains, including "social spaces such as the military, politics, economics, culture, and the psyche" (2). In an increasingly connected world, information superiority appeared critical, and indeed many experts specifically pinpointed the domain as likely holding future importance (3).

The potential spillover of conflict and blurring categories of engagement posed new challenges to international peace and security. This messier method of warfare has crystalised over decades, with the 1991 Gulf War (involving extensive use of space technologies), the Israel-Lebanon conflict in 2006 (marked by "novel applications of technology"), and the leadup to Russia's 2014 annexation of Crimea presenting what some have labelled "hybrid warfare" (4).

The Strategic Dimension

Irregular and unconventional methods have long been a feature of war and conflict. But it is the degree of hybridity that scholars point to as the defining characteristic of the contemporary era, with fewer

barriers, diversified actors, and new technologies playing a role in war that is "fought simultaneously in a number of spheres, on different levels, and in the never-ending, twenty-four-hour news cycle" (5).

Cyberspace—embedded in all aspects of society—has been designated in some military circles as a new operational domain (6). Outer space has also become important in light of expanding technologies and the increasing participation of new actors. National security doctrines and strategies of states account for this increasingly multidimensional nature of security threats, with some alluding to notions of multidomain strategic stability (7).

This essay examines how the defining trait of hybridity—interplay across domains—impacts the strategic context, considering ramifications for nuclear deterrence and related risks, arms control and disarmament.

In recent months, Russia and the US, and China and the US, have made modest strides towards respective bilateral strategic stability talks (8). The more holistic approach among the so-called 'great powers' suggests a viable option for supplanting the Cold War legacy nuclear arms control agreements that have largely fallen by the wayside. Yet, for these talks to produce concrete outcomes, there remains a need for all sides to better understand cross- and multidomain developments, underpinning strategic armament dynamics, and related threat perceptions. This essay seeks to contribute to that discussion.

Interplays Past

Cross-domain interactions have been part and parcel of the strategic conversation since the dawn of the nuclear age. Electronic warfare predates the Manhattan Project, and, while not considered by military strategists at the time to be taking place in a separate operational domain, was characterised by an emphasis on tipping the information scale. Operations that centred on jamming radar and radio equipment, including in navigation and guided missile systems, carried on through the Cold War—albeit now with potential nuclear consequences (9).

The US and Soviet Union engaged in efforts to interfere with each other's strategic communications, even exploring the electromagnetic effects of a high-altitude nuclear detonation on electronic systems (10). Some have claimed that the US developed a sophisticated plan to identify the "military-operational, technological, and intelligence requirements" necessary to target Soviet command and control—an expansive approach to undermining the adversary's retaliatory capability (11).

The interplay between cyberspace, outer space, and nuclear weapons has deep historical roots as well, as the development of the computer network is entangled with that of missile defence. Operational in the 1960s, the US Semi-Automatic Ground Environment (SAGE) air defence system consisted of computerised control centres linked together by digital signals; the system coordinated and processed data from hundreds of radar sites (12). SAGE was the precursor of the Ballistic Missile Early Warning System, which operated in conjunction with missile detectors and reconnaissance satellites in orbit (13).

Recognising the accompanying escalation risk, the US and Soviet Union signed the 1971 Accidents Measures Agreement, aiming to prevent the outbreak of nuclear war linked to interference with

early warning and communications systems (14). Multilateral treaties also prohibited the testing and deployment of nuclear weapons in outer space. Despite these constraints in the space race, not all forms of weaponisation were curtailed, with many gaps left by the 1967 Outer Space Treaty and applicable space law (15).

In a harbinger of the current era, technological progress rather forcefully reshaped the strategic context. The space-nuclear nexus acquired new significance in the 1980s, as the deployment of anti-satellite weapons by the superpowers drove a "clearer awareness of the dangers of a military escalation in space" (16). Nevertheless, the dangers grew.

US President Ronald Reagan's 1983 announcement of the Strategic Defense Initiative (SDI), an ambitious effort to channel decades of research into an advanced comprehensive missile defence system, relayed Washington's intent to undermine the Soviet strategic arsenal. The initiative, dubbed "Star Wars," envisaged the deployment of hundreds of space-based interceptors (17). Moscow responded to what it perceived as a direct threat to its deterrence capability, and the arms race resumed. While SDI ultimately failed, the US reorientation to a mixture of offensive and defensive systems had altered the strategic calculus, creating governance and regulatory challenges in bilateral and multilateral fora.

The State of Play

Technological developments in the twenty-first century have had clear ramifications for cross-domain interactions, including in the context of nuclear risk, arms control, and disarmament. While a thorough accounting is beyond the scope of this essay, this section identifies common trends across cyberspace and outer space.

Expanded capability

A growing number of states have developed national cyber defence doctrines and devoted immense resources to that sector, underscoring the strategic value placed on the domain. While less is known about cyber offensive capabilities, these have likely followed suit, given the blurred line between offence and defence. Indeed, states are more frequently conducting operations through foreign connected infrastructure, and the planning and scale of operations have grown as well (18).

The distributed denial-of-service attack on Estonia in 2007 marked a watershed moment, both in its widespread effect across state infrastructure and in the manner in which the operation was "integrated and synchronised" with economic and diplomatic activity for strategic effect (19). Meanwhile, the 2010 Stuxnet computer malware directly impacted physical equipment—altering the frequency of motor operations of centrifuges at Iranian nuclear facilities while suppressing damage detection tools (20). Cyber operations in 2022 on satellite internet services provided by commercial company Viasat resulted in large-scale disruptions in Ukraine and parts of Europe (21). Even the most secure systems may be vulnerable to such sophisticated operations. Nuclear modernisation plans will only intensify connectivity across nodes, creating new entry points for potential intrusion (22).

Similar trends are evident in the space domain. "Counterspace," a term encompassing the broad set of capabilities or techniques used to gain space superiority, is growing among several states—extending beyond the 'great powers' (23). Notably, the development of these capabilities includes offensive and defensive elements.

A particularly concerning aspect of this trend is increased "destructive" (also called "debris-creating") testing of direct-ascent anti-satellite weapons (24). Since 2007, anti-satellite tests have been conducted by China, India, Russia, and the US, resulting in the creation of considerable amounts of space debris—and posing additional hazards for all other users of space. Moreover, the most recent of those tests, by India in 2019 and Russia in 2021, featured the use of repurposed missile defence systems striking their targets (25). All of this underlines the cross- and multidomain dynamics linked to these technologies and capabilities.

Expanded involvement

Hand-in-hand with advancements in capabilities in cyberspace and outer space is the widened range of stakeholders involved in both domains. The Council on Foreign Relations reports that 34 states, including all nine nuclear-armed states, are suspected of having engaged in cyber operations since 2005 (26).

The defining traits of cyber conflict—including its asymmetric nature, low cost of entry, and difficulty in attribution—have made it an attractive proposition for non-state actors as well. While those groups tend to be motivated by financial gain, some have taken actions related to military and security affairs. Perhaps more concerningly, there exist incentives for states to employ non-state actors to carry out operations on their behalf, including by providing political and legal shielding, especially in the context of pursuing "limited strategic goals" (27).

Dynamics in space activities have similarly transformed, with outer space no longer accessible only to a small group of states. In addition to China, Russia and the US, which have advanced counterspace capabilities, the pursuit of these technologies has significantly increased among other states, with smaller and middle powers becoming more active (both independently and in coordination with one another).

Counterspace capabilities, for instance, are being developed by an expanding group that includes Australia, France, India, Iran, Japan, North Korea, South Korea, and the UK (28). Some, however, argue that the growing capacity has potentially given these countries greater influence over ongoing governance discussions at the multilateral level (29).

The private sector's rate of innovation has also increased across a broad range of commercial activities, such as space tourism and space resource utilisation. That sector has also begun to develop technologies for orbital debris removal to mitigate the impact of generated debris. Given the inherently dual use—and potentially dual purpose—nature of commercial activity, exponential and unregulated growth underscores the need for a multidomain and multistakeholder approach.

Expanded convergence

Cyber operations comprise part of the growing array of non-kinetic capabilities that can directly threaten space-based assets. However, even beyond the direct interplay across those domains, developments in each are linked to and, in some cases, facilitate other technological processes with strategic implications, including the link between missile defence systems and anti-satellite capabilities discussed earlier. There are many other examples, for instance:

- The digitalisation and networking associated with nuclear modernisation will likely be accompanied by the greater incorporation of machine learning and automation, including for data processing tasks linked to early warning systems (30).
- Global Positioning System satellites and sensors in space will further enable the guidance systems of hypersonic missiles and other conventional precision-strike capabilities that are impacting the strategic balance.
- Cyberspace is also fundamentally transforming the practice of information warfare, with the proliferation of capabilities threatening to poison the information ecosystem and alter the environment that critically provides decision-makers with needed "contextualized, reliable, [and] trustworthy information" (31).

All of these can complicate the practice of nuclear deterrence.

Significance for Nuclear Risk

Reflecting realities on the ground, the national security doctrines and strategies of some nuclear-armed states seem to extend the role of nuclear deterrence beyond traditional domains—or at least create the space for them to do so.

The 2018 US Nuclear Posture Review, which cited "significant non-nuclear strategic attacks" as an example of the extreme circumstances that could drive consideration of nuclear use, expressly includes cyber as an example of a non-nuclear strategic threat (32). The Russian Federation lists as one of its conditions for possible nuclear response an "attack by adversary against critical governmental or military sites… disruption of which would undermine nuclear forces response actions" (33).

With respect to the domains considered in this essay, it is significant that the document does not narrow the type of attack (kinetic or non-kinetic) nor the placement of the sites considered (terrestrial or in space).

Even without express doctrinal change, there is a broader recognition of the altered strategic environment, and the need for nuclear deterrence to function alongside other capabilities to act against "all forms of aggression" and manage "the full spectrum of possible conflicts" (34). For instance, while China reiterates the unequivocal nature of its no first use policy, Chinese scholars have openly suggested it revisit that policy in the context of cyber operations (35). It is also revealing that its officials cite US activities in "nuclear, outer space, cyber and missile defense" as examples of its provocative behaviour

(36). Overall, developments across domains appear to be creating additional points of contention, contributing to what the UK has labelled a "more complex range of routes for escalation" (37).

Indeed, the trends mentioned above in cyberspace and outer space suggest new and varied modes of nuclear deterrence failure, as well as a greater number of actors who can set these into motion. The purposeful ambiguity afforded in nuclear doctrines, in general and with respect to new domains, can lead to red lines being crossed inadvertently, for instance, with the undermining of a state's assured second-strike or retaliatory capability in a manner that prompts a 'use it or lose it' scenario. Cyber operations that affect the operations of ballistic missile submarines or nuclear early warning systems constitute a direct means to this end (38). Another path involves space operations that put infrastructure critical to nuclear command, control, and communications at risk, a possibility exacerbated by increased activity in space and the entanglement of nuclear and non-nuclear assets (39).

The intertwined nature of strategic considerations and the impact of capabilities, activities, and behaviours beyond their individual domain have other implications for deterrence-related risk in terms of probability and consequence. There exists a litany of cyberspace and outer space-related operations with potentially destabilising effects, with the ability of these to disrupt reliable communication, upend the information ecosystem (and feed into the 'fog of war'), or extend the effects of conventional operations.

Such events can contribute to more prolonged crises and affect the nuclear decision-making calculus, thus indirectly driving escalation pathways. The presence of sophisticated capabilities in other domains also raises the possibility of horizontal escalation and harder-to-contain conflict. These risk trends appear likely to continue, given the scope, pace, and incorporation of technological advancement.

Pathways Forward

As recent history demonstrates, multidomain interactions complicate not only risk but nuclear arms control and disarmament processes as well. Principles of mutual restraint and numerical parity, the cornerstone of bilateral Cold War-era agreements, have less relevance in an environment marked by more actors, more asymmetries, more capabilities, and more interconnectivity between them. For instance, the direct linkage between offensive missiles, missile defence, and space security, already marked by "continual 'strategic tension," provides clear challenges to policymakers seeking to address these capabilities (40). At the same time, negotiations that consider their interplay will have to account for their individual nuances, for instance, the nature of missile deployments, theatre- and tactical-level missile defence integration, and dual-use space activities. The task at hand is considerable.

Reducing escalation risk

During the Cold War, concerns about escalation pathways centred primarily on lower-level, regional conventional confrontation that could spiral into full-scale nuclear war. In the aftermath of the Cuban Missile Crisis, the US and Soviet Union developed a toolkit to guard against that possibility.

In addition to establishing a direct communications link between Washington and Moscow in 1963, the two sides addressed military behaviours and incidents that could be seen as provocative, establishing

procedures for regulation in the Agreement on the Prevention of Incidents On and Over the High Seas (1972), the Agreement on the Prevention of Nuclear War (1973), and the Prevention of Dangerous Military Activities Agreement (1989).

These were a critical complement to a suite of agreements that curbed specific nuclear-related capabilities, including the Anti-Ballistic Missile Treaty (1972), the Strategic Arms Limitation Talks/ Treaty I and II (1972 and 1979), and the Strategic Arms Reduction Treaty (1991). They also became the foundation for a larger conflict-prevention and management framework under the auspices of the Organization for Security and Co-operation in Europe (the Vienna Document of 2011) and the model for several US-China memorandums of understanding.

A comparable architecture in cyberspace and outer space will help mitigate escalation pathways linked to these domains, both horizontal and vertical. There are already traces of a foundation, from longstanding international space treaties to the two 2021 UN consensus reports on information and communication technology in the context of global security. Yet a narrower focus is critical.

The bilateral US-Russia and US-China hotlines for cyber incidents could act as a bridge to further information exchange and restraint in that domain, including in the context of cyber military exercises or declaring certain sectors "off-limit" from cyber operations (41).

States could also consider updating the agreements mentioned above on military behaviours and incidents to include non-kinetic capabilities such as cyber operations—this could be a logical extension of existing provisions on lasers, for instance. Similarly, existing Nuclear Risk Reduction Centers in Washington and Moscow, whose scope expanded in 2017 to consider cyber incidents between those states, can serve as a model—for other configurations of states as well as issues in other domains (such as outer space) with strategic considerations. Specifically in space, a similar incidents hotline among key players would be welcome. Statements by Lt. Gen. Saltzman of the US Space Force demonstrate that there is scope to pursue such a measure (42).

The 1971 Accidental Measure Agreements could be updated to reflect developments in the space environment and incorporate contemporary threats to nuclear early warning and command, control, and communications. Additionally, states could look to enhance the implementation of previously proposed transparency and confidence-building measures (43).

These include reaching a common understanding on terms and thresholds; improving mechanisms for collective reporting of activities; committing to prenotification for scheduled manoeuvres and uncontrolled high-risk re-entry of space objects; and broader engagement in information-sharing, including on a unilateral basis.

All this would help reduce the risk of misunderstanding, misperception, and miscalculation that could drive escalation. Private sector technologies and engagement could enhance these efforts, for instance, in the context of data-sharing on space situational awareness capabilities.

Rethinking Arms Control and Disarmament

Interactive dynamics across domains, and the increasing presence of hybridity in warfare, necessitate a fundamental recalibration of arms control concepts, particularly strategic stability. Cyberspace and outer space domains are not conducive to traditional means of verification. Moreover, there is little appetite for constraints on specific capabilities or systems in those domains.

What is necessary, and perhaps more plausible at this stage, is an open-ended dialogue that allows stakeholders to jointly explore how such systems are employed and exchange key assumptions, perceptions, and concerns (44). This discussion can pave the way for regularised engagement, covering the strategic impacts of developments across domains and identifying specific behaviours of concern. Perhaps—as with the Strategic Arms Limitations Talks—this can help to facilitate the confidence-building required to develop agreements to address these.

Bilateral strategic stability talks—referred to at the outset—provide a vital piece of the puzzle. Yet, expanded capabilities, engagement, and convergence across domains call for the development of parallel tracks, involving different configurations of stakeholders and considering domains individually as well as their nexus.

The P5 process, which brings together the five NPT nuclear weapon states (China, France, Russia, the UK and the US), had identified 'strategic risk reduction' as a priority topic: the framing seems a natural conduit for such states to explore risk stemming from cross-domain interactions. Meanwhile, discussions in the UN open-ended working group on space security could present guidance in identifying responsible and irresponsible behaviours in outer space (while acknowledging the complementarity of norms and legally-binding treaties). The two UN reports on cyberspace have already proposed a series of multilateral cooperation and transparency measures (45). As states take these proposals forward, they would be remiss not to consider those capabilities, activities, and behaviours in the broader strategic context, including their ramifications for nuclear deterrence and related risks. After all, the expansive nature of warfare necessitates a similarly holistic approach to international peace and security.

Endnotes

(1) Roy Thornton, *Asymmetric Warfare: Threat and Response in the Twenty-First Century* (Cambridge: Polity Press, 2007), pp. 7.

(2) Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), pp. 206.

(3) Steven Metz, *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare* (Carlisle: Strategic Studies Institute, 2000); Jeffrey McKitrick et al., "The Revolution in Military Affairs," in *Battlefield of the Future: 21st Century Warfare Issues*, eds Barry R. Schneider and Lawrence E. Grinter (Maxwell Air Force Base: Air University Press, 1998), pp. 36.

(4) Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* 52 no. 37 (2009), http://intelros.ru/pdf/jfq_52/9.pdf; Alexander Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe," *International Affairs* 92 no.1 (2016), https://www.jstor.org/stable/24757841#metadata_info_tab_contents.

(5) Dmitri Trenin, "Avoiding U.S.-Russia Military Escalation During the Hybrid War," *Carnegie Endowment for International Peace: U.S. Russia Insight*, 2018, pp. 2, https://carnegieendowment.org/files/Trenin_Hybrid_War_web.pdf

(6) Lesley Seeback, "Why the Fifth Domain is Different," *The Strategist*, 2019, https://www.aspistrategist.org.au/why-the-fifth-domain-is-different/.

(7) Government of the United Kingdom, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, 2021, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/; State Council, People's Republic of China, *China's National Defense in the New Era*, 2019, https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

(8) Russia and the US convened their dialogue three times and established two working groups prior to the invasion of Ukraine in February 2022.

(9) Research Institute of Swedish National Defence on Electronic Warfare, *FOA Information from the Research Institute of Swedish National Defence on Electronic Warfare* by Martin Fehrm, 1967, https://apps.dtic.mil/sti/citations/ADA111468.

(10) Beyza Unal and Patricia Lewis, "Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences," *Chatham House*, 2018, https://www.chathamhouse.org/2018/01/cybersecurity-nuclear-weapons-systems.

(11) Benjamin B. Fischer, "CANOPY WING: The U.S. War Plan That Gave the East Germans Goose Bumps," *International Journal of Intelligence and CounterIntelligence,* 27 no. 3 (2014), pp. 439, https://www.tandfonline.com/doi/abs/10.1080/08850607.2014.900290.

(12) Stephen J. Lukasik, "Why the Arpanet was Built," *IEEE Annals of the History of Computing*, 2011.

(13) Bin Cheng, "The United Nations and Outer Space," *Current Legal Problems,* 14 no.1 (1961).

(14) US Department of State, *Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War Between The United States of America and The Union of Soviet Socialist Republics (Accidents Measures Agreement),* 1971, https://2009-2017.state.gov/t/isn/4692.htm.

(15) Almudena Azcarate Ortega, "Placement of Weapons in Outer Space: The Dichotomy Between Word and Deed," *Lawfare Blog*, 28 January 2021, https://www.lawfareblog.com/placement-weapons-outer-space-dichotomy-between-word-and-deed (accessed 31 May, 2021).

(16) Daniël Goedhuis, "Some Observations on the Efforts to Prevent a Military Escalation in Outer Space," *Journal of Space Law* 10, no. 1 (1982), pp. 13.

(17) Paul Meyer, "Ballistic Missile Defense and Outer Space Security: A Strategic Interdependence," *UNIDIR Space Dossier*, 2020, pp. 11, https://unidir.org/publication/space-dossier-file-6-ballistic-missile-defence-and-outer-space-security-strategic (Meyer).

(18) Andraz Kastelic, "International Cyber Operations: National Doctrines and Capabilities," *UNIDIR*, 2021, https://unidir.org/cyberdoctrines.

(19) Una Aleksandra Bērziņa-Čerenkova et al., "Hybrid Threats: A Strategic Communications Perspective," *NATO Strategic Communications Centre of Excellence,* 2019, pp. 52, https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79.

(20) Doreen Horschig, "Cyber-Weapons in Nuclear Counter-Proliferation," *Defense & Security Analysis* 36, no. 3 (2020), pp. 352-371.

(21) "KA-SAT Network cyberattack overview," *Viasat*, Mar. 30, 2022, https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/; Matt Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine," *Wired*, Mar 23, 2022, https://www.wired.com/story/viasat-internet-hack-ukraine-russia/

(22) Andrew Futter, "The Danger of Using Cyberattacks to Counter Nuclear Threats," *Arms Control Today*, 2016, https://www.armscontrol.org/act/2016-07/features/dangers-using-cyberattacks-counter-nuclear-threats.

(23) Brian Weeden and Victoria Samson, eds., "Global Counterspace Capabilities: An Open-Source Assessment," Secure World Foundation, 2022, https://swfound.org/counterspace/ (*Weeden and Samson*).

(24) Nivedita Raju, "A Proposal for a Ban on Destructive Anti-satellite Testing: A Role for the European Union?" *EUNPDC Non-Proliferation and Disarmament Papers,* no. 74 (2021).

(25) Raju, "A Proposal for a Ban on Destructive Anti-satellite Testing: A Role for the European Union?"; Nivedita Raju, "Russia's Anti-Satellite Test Should Lead to a Multilateral Ban," *SIPRI*, 2021, https://www.sipri.org/commentary/essay/2021/russias-anti-satellite-test-should-lead-multilateral-ban.

(26) Council on Foreign Relations, "Cyber Operations Tracker," 2020, https://www.cfr.org/cyber-operations/#OurMethodology

(27) Johan Sigholm, "Non-State Actors in Cyberspace Operations," *Journal of Military Studies* 4, no.1 (2013), pp. 24.

(28) Weeden and Samson, "Global Counterspace Capabilities: An Open-Source Assessment."

(29) Rajeswari Rajagopalan, "Changing Space Security Dynamics and Governance Debates," in *Commercial and Military Uses of Space,* eds. Melissa de Zwart and Stacey Hendersen (Singapore: Springer, 2021), pp. 165.

(30) Jill Hruby and M. Nina Miller, "Assessing and Managing the Benefits and Risks of Artificial Intelligence in Nuclear-Weapon Systems," *NTI Paper*, 2021, https://media.nti.org/documents/NTI_Paper_AI_r4.pdf.

(31) Herbert Lin, "The Existential Threat from Cyber-Enabled Information Warfare," *Bulletin of the Atomic Scientists* 75, no. 4 (2019), pp. 189.

(32) US Department of Defense, *Nuclear Posture Review 2018*, 2018, pp. 21, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEWFINAL-REPORT.PDF.

(33) President of the Russian Federation, *Basic Principles of State Policy of the Russian Federation on Nuclear Deterrence*, 2020, para. 19.

(34) Foreword by the French Minister of the Armed Forces, *Strategic Update 2021*, 2021, https://cd-geneve.delegfrance.org/Defence-and-National-Security-Strategic-Review-1890; Inter-Services Public Relations of Pakistan, *Press Release no. PR-133/2013-ISPR*, 2013, https://www.ispr.gov.pk/press-release-detail.php?id=2361.

(35) Qin An, "Nuclear deterrence needed to prevent cyberattacks from paralyzing China's nuclear response," *Global Times*, 24 August 2020, https://www.globaltimes.cn/page/202008/1198665.shtml?id=11.

(36) State Council Information Office of the People's Republic of China, *China's National Defense in the New Era,* 2019, http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm.

(37) UK Government, *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy,* 2021, pp. 72, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf

(38) Wilfred Wan, Andraz Kastelic, and Eleanor Krabill, "The Cyber-Nuclear Nexus: Interactions and Risks," *UNIDIR*, 2021, https://doi.org/10.37559/WMD/21/NRR/03.

(39) John Borrie, "Nuclear Risk and the Technological Domain: A Three-Step Approach," in *Nuclear Risk Reduction: Closing Pathways to Use*, ed. Wilfred Wan, *UNIDIR*, 2020, https://doi.org/10.37559/WMD/20/NRR/01.

(40) Meyer, "Ballistic Missile Defense and Outer Space Security: A Strategic Interdependence."

(41) Steven E. Miller, "Nuclear Hotlines: Origins, Evolution, Applications," *Journal for Peace and Nuclear Disarmament* 4, no. 1 (2021), https://doi.org/10.1080/25751654.2021.1903763.

(42) Sandra Erwin, "One way to help prevent wars in space? Military hotlines with Russia and China," *Spacenews*, 3 November 2021, https://spacenews.com/one-way-to-help-prevent-wars-in-space-military-hotlines-with-russia-and-china/.

(43) United Nations General Assembly, *Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities*, UN document A/68/189, 2013.

(44) Lora Saalman, "Multidomain Deterrence and Strategic Stability in China," *SIPRI Insights on Peace and Security,* 2022, https://www.sipri.org/sites/default/files/2022-02/sipriinsight2202_multidomain_deterence_china.pdf.

(45) United Nations General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN document A/76/135, 2021; United Nations General Assembly, *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/AC.290/2021/CRP.2, 2021.

The Next Generation of Warfare: Grey Zone Operations

Amarjit Singh

Understanding war has been the main preoccupation of nations. The primordial desire of humankind to dominate is achieved through a victory in war, which means making the enemy 'do our will'. The historical and contemporary understanding of war is using the element of the military instrument of national power to destroy the capacity and capability of the enemy to resist the imposition of our will. In the classical understanding of war, the primary tool is the use of physical violence. Underlying all other objectives of war is the inherent human urge to become the 'hegemon' in group-based social hierarchies. The threat of competition must be eliminated to retain hegemony, and this leads to war. War is a play of offence and defence; one imposing its will on the other, and the other resisting to prevent acquiescing. War is all about attaining more power by using your power. In the prosecution of war, Vilfredo Pareto's 'Elite Theory of Power' holds good. Irrespective of being a democracy or an autocracy, political power lies in the hands of a small elite, and war is one of the instruments to increase this power.

According to Prussian general and military theorist Carl von Clausewitz, "War has an enduring nature that demonstrates four continuities: a political dimension, a human dimension, the existence of uncertainty and that it is a contest of wills" (1). These continuities are still valid in modern-day war, which reinforces that the nature of war is constant. There must be a political objective decided by the elites, which is generally supported by a majority and executed by the military in conditions of uncertainty in respect of the ultimate outcome. The change of warfare comes in the form of its character, which involves the mode of conduct, strategies, and technologies. In general, militaries detest change. They thrive on tradition. These inherent characteristics dictate that changes in warfare are slow evolutionary processes. But there comes a time when military leaders of genius or a breakthrough in technologies bring about spectacular victories that become a compulsion to follow. Whenever such a

revolution happens, military historians and strategists call it a change in the generation of warfare or a military revolution.

The Many Generations of Warfare

American scholar William S. Lind laid out a framework for understanding the revolution of war through four generations that are differentiated through military objectives, weapons, and strategy (2). The first generation denotes the use of physical strength with a workforce organised in rank and file. War was a direct physical confrontation of men with personal weapons. The objective in the first generation of warfare was the destruction of the enemy's military strength, which denoted the fall of the complete nation.

The second generation was characterised by the use of massed firepower, which resulted from the advent of the machine gun and artillery, and because this trench warfare developed in the early stages of the First World War. The range of their weapons determined the physical distance between opposing soldiers, and the rate of attrition was the deciding factor.

The third generation of warfare evolved to defeat the trench war. This was done by the speed of movement of firepower, with the aim of encircling the enemy. The deciding factor in the third generation of warfare was the mental and physical dislocation of the enemy by manoeuvre of firepower and creating a surprise. It was the tank that enabled this effect on the battlefield. The third generation broke the linearity of the battle geometry where targets in depth could be addressed before the front-line breaks.

The fourth generation is where the state loses its monopoly on war, and there is a return to a world of nations and cultures. This warfare is characterised by blurring the lines between war and politics, and combatants and civilians. The three levels of war—strategic, operational, and tactical—are converged and become interchangeable. Small teams operating at tactical levels achieved strategic outcomes. Asymmetric warfare and the reinvention of guerrilla warfare were the distinguishing features. Terror became one of the weapons to impose one's will on the opponent. The term hybrid war aptly defines the fourth generation of warfare, where conventional war is coupled with insurgency, terrorism, cyber war, and informational dominance to defeat the enemy. Analyst and author Frank Hoffman defines hybrid war as a "blend of the lethality of state conflict with the fanatical and protracted fervour of irregular war (3)." With the fourth generation of warfare in place, nations can fight a war by proxy by empowering groups to fight on their behalf while retaining the deniability of their involvement.

Now, the fifth generation of war is being discussed, which can be defined as "not physically violent — but it's culturally, socially, and economically violent" (4). This warfare is primarily executed through non-kinetic military action, such as social engineering, misinformation, and cyberattacks using emerging technologies, such as artificial intelligence (AI) and fully autonomous systems. Fifth-generation warfare has also been described as a war of "information and perception" (5) where the warrior hides in the shadows, geographically isolated from the battlefield, fighting the battle in cyberspace to destroy the enemy's economic and social assets. The weapons used here are information and cyber technologies, which target the perceptions, controls the narrative, and destabilises the economy.

Notably, the arrival of the new generation of warfare does not make the previous generation obsolete. Indeed, it is perhaps only the first generation of war that has been pushed to obsolescence, while all other generations of warfare can be fought concurrently. The war in Ukraine demonstrates a distinct second generation of war, using the trenches and fortifications being adopted by the Ukrainians and the use of massed artillery fire by the Russians. This war has also demonstrated manoeuvre warfare (third generation) by the use of large, mechanised columns that attempted to encircle Kiev and Mariupol. The fourth generation of warfare is being conducted by the special forces of Russia and Ukraine as also from other countries in the form of mercenary troops. The fifth generation of war is in the news and social media, which is whipping passions, changing perceptions, and spreading misinformation (as many as 200,000 cyber experts from all around the world responded to the Ukrainian president's call for help in cyber and perception management) (6). The fact remains, as Lind says, "Whoever is first to recognize, understand, and implement a generational change can gain a decisive advantage. Conversely, a nation that is slow to adapt to generational change opens itself to catastrophic defeat" (7).

The Sixth Generation of Warfare

The next generation of warfare—the sixth generation—is already underway, but this terminology is still to be acceptable in the study of warfare. A study of the battlefield indicators and the extrapolation of the trends, along with a pragmatic judgement, can showcase a general picture of the future of war.

Some of the characteristics of the next generation warfare will be:

- War will be a clash of ideologically opposing cultures and civilisations. Territorial and economic equations will not be the foremost objects of war.
- War is no longer a violent conflict between states. It is a clash of a state against a group, usually a proxy of another state. The war may just be between two civilisations. The "state", as defined by the Treaty of Westphalia, will soon lose its identity and nations, and civilisations will assume power.
- War will not be declared; it will start covertly and remain covert till it is nearing its culminating point. The target nation may not realise that it is under attack until the death blow is struck.
- War will not be fought along defined borders; it encompasses the whole of the nation. The geographic space will not be important. The psychological space in the minds of the leaders (elites) and masses will be the centre of gravity.
- Controlling the minds of the population by selectively delivering information or misinformation will be key. Psychological manipulation and striking terror will be the aim of war plans. Mass casualties and control of geographical area will lose their bargaining value. The assessment of victory in terms of territory gained and casualties inflicted is no longer valid. The factors of victory assessment will be the number of minds that one can capture through terror, coercion, or bribery and forced to conform. Defence, therefore, must be built to save the "mind" from manipulation. Victory will be assessed in terms of psychological subjugation of leaders of opponents to voluntarily change their way of life and society and give up their power to the aggressor. This conforms to the basic nature of war, of imposing your will on the enemy, but is grossly in variance with the conventional understanding of the physically violent character of war.
- Psychological tools will be the weapons of choice, and conventional forces will be used only in the endgame to claim victory. Non-military means of coercive power and tools of terror

> will be the new weapons of mass destruction. Psychological tools will profile individuals, and extensive communications and automation will attack each person individually with a barrage of misinformation to subvert their mind to acquiesce to the aggressors' will.

The term for this new form of war is cognitive warfare, where the human mind is the battlefield (8). The aim of this new warfare is to bring about change in what people think, and how they think and act. It shapes beliefs and group behaviour and has the potential to fracture and break up an entire society in such a way that its leaders and masses do not have the collective will to resist the offensive intentions of the aggressor. The whole aim of war can be achieved without the application of violent force or terror. Surprisingly, the groups that are more susceptible to this type of warfare are politically connected and the averagely well-informed and educated.

A few countries have very secretly analysed this new character of warfare. The US has understood it after fighting and losing conventional wars in Vietnam, Afghanistan, and Syria. On the other hand, Russia has been studying a new concept for the last 20 years and has demonstrated its prowess in this kind of warfare in Georgia (9), Crimea, and Chechnya. Russia has also been accused of altering voting choices in the 2016 US presidential elections. In 2013, Russian Chief of the General Staff Valerii Gerasimov stated, "The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of weapons in their effectiveness" (10). China has demonstrated its prowess in this kind of warfare by venturing in the darknet. This is the new war of information where the main weapons systems are psychological, robotics, AI, and mass media. A new form of Cold War has emerged, and there are three visible leading global players—Russia, China, and the US. There may also be smaller players that are invisible, who are probably more powerful and better equipped to win the future war. As part of an ambitious effort to restore his military to its former Soviet glory and likely beyond that, Russian President Vladimir Putin has prioritised not only electronic warfare but also the use of AI, which he famously called "the future, not only for Russia, but for all humankind" in a September 2017 back-to-school speech to students in Yaroslavl. "Whoever becomes a leader in this sphere will be the master of the world," Putin said, "And I would very much like it that there is no monopoly of this in any specific pair of hands (11)." This declaration of seeking power is probably the cause of the current Ukraine war, which overtly seems to be a conventional war, but the real war is a proxy war by the US on Russia, which is the battle of minds to prove who the evil power is.

The recent unveiling of China's new PSYOP (psychological operations) aircraft, the Gaoxin-7 (12), marks an important step forward for People's Liberation Army's psychological warfare capabilities. What it carries onboard is unknown. Meanwhile, the US has initiated the 'Disinformation Governance Board', with President Joe Biden stating "There is truth and there are lies. Lies told for power and for profit. And each of us has a duty and responsibility, as citizens, as Americans, and especially as leaders – leaders who have pledged to honor our Constitution and protect our nation — to defend the truth and to defeat the lies" (13). What he has actually initiated is a defence mechanism to save the minds of Americans. All these are battle indicators that China, Russia, and US are well into the art of warfighting the sixth generation of war, while the prowess of the other countries remains unknown.

The war of the mind space will need a different approach. The weapons for this kind of war will be big data, individual profiling, psychological toolkits, AI, and the media for communications, each being a weapon of mass destruction. The objective of the war will be to attain reflexive control over the target

population. Reflexive control can be defined as a "means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action" (14). Russians apply this concept to cause a stronger adversary to voluntarily choose the actions most advantageous to Russian objectives by decisively shaping the adversary's perceptions of the situation. Russia's modern information warfare adapts Soviet reflexive control to the contemporary geopolitical context to compel the enemy to act according to the desired plan and incline him to make predetermined decisions voluntarily. This means a nation can be defeated without knowing it has lost. The subjugation of smaller nations by western culture is an example. The US has control over many smaller countries through reflexive control. This warfare controls the decision-making process of the target. To stretch the argument to the current Ukraine war, it can be said that the US has reflexive control over the president of Ukraine and Russians have it over the people of Donbas.

The decision-making process of individuals is controlled by input information. This input information forms the basis of the next generation of warfare. The business world has already perfected the control of inputs by manipulating the results in search engines, pushing advertisements, and controlling the reviews of products. The war preparation starts with data collection. Data has already been collated by social media giants and is traded as a commodity over the internet. This data is used to generate a profile of individuals or a group to understand their core values and cultural beliefs. The leadership of nations is a special target. This data supplies information of the target population's behaviours and likes and dislikes. Psychological tools are applied to gauge the type of inputs to be supplied to the target. The functioning of the mind and its responses forms the basis for designing the kind of information or misinformation that must be fed to generate the desired decision. The designed inputs are fed through trusted social media to individuals separately or to a group. The inputs are repeated, forced in through as many devices as possible, until the decision-making of the individual or group is altered.

What Lies Ahead

This type of warfare is not exactly new; Adolf Hitler used it during the Second World War. Indeed, a few of the principles he crafted are still being used in some form today. Hitler postulated that propaganda was an important tool to win the conventional war. According to him, to be effective, propaganda must avoid abstract ideas and appeal to emotions; it should be constantly repeated using stereotyped phrases; only one side of the argument should be given; opponents must be criticised, and one enemy must be chosen for special vilification. Joseph Goebbels perfected the art of using propaganda, and can be credited in some way for the advent of the sixth generation of warfare. His principles of propaganda are well-documented and studied (15). Over the years, the art of influencing the mind in warfare has been playing out in the background, but with new technologies and AI, the form of warfare is becoming a major complement of war and can attain political goals by itself.

The Arab Spring, the Orange Revolution, the Trump presidential campaign, the expansion of NATO, and the media blitzkrieg against China and Russia are some of the overt operations that can be attributed to the sixth generation of war. The very character of this type of war is covert and, therefore, most of these operations happen without anyone's awareness. How the superpowers in this type of warfare are manipulating us will not be known because we are made to feel confident of our decisions.

There is research going on that is still in the realm of secrecy. For example, consider the 'Joshua Blue' project by IBM. The Joshua Blue programme aims at "evolving an emotional mind in a simulated environment (16)." It aims at enhancing AI by evolving such capacities as common-sense reasoning, natural language understanding, and emotional intelligence, acquired in the same manner as human minds acquire them. The main goal of Joshua Blue is to achieve cognitive flexibility that approaches human functioning. In other words, this is AI that could be diffused with our thoughts because it has been designed to 'think like a human'. NASA is also developing a computer programme that can silently read spoken words by analysing nerve signals in our mouths and throats. It does not take much to realise that the US agencies have access to a perfected version of this technology. NASA's signals intelligence monitors the brainwaves of their targets by satellite and decodes the evoked potentials that the brain emits. As such, by using lasers/satellites and high-powered computers, the agencies have now gained the ability to decipher human thoughts from a considerable distance.

Power has generally been defined in military and economic terms. Geopolitical theories have been based on the heartland, rim land, sea power, or China's Belt and Road Initiative. It is now time for a geostrategist to present a theory that is based on the acquisition of power through the control of minds. The new hierarchy of hegemony will be defined by information domination, which will be characterised by the exploitation of big data and AI to attain reflexive control over the target's decision-making process. Superpower status will be defined in the capacity to handle data and weaponise it to control people's minds and make them do your will. It may be a rational assumption that some technologies and strategies have been adopted from ideas in fictional work, comics, and movies, and if so, it may be relevant to quote Morpheus from the movie *Matrix* (1999): "It is the world that has been pulled over your eyes to blind you from the truth... That you are a slave, Neo. Like everyone else you were born into bondage. Born into a prison that you cannot smell or taste or touch. A prison for your mind".

Endnotes

(1) Carl von Clausewitz, "On War," Michael Howard and Peter Paret, eds and trans (Princeton: Princeton University Press, 1984), pp. 89.

(2) William S. Lind et al., "The Changing Face of War: Into the Fourth Generation", *Marine Corps Gazette*, October 1989, pp. 22–26, https://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html

(3) Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly*, issue no. 52, 1st Quarter (2009), https://smallwarsjournal.com/documents/jfqhoffman.pdf

(4) Umair Haque, "Ten Rules for 5G Warfare," *Harvard Business Review,* August 14, 2009, https://hbr.org/2009/08/obamas-war-and-how-to-win-it

(5) Daniel H Abbott, eds., *The Handbook of 5GW* (Nimble Books, 2010)

(6) Ariel Bogle and Dylan Welch, **"International hackers answer Ukraine's call to launch cyber operations against Russia,"** *ABC NEWS***,** March 2, 2022, https://www.abc.net.au/news/2022-03-02/hackers-answer-call-in-ukraine-russia-war/100873490

(7) William S. Lind and Gregory A. Thiele, *4th Generation Warfare Handbook*, (Castalia House Kouvola, Finland, 2015) www.castaliahouse.com

(8) Johns Hopkins University and Imperial college London, "Countering Cognitive warfare: Awareness and Resilience," *NATO Review,* 20 May, 2021, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

(9) Ariel Cohen and Robert E. Hamilton, *The Russian Military and the Georgia War: Lessons and Implications* (Carlisle: US Army Strategic Studies Institute, 2011)

(10) Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War" *In Moscow's Shadows*, (2014), http://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/#more-2291

(11) Radina Gigova, **"Who Vladimir Putin Thinks Will Rule the World,"** *CNN*, September 2, 2017, https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html

(12) Aaron Jensen, "China Prepares for Psychological Warfare," *The Diplomat*, 14 August, 2013, https://thediplomat.com/2013/08/china-prepares-for-psychological-warfare/

(13) Global Engagement Centre, "Disarming Disinformation: Our Shared Responsibility," US Department of State, https://www.state.gov/disarming-disinformation

(14) Timothy L Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Studies, Taylor and Francis Group,* (2004), https://www.tandfonline.com/doi/abs/10.1080/13518040490450529

(15) Leonard W. Doob, "Goebbels' Principles of Propaganda," *Public Opinion Quarterly*, (1950) pp 419-442

(16) Sam S. Adams et al., "Project Joshua Blue: Common Sense via Common Experience," *IBM Research*

(17) Nancy Alvarado et al., "Project Joshua Blue: Design Considerations for Evolving an Emotional Mind in a Simulated Environment," *IBM, Thomas J. Watson Research Center, International Conference on Robotics and Automation (ICRA'99),* Vol. 4, Page(s): 2868 –2873

Cyberattacks Against Satellites by Non-State Actors: The Attribution Problem

Ashok G.V.

In a prelude to the Russia-Ukraine conflict, the European Union, the UK, and the US issued statements condemning the Russian attempts to disrupt satellite communication services offered by Viasat, a private corporation based out of the US (1). Though the intended target of the cyberattack presumably was the Ukrainian military communication infrastructure, civilians were affected in equal measure. While the consequences of this cyberattack did not escalate beyond the disruption of communication, cyberattacks represent a more fundamental threat to the sustainability of space since they risk creating debris when they temporarily or permanently affect the functionality of space objects.

Also, cyberattacks are not traditionally associated with state action alone and is often undertaken by non-state actors (2) who may or may not be acting on behalf of the State. Given this trend, the traditional problem statements around attribution, such as the burden of proof in the context of cyberattacks, represents an opportunity for states to undertake cyberattacks with plausible deniability, taking shelter under the defence that rogue non-state actors undertook the attack. However, when the cyberattack is directed towards an object in space and there exists potential to disable its functionality, whether temporarily or permanently, the very sustainability of space is threatened. With the potential ramifications being as severe and long-lasting as the Kessler syndrome (3), there is a need to examine the question of attribution in cyberattacks against space objects to determine the impact, if any, of international space law on the subject of attribution and the consequential questions of state responsibility.

The current legal landscape represents a curious conundrum pertaining to the question of attribution in non-state-driven cyberattacks against space objects. This conundrum can be understood by exploring

the link between state responsibility and attribution. Attributing a cyberattack to a state invites state responsibility for the consequences. Thus, a lesser burden of proof translates to greater certainty of state responsibility and a higher burden of proof lessens the probability of state responsibility. In instances of state responsibility with respect to a violation of international law, the aggrieved party can access a variety of rights for relief, including reparations and the right to respond in self-defence (4), subject to the principles contained in the United Nations Charter.

However, far removed from the terrestrial theatre of conflict, space as a theatre of warfare represents complex challenges. If, for example, there exists evidence to suggest that one State is complicit in a cyberattack against a satellite in use by another state, a proportionate response in self-defence would likely involve an attack against a satellite in use by the aggressor state. However, such an exercise of the right of self-defence by the aggrieved State exacerbates the risk of space debris, even though it would be a legitimate expression of the State's rights under the laws of armed conflict. Such action, while lawful, is counterintuitive to the overall objective of preserving the delicate sustainability of space, a principle sacred to international space law. Therefore, the question of attribution involving attacks against space objects raises unprecedented complexities and requires a careful analysis of international law.

Space Law and Jus Cogens

A wrongful act resulting from a breach by a state of any international obligation that is essential for protecting the global community's fundamental interests constitutes an international crime (5). Examples of such crimes include colonial domination, slavery, genocide, apartheid, and massive pollution of the atmosphere of the seas (6). The particular instance of the pollution of the atmosphere of the seas holds parallels for the current discussions around space. To be specific, the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies ('Outer Space Treaty') (7) suggests that space is today what the international waters have always represented, a global resource held for the common benefit of all (8). Therefore, there exists sufficient foundation to argue that the sustainability of space assumes the same importance to humankind as does the cause of preventing pollution of the seas. Indeed, one could argue that the very scheme of the Outer Space Treaty alludes to space as a resource as common to humankind as the sea.

As an extrapolation of the principles of *jus cogens* that emerge in the context of the international space law, states are obligated—under international telecommunications laws, and under the constitution, convention, and regulations of the International Telecommunication Union (ITU) regulations—to prevent harmful interference in telecoms operations (9), the transmission of false or deceptive distress, urgency, safety or identification signals, and to collaborate in locating and identifying stations under their jurisdiction that transmit the same. Given that in the context of a cyberattack against a satellite, the deployment of malicious code or malware, in whatever form and manner, qualifies as a space activity, it attracts the prohibition contained against harmful interference under Article 45 of the ITU regulations (10).

Yet, even the most pacifist principles contained in the Outer Space Treaty or ITU regulations still do not account for the rights accrued to a nation under the law of armed conflict (11). Be it a kinetic or a cyberattack against a satellite, under specified circumstances to be determined in accordance with the

law of armed conflict, targeting a satellite or a space object is permitted, especially where such satellite or space object aids the military activities of a party to the conflict.

Based on this brief analysis of international space law, international telecommunications law, and the law of armed conflict, the following emerges:

- Freedom of access to space is a sacrosanct feature of international space law and potentially qualifies as jus cogens.
- Thus, states are under an obligation to not undertake any attacks against satellites or space objects, except in accordance with the law of conflict and the UN Charter.
- Though the duty of a state to investigate the source of a cyberattack in its territory and to extend cooperation to the victim state is not very clear under international law, an analogous principle to that effect is found in a state's obligation to prevent the transmission of false or deceptive signals from its territory under Article 47 of the ITU regulations.

Attribution in Cyberattacks Against Satellites/Space Objects

The question now is if there is a violation of the obligations and principles of international law identified in the preceding section vis-à-vis cyberattacks against satellites or space objects, especially at the hands of non-state actors, what, if any, is the responsibility of states?

An analysis of scholarly work on attribution in the context of cyberattacks reveals a common pattern: the high burden of proof to be satisfied to attribute a cyberattack to a state and thus invite state responsibility (12). Typically, and in principle, attribution of a cyberattack to a State can be undertaken on the basis of a State either authorising the attack or persons in positions of power and authority within the State undertaking such actions (13). Alternatively, as held in the case of the *United States of America v. Iran* (14), the failure of a state to discharge a duty (15) under international law could also invite responsibility under the principles enunciated in Article 11 of the Draft Articles of State Responsibility.

But be it commission or omission, attribution of an internationally wrongful action to a State is often an impossible task, as is evident from the finding of the International Court of Justice in the Nicaragua case (16), where despite the court's determination that the US had provided subsidies and other support to the Nicaraguan contras, it ultimately concluded that the evidence did not prove that the US exercised control over decisions made in the field by the persons accused of the internationally wrongful actions.

However, while these sources of law do provide some guidance on the questions of attribution in case of cyberattacks, the limitations they impose on grounds of burden of proof can, to some extent, be mitigated when the cyberattack targets a space object due to the operation of Article VI of the Outer Space Treaty (17). Activities on the Earth also qualify as space activities when they involve activities or otherwise achieve effects in outer space, such as the control of space objects (18).

In such a scenario, the fact that a non-state actor acted without authorisation by the State may still not offer a defence to state responsibility under Article VI of the Outer Space Treaty. This can be inferred from the judgement of the International Court of Justice in the case of *Bosnia and Herzegovina v Serbia and Montenegro* (19), where it was held that though the persons indulging in internationally wrongful

acts acted outside of the scope of the State's internal laws, the fact that such internationally wrongful acts were undertaken based on "complete dependence" on the State still invites state responsibility. Contextual evidence around a cyberattack—such as the target State, the targeted device, and the scale of an attack itself—can provide information regarding the identity of the attacker (20) and, therefore, it would be difficult to presume that the State was not complicit in a cyberattack against a satellite or space object as that requires both sophisticated infrastructure, capabilities, networks, and intelligence (21).

Furthermore, due to the regulatory measures under domestic law reflecting the regulations of the ITU, activities on the ground undertaken to communicate with satellites are often the subject matter of lawful intercept and monitoring powers of the licensing State. Since mounting a cyberattack against a satellite involves infrastructure and telecommunication capabilities, which are subject to significant regulations and licensing under domestic law, one could argue that a cyberattack against a satellite could not have happened if not for the complete dependence on the State or at least without the knowledge or the means to such knowledge of the State. As such, a state whose territory is used to mount a cyberattack faces the legal risk of responsibility under principles far less cumbersome than the ones employed to attribute actions to the State for non-space cyberattacks. Thus, the principles that emerge for the attribution of cyberattacks to a state are as follows:

- Due to the operation of Article VI of the Outer Space Treaty, whether an attack against a satellite is mounted by a state or a non-state actor, the nation from whose territory such an attack is mounted is internationally responsible for the same.
- States are under an active obligation to prevent their territory from being used to mount cyberattacks contrary to international law, by employing reasonable standards to comply with the requirements against harmful interference under Article 45 of the ITU regulations.
- A failure to cooperate in investigating the source of a cyberattack originating from its territory could offend the spirit, if not the letter, of Article 47 of the ITU regulations.
- Even if one were to step outside the perspectives of the Outer Space Treaty, given the sophisticated infrastructure and telecoms capabilities required to mount such a cyberattack against a satellite, the State from whose territory it is mounted, especially if such state reserves powers of intercept and monitoring over telecoms, could attract responsibility on the basis of the "complete dependence" principles and on principles of not taking sufficient steps to prevent the breach of the obligations under the Outer Space Treaty and Articles 45 and 47 of the ITU regulations.

Ramifications of Attribution Specific to Space Law

While the legal position, based on an assessment and review of international space law, suggests a lesser burden of proof to achieve attribution and, therefore, heightened state responsibility, the consequences that arise from such attribution and state responsibility remain unclear. For example, in the *Enrica Lexie* case (22), though the actions of the Italian marines in opening fire on Indian fisherman was held to be reasonable (23), Italy was directed to pay compensation as such an action, even if reasonable under the circumstances, still violated India's rights under the law of the sea (24). It remains to be seen whether a similar stand will prevail under the Liability Convention (25) for an attack mounted on a satellite.

Perhaps one could argue that given the ITU framework permits lawful intercept and monitoring of telecommunication activity (26), the State in whose territory the cyberattack is mounted has a duty to

prevent its territory or infrastructure from being used for such purposes (27), and to investigate (28) and report its findings to the State aggrieved by the cyberattack, failing which, attribution by omission would follow under Article 11 of the Draft Articles of State Responsibility (29) read with the ratio laid down by the International Court of Justice in the case of *United States of America v. the Islamic Republic of Iran*. Nevertheless, given the threats that cyberattacks represent to the sustainability of space, international law must evolve and address:

- The duty of nations to investigate cyberattacks against satellites and share their findings with the State aggrieved by the same.
- Impose minimum standards of due diligence and regulations that can govern lawful intercept and monitoring powers of nations to ensure real intelligence on cyberattacks.
- Codification of the principles of state responsibility specific to cyberattacks against space objects and satellites consistent with the principles of the Outer Space Treaty.
- Dispute resolution mechanisms and defining the limits of the right of self-defence in cases of cyberattacks against satellites and space objects.

As states increasingly develop sophisticated means to target space-based assets, having clarity of the applicable principles of law could greatly aid the cause of containing the theatre of warfare from escalating into space and in ensuring that the use of force via cyberattacks, even if justified under the laws of armed conflict, is avoided and more civilised forms of dispute resolution become available.

Conclusion

In cases of cyberattacks against space assets, attribution must be seen from the perspective of the Outer Space Treaty if one were to accept that the duty to avoid a threat to the sustainability of space as a vital objective of international law. Although each branch of international law (concerning space, armed conflict, telecoms, or the sea) provides different pieces of the puzzle in isolation, they begin to present a clear framework for attribution and state responsibility when put together. However, while jurists can employ the best creativity to construct a legal framework to resolve controversies involving attribution in cyberattacks against satellites by extrapolating existing principles of international law, they remain no substitute for the emergence of a clear legal framework based on the consensus of nation-states. Until such clarity emerges in the legal framework around cyberattacks against satellites and space objects, there is no significant legal means of deterring such attacks. After all, the future of warfare cannot be adequately addressed unless the law matches pace with emerging trends.

Endnotes

(1) Patrick Howell O'Neill, "Russia hacked an American satellite company one hour before the Ukraine invasion", *MIT Technology Review,* May 10, 2022, https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/

(2) Jason Jolley, "Compounding the Issue of Authorship Are the Blurred Lines between States and so-Called Patriot Hackers (Hacktivists) or State Proxies (Proxies): Hacktivists and Proxies May Carry out Cyber-Attacks (Both Malicious and Militarized) on a Perceived Enemy of Their State with Acquiescence from Said State," in *Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law*, 34–34 Kindle Edition, (2017).

(3) Mike Wall, "Kessler Syndrome and the Space Debris Problem", *Space.com*, November 15, 2021, https://www.space.com/kessler-syndrome-space-debris .

(4) Christian Henderson, "Non-State Actors and the Use of Force" *Non-State Actors in International Law*, ed. Math Noortmann, August Reinisch and Cedric Ryngaert, (London: Hart Publishing, 2015), pp. 77–96.

(5) Malcom N. Shaw, "Serious Breaches of Preemptory Norms (Jus Cogen)" in *International Law*, 6th ed., (Cambridge: Cambridge, 2008), pp. 807–8.

(6) Shaw, "International Law", Pg. 807

(7) See Articles 1 to 4 of the Outer Space Treaty

(8) Ekta Rathore and Biswanath Gupta, "Emergence of Jus Cogens Principles in Outer Space Law," *Astropolitics 18*, no. 1 (2020), pp. 1–21, https://doi.org/10.1080/14777622.2020.1723353.

(9) Article 45 of the Constitution, Convention and Telecom and Radio Regulations of the ITU.

(10) Michael N. Schmitt, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", (Cambridge Core. Cambridge University Press, 2017), pp. 272-3. https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9.

(11) Lee R.J., "Jus ad Bellum in Outer Space: The Interrelation between Article 103 of the Charter of the United Nations and art. IV of the Outer Space Treaty", *Hein Online* (advance online publication), doi: IAC-02-IISL.3.02

(12) Jason Jolley, "As such this book would argue that demonstrating complete dependence or control over a non-state actor so as to attribute the acts as that of a state organ is virtually impossible in cyberspace," in *Attribution, State Responsibility, And The Duty To Prevent Malicious Cyber-Attacks In International Law*, p. 94.

(13) See Article 8 of the Draft Articles on State Responsibility

(14) United States Diplomatic and Consular Staff in Tehran, *Judgment, 1.C.J. Reports,* 1980, p. 3

(15) The finding of the court was based on the failure on the part of Iran to extend protection to the consular and diplomatic staff of the United States Embassy when it was overrun by the supporters of the Khomeni Government

(16) The Republic of Nicaragua v. The United States of America, 1986 I.C.J. 14

(17) Under Article VI, a state bears international responsibility for national activities in space, whether undertaken by state or non-state actors.

(18) Schmitt, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations"

(19) "The passages quoted show that, according to the Court's juris- prudence, persons, groups of persons or entities may, for purposes of international responsibility, be equated with State organs even if that status does not follow from internal law, provided that in fact the per- sons, groups or entities act in "complete dependence" on the State, of which they are ultimately merely the instrument. In such a case, it is appropriate to look beyond legal status alone, in order to grasp the reality of the relationship between the person taking action, and the State to which he is so closely attached as to appear to be nothing more than its agent : any other solution would allow States to escape their inter- national responsibility by choosing to act through persons or entities whose supposed independence would be purely fictitious." Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43.

(20) Delbert Tran, "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack", *20 YALE J. L. & TECH. 376* (2018), pp. 393-4.

(21) Younis Dar. "Why Satellite Hacking Has Become the 'Biggest Global Threat' for Countries like US, China, Russia & India?" *Latest Asian, Middle-East, EurAsian, Indian News*, October 24, 2020. https://eurasiantimes.com/why-satellite-hacking-has-become-the-biggest-global-threat-for-countries-like-us-china-russia-india/

(22) The Italian Republic v. The Republic of India concerning the 'Enrica Lexie' Incident, PCA Case No 2015-28.

(23) Enrica Lexie Case, pp. 1070 - 1077

(24) Enrica Lexie Case, pp. 1086.

(25) Convention on International Liability for Damage Caused by Space Objects

(26) "The first relevant principle is embodied in Article 33 of the ITU Constitution, and establishes the non discriminatory use of "the international service of public correspondence", including relevant satellite communications. Articles 34 and 35, entitled "Stoppage of Telecommunications" and "Suspension of Services", affect and counterbalance this right by permitting Member States to suspend ingoing and outgoing telecommunications, including those transmitted by satellite, with respect their own territory, on the condition that they publicly notify the stoppage or suspension as stipulated. These authorities stems from a state's capacity as a sovereign to control the flow of information through its territory, yet does not extend beyond its borders other than in exceptional situations", Deborah Housen-Couriel, "Cybersecurity Threats to Satellite Communications, Towards a Typology of State Actor Responses", Article in *Astronautica*, July, 2016.

(27) Article 45 of the Constitution, Convention and Telecom and Radio Regulations of the International Telecommunication Regulations

(28) "Moreover, the ITU norms specifically prohibit harmful interference with transmissions, and require states to operate with transparency regarding any interruptions to the satellite communications of other states. These provisions are rooted in a long-standing treaty regime that has developed over the course of the evolution of wireless communications since the 19th century, and to which nearly all states are bound at present", Deborah, "Cybersecurity Threats to Satellite Communications", Towards a Typology of State Actor Responses.

(29) "However, if the other State adopts them, for instance by intentionally employing its cyber capabilities to protect the non-State actor against counter-cyber operations so as to facilitate their continuance as acts of that State, the requirements for attribution have been met.", Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (p. 99).

Future of Warfare in the Changing Technological Context: An Indian Military Perspective

Raj Shukla

It is said that militaries prepare for the last war. However, more often (and perhaps more accurately), they end up preparing for the wrong war because of the inability to look into the future with perspicacity and appreciate sufficiently its complex and ever-changing landscape. The difference between winning and losing is often about getting the strategic-military futures right. The future of war, therefore, will be one of the most difficult challenges that militaries and nations grapple with, with getting it right being a rather elusive strategic prize. For instance, the raising of an entirely new command under a four-star general in the US (the US Army Futures Command) in July 2018 underlines the importance of dissecting futures in an institutional manner; the Futures Command is focussed on 'future readiness' as against the other army/ combatant commands that are focussed on 'fighting tonight'.

This essay seeks to re-evaluate the concept of war in a future conflict by examining the attributes of the broader strategic context that impact the physical fight: nature and character of war; the utility of force amidst changing paradigms of war; civilisational stratagems as shapers of warfighting strategies; the salience of the technology dynamic; likely contours; and attributes.

Nature and Character of War

It is important to begin by underlining the main distinction between the nature and character of war. Imagine a war where several sides are fighting, but it is not clear who is on which side; combatants do not wear military uniforms, many are foreigners, and they fight in the name of religion. They label

their enemy apostate and inflict the cruellest punishment on disbelievers; civilians are prey, and whole communities are looted and raped. Fighters carve out independent states in God's name and extort people of their wealth. The conflict becomes a holy mess to external observers, and some even conclude religion itself is evil. To many, this may seem like a recounting of West Asian conflicts of recent times. But these characteristics are of the 'War of Saints' fought in Italy between 1375 and 1378 (1).

There are indeed stunning parallels between then and now. The religion in question during the War of Saints was Christianity, not Islam, and the sectoral divide was Papists vs Anti Papists, not Shias vs Sunnis. As such, the nature of war in terms of violence, the resultant blood and gore, the victor imposing its will on the vanquished, combat cohesion, and the concepts of unit or tribal pride and honour is constant and unchanging. However, the character—how wars will be fought in terms of the strategic context, technologies, weapons, combat imagination, and leadership—changes rapidly. Just as a new clock cannot change the nature of time, even a new and transformative metric like artificial intelligence (AI), which will allow combat systems to think and act faster, will not change the nature of war. It will, however, significantly impact how wars will be fought.

Smart militaries do everything to strengthen attributes that reinforce the nature of war. Yet, they are sufficiently agile and fleet-footed to adapt and retool to meet contingencies arising from the rapid changes in the character of war. Both facets are equally critical. Indeed, the fiasco of the US's pullout from Afghanistan was a result of the failure to adequately appreciate the strengths of the Taliban when viewed from the lens of the nature of war. Similarly, the unravelling of the Russian military in Ukraine is mainly due to the failure to fathom the humongous change in the character of war.

The Utility of Force Amidst Changing Paradigms of War

Since the nature of war is unchanging, violence will never cease, it will only reappear in different nuances and forms (kinetic and non-kinetic). The instrument of force (symbolised by modern, joint militaries) will have to discover newer ways of being utilitarian; it must be agile, constantly reinvent itself, and adapt to the changing strategic context.

Reading the changing strategic context correctly and adapting the use of militaries accordingly is, therefore, paramount and lies at the heart of the future of war challenge. In some ways, it is just about keeping pace with the evolution of warfare because the simple truth of history is that warfare evolves faster than warfighters do.

Countries that make a determined, professional bid to understand the changes in the constantly evolving strategic landscape are likely to get the construct of the future of war right. Concurrently, they need to smartly retool their militaries to strengthen their chances of winning.

In this context, strategic communities often make two prominent errors: their unwillingness to receive the futures; and their lack of appreciation for the changing paradigms of war.

An incident from the US could be illustrative of such short-sightedness. General William "Billy" Mitchell, a US war hero and pilot during the First World War, had seen the future and believed it was

air power. In 1924, he suggested that aircraft carriers should replace battleships. At that time, only a stunt pilot would have considered landing a plane on a moving ship. Months later, he also predicted war between Japan and the US, initiated by a Japanese surprise attack from the air. Incredibly, he asserted that such an attack would occur at Pearl Harbour. He reasoned that the Japanese needed to hit only one island to cripple the US's Pacific fleet. The top brass already thought Mitchell was eccentric, but these new assertions went too far, and his court-martial followed. Mitchell was found guilty and suspended from the army. In 1941, the Japanese initiated the surprise aeroplane attack on Pearl Harbour. They sank or damaged eight American warships within two hours, including the famed USS Arizona, destroying 188 aircraft and killing 2,403 people. The US and Japan went on to fight one of the greatest naval battles in history (Battle of Midway) entirely with aviation.

Mitchell's case shows us that changing strategic minds is difficult, especially when it comes to the future of war. When the Pacific War ended, the aircraft carrier had supplanted the battleship as the supreme platform on the ocean, just as Mitchell had foretold 20 years earlier. Mitchell saw the future, but no one believed him. The stakes are considerable, and the dogma thick. People are rarely ready to receive the future (2).

Changing Paradigms of Warfare

One may also get the construct of war wrong if they fail to recognise its changing paradigms. Military tools and sensibilities that deliver in one paradigm of war—loosely defined as a set of postulates that, for a time, provide model problems and solutions to the military-strategic community—turn out to be blunt instruments in another.

In the last seven decades, two major paradigms have emerged—massive industrial wars, and wars among the people. Now, a turn to a third paradigm—digital wars—appears likely.

Industrial war paradigm

In the paradigm of industrial wars, unresolved political disputes between two conflicting ideologies—for instance, Nazi Germany and Liberal Europe during the Second World War—were taken to a remote military battlefield, where rival armies slugged it out. Unresolved political disputes were settled in the military arena, with armies delivering on their political promise. A massive inter-state industrial war was chosen as the medium to establish the victor and vanquished. An Allied victory on the battlefield proved the sway of Anglo-American democracy over Nazism just as the military victor of the Cold War saw its espoused cause of Western liberal democracy triumph over Soviet-era communism.

Combat platform paradigm

A paradigm shift began with the advent of nuclear weapons in 1945. It became dominant towards the end of the Cold War, with nuclear weapons and the concept of mutually assured destruction making industrial war as a massive deciding event virtually impossible. Wars turned non-industrial against non-state opponents; from armies with comparable forces fighting on remote battlefields, the paradigm

changed to a strategic confrontation between a range of combatants, with battles occurring in the streets, houses, and fields among the people. Wars now took place in the presence of civilians, against civilians, and in defence of civilians. Civilians were targets, objectives to be won, and an opposing force (3).

Combat in these wars among the people was akin to armed politics. Even when a weapon or combat effect was militarily useful (air-delivered ordnance, for instance), its use had to be curtailed because the political ill effects far exceeded their military value (4).

In conflicts of this kind—such as in Iraq, Afghanistan, Syria, and Libya—compartmentalised, mutually exclusive military and political endeavours have proved counterproductive. The al-Qaeda and Taliban can be defeated militarily or even through spectacular, light, mobile military campaigns, such as 'Operation Iraqi Freedom'. However, if the dominant political questions are not addressed, they will emerge in time, space, and other avatars, much like ISIS and other motley groups.

Despite their big budgets and whiz-bang technologies, wars failed to end conflict decisively; even when the military operation was a success, the fundamental political problem lay unresolved. Wars, therefore, continued to fester for long periods, invoking references such as 'endless wars'. Military tools configured for industrial-era conflict were found inadequate in wars among the people. Instead of retooling for the changing paradigm, strategic commentators began criticising the decreasing utility of the instruments of force.

Once a dominant symbol of industrial-era conflict, the declining utility of the tank in the changing paradigm of wars is increasingly evident. The waning use of the tank in combat is critical to explaining the change in the combat platform paradigm in the twentieth century. However, the military community has refused to acknowledge this. In 2005, General Rupert Smith reminded us that the last real tank battle—in which the armoured formations of two armies manoeuvred against each other (supported by artillery and air forces), and where the tanks were a decisive force—occurred in the 1973 Arab-Israeli war on the Golan Heights and the deserts of Sinai (5).

In the decades since Iraq, Lebanon, Georgia, Chechnya, and Syria, armoured formations either followed or supported the application of airpower and artillery, or their units and subunits were committed piecemeal as part of infantry-armour assaults in urban terrain. But the use of the tank as a machine of war organised in formation, designed to do battle, and attain a definitive result, has not occurred since 1973.

Since 1994, 78 percent of tank casualties have occurred in urban warfare/built-up areas. In Chechnya (1999-2000), the Russians lost 122 out of 146 tanks and infantry combat vehicles to tank ambushes due to the sheer intensity of urban warfare. Upgrades (such as fused sensors, counter-drone integration, better situational awareness, and active protection systems) could have secured the tanks. But since little was done, we now see the tank (with over 800 losses) as somewhat of a twentieth-century legacy platform, struggling to find its own in twenty-first-century warfare in the ongoing Ukraine conflict. Once again, Russia's unwillingness to read the writing on the wall and insistence on using dated tanks has resulted in its unravelling.

In the Indian context, the army is revisiting the paradigm of large tank battles and embracing the concept of smaller, technologically-enabled Integrated Battle Groups with higher readiness levels. Newer windows for the employment of armoured/mechanised forces in Ladakh and Sikkim are being leveraged. If one revisits the utility of armour in future wars in imaginative ways, the tank will not only survive but remain a powerful platform.

Digital war paradigm

In the ongoing Ukraine war, we may also witness the beginnings of a transition to an entirely new paradigm, digital wars. Ukraine, a side with solid, digitally-enabled proficiencies, is mounting a serious challenge to the formidable Russian military, albeit one with a pronounced reliance on large and sluggish legacy platforms.

A suite of small and emerging digital technologies (electronic warfare, micro-electronics, drones, precision attack systems, loiter munitions, and star link terminals enabling high data rates) are challenging the traditional leaders of combat. Swarming is challenging surging, surveillance and precisionary are challenging fire and manoeuvre, and light and small is beating large and heavy. Not surprisingly, the US Marine Corps is remaking itself and shedding its heavy tanks and tube artillery in favour of digitally-enabled systems (drones, long-range rocket artillery and maritime strike Tomahawk missiles) (6).

Civilisational Stratagems as Shapers of Warfighting Strategies

As Cold War 2.0 between the US and China and their respective allies intensifies, we are also witnessing a clash of sorts between their civilisational stratagems and strategic outlooks, with a distinct imprint on the conduct of war.

For instance, western militaries invested in Clausewitz (the lion) tend to do better in the kinetic domain; those that lean towards Sun Tzu (the fox) are more likely to prevail in the grey zone in stealth wars. (7) When ‘brute force’ is posited against ‘strategic cunning,’ the latter is bound to triumph. In the sub-threshold space (of war and peace), where deception and trickery rule the roost, Clausewitz (who dismisses ruses as weapons of the weak) is bound to come a cropper against Sun Tzu (a votary of ruses/trickery as weapons of choice) (8). This explains the People’s Liberation Army’s successes in the South China Sea, where they have altered geostrategic realities without firing a shot, or even Russian successes in Georgia and Crimea. Yet, as events in Ukraine have shown, combat attributes that are useful to fashion victories in the grey zone are of little utility in all-out lethal combat.

In future wars, developing parallel competencies in competition and conflict will be salient and result in victories. Intelligent militaries must tailor their doctrines and strategies to the prevalent operational paradigm. Strategic cunning must be met with equal cunning and deft manoeuvres in the non-kinetic space while retaining the ability to unleash calibrated and precise kinetics when faced with all-out lethal combat.

The Salience of the Technology Dynamic

The world is currently being swept by a new great game in technology (9). The change is humungous in the technological domain, primarily due to the convergence of a spate of disruptive technologies. If futurist Ray Kurzweil is to be believed, the twenty-first century will see 20,000 years of exponential change packed into a single century (10). Indeed, technology is being dubbed the fourth factor of production in addition to land, labour, and capital (11).

Militaries will not be immune to the accelerating pace of technological change. Technological adoption in tandem with agile doctrinal adaptation and organisational restructuring will give armies of tomorrow a sharp, calibrated edge over competitors and adversaries.

The value of focussed technological adaptation is already visible to the discerning eye. There was a time when doctrines drove technological developments; today, technologies are driving doctrinal cycles. Technological advancement is making unequals equal in combat.

This determined technological upturn is the arrow in the Chinese quiver that is being leveraged to address the US military's asymmetric strength, and is also causing considerable displacement anxiety.

Even a modest power like Türkiye has leveraged technological prowess in domains like drones and electronic warfare) to emerge as a drone superpower of sorts, but reinforce its statecraft by enhancing its strategic heft by developing power projection capacities that enable the elimination of threats at the source (12). It has also leveraged this expertise for commercial benefit (war as a service) by providing drone and allied technologies to regional and global customers at a minimal cost.

Likely Contours: Attributes of a Future-Ready Force

How should national security enterprises or global militaries prepare for the future? What could or should be the attributes of a 'future-ready force'? How do we create an ecosystem that will help us better respond to the challenges associated with the new paradigm of digital combat? The ten postulates that follow may help frame the debate.

In getting the contours of the strategic-military futures and the parameters of future readiness right, an ecosystem of insightful strategic minds and robust institutions is perhaps the most critical. Such ecosystems help foster a culture of futurism and develop deep strategic insights, thus bringing about clarity and competitiveness in the nation's strategic sensibilities.

Given that Ukraine is perhaps only the first chapter in the unfolding Cold War 2.0, the global security environment is likely to worsen, and the strategic-military competition is bound to intensify. In myriad contingencies in Europe, the Indo-Pacific, and West Asia, there is a possibility of such competition straying into all-out conflict. Militaries of the future, therefore, will need to develop parallel competencies in competition and conflict. They will have to be as adept in the grey zone paradigm as in lethal combat, not as an either/or choice, but as a set of integrated, free-flowing competencies. Yet another valuable

lens to assess the 'future of war' is through the 'text and context' paradigm in the operational frame. Since the nature of war is unchanging, the text of the fight in terms of the fundamentals of combat will not change. Therefore, mastery of the primary domains will remain an absolute necessity in combat. There is considerable scope for imaginative thought and leveraging that is informed by experiences in the previous two paradigms of war (industrial conflict and wars among the people) to begin exploring the tenets of digital wars.

Digital capacities in combat are transforming warfighting like never before. As a singular measure, digitally-enabled surveillance and precisionary are challenging proficiencies in fire and manoeuvre, which has been the fundamental prowess in combat for centuries. Autonomy, combat clouds and enterprise-power command and control systems have the potential to take warfighting to an entirely new level. Sagacious militaries have begun preparing for the inevitable, the mammoth transition from industrial=era warfighting to digital combat. With smart investments in digital proficiencies of the future, they aspire to turn the future fight decisively in their favour.

Global militaries, fundamentally, have been instruments of attrition. Given the impact of technologies like AI, space, cyber and electronic warfare, the cognitive domain is fast becoming salient. Undoubtedly, future militaries will have to be as proficient in the cognitive domain as they are in attrition warfare.

AI and associated technologies—quantum, blockchain, Big Data analytics, robotics, biotech, and programmable materials—will transform not only militaries but the very foundation and future of power (13). AI-enabled technologies are already transforming intelligence, targeting, vertical lift, and precisionary. A hypersonic missile coming in at Mach 10 speeds cannot be responded to by human reaction or judgment; it will have to be responded to via AI or machine learning. Militaries that invest in AI thoughtfully today will be the leaders of tomorrow.

Strategic-military futures will be shaped not merely by the adoption of technology, but also by the quality of technological innovation. Chinese President Xi Jinping and CIA Director William Burns have made it clear that 'technological innovation,' will be a decisive metric in determining the international pecking order of the future (14).

The defeat of the Soviet military during the Cold War, despite massive investments in military hardware, could be attributed to the absence of a domestic innovation hub. To give a fillip to innovation, the national security system will have to be infused with a culture of energy and enterprise. This culture is more a feature of the private sector and start-ups than state-owned defence enterprises. Elon Musk has demonstrated that even high-end national security ventures like space, which was once a state enterprise, things are now fast becoming a company enterprise. The US Army Futures Command's stated purpose is that of public-private enterprise synergy. In national security pursuits of the future, a collaboration between the military and business is vital. That the US Army Futures Command is headquartered in Austin, Texas, where Musk has a massive innovation hub, is no coincidence; it underlines the need for greater cross flows between the military and global innovation engines. The thought and speed with which private sector competencies and start-up energies are integrated into capacity building and warfighting will determine the power of future militaries.

In the long run, however, the true strategic advantage will be derived from investments in the deep technologies of the future. In information and communications technologies, for example, states with prowess in the core of the stack, rather than mere proficiencies in services and applications, will emerge as leaders of the strategic pack. A race is already afoot in several other domains of deep tech: mastery of outer space, new chemistries for batteries, microelectronics, the science of brain-computer interface, and programmable materials. Leaders in these domains are likely to emerge as dominant players. Wiser militaries have not only taken note but have also joined in the competition in hard tech with vigour (15).

It is also apparent that national security, especially the niche domains of combat, is getting so complex and sophisticated that military capacity-building of the future will need to pivot from mere equipment and platform acquisition to talent acquisition. As a significant new marker in human relations, the impact of these new talent pipelines will be game-changing. For instance, Israel's Units 8200 and 9300 recruit not only the best of local talent but also operate as start-ups to maximise combat efficiencies. Global militaries will need to adapt to the new talent paradigm expeditiously.

None of these advancements would be possible without the help of agile bureaucracies. Importantly, centralisation, rules and procedures mitigate against the spirit of innovation, the latter being an ethos and philosophy that will die in the face of centralisation and control. To truly unleash the spirit of innovation, we will need a leap of bureaucratic faith. The transition to digital combat will only become a reality if government intervention is minimised, rules and procedures are scaled down, innovation centres are created in every arm of government, a new culture of risk-taking is encouraged, failures funded, and entrepreneurial cross connects allowed their natural flows.

The abiding lesson for the future also lies in the skilful fusion of all available competencies to drive capacities in national security. The calibrated exercise is driven by the understanding and acknowledgement that national security is increasingly becoming such a complex and interwoven subject that no single institution can accomplish its myriad objectives on its own.

Civil-military fusion is indeed the mantra for the future. China, Israel, the US, and even Türkiye embrace its tenets in their unique ways. It calls for a dissolution of all silos and the bringing together of the talents and attributes of the military, industry, business, academia, centres of science, start-ups, technologists, domain specialists, and associated bureaucracies in the pursuit of national security objectives.

Conclusion

In human affairs, wars are a constant. But they also go through paradigm shifts in keeping with the capabilities of the period. Developing a sophisticated understanding of these changing paradigms is a complex but critical function of statecraft. As we have seen, intelligent leveraging of its many levers could help us hypothesise the evolving tenets of the character of war with reasonable accuracy and retool militaries accordingly. Countries that do so with wisdom and skill will prevail in the strategic–military competition and all-out lethal conflicts.

Endnotes

(1) Sean McFate, *The New Rules Of War: Victory In The Age Of Durable Disorder* (Harper Collins Publishers), pp.25-26.

(2) Sean McFate, *The New Rules Of War: Victory In The Age Of Durable Disorder* (Harper Collins Publishers) pp. 17-19.

(3) Rupert Smith, *The Utility of Force – The Art of War in the Modern World* (Penguin Books, 2019), pp.4.

(4) Emile Simpson, *War From The Ground Up – Twenty First Century Combat As Politics* (Oxford University Press, 2013), pp.232.

(5) Rupert Smith, The Utility of Force – The Art of War in the Modern World (Penguin Books, 2019) , pp.2.

(6) Kyle Mizokami, "After Nearly a Century, the US Marine Corps Is Ditching Its Tanks," *Popular Mechanics,* March 24, 2020*,* https://www.popularmechanics.com/military/weapon*,*

(7) Clausewitz says that ruses are weapons of the weak; Sun Tzu opines that they are weapons of choice

(8) Sean McFate, The New Rules Of War : Victory In The Age Of Durable Disorder (Harper Collins Publishers),pp. 204-205.

(9) Anirudh Suri, *The Great Tech Game: Shaping Geopolitics and the Destinies of Nations* (Harper Collins Publishers, 2022), pp.3.

(10) Ray Kurzweil, "The Law of Accelerating Returns," *Kurzweil,* March 7, 2001, https://www.kurzweilai.net/the-law-of-accelerating-returns

(11) Anirudh Suri, *The Great Tech Game: Shaping Geopolitics and the Destinies of Nations* (Harper Collins Publishers, 2022), pp.94.

(12) Ken Moriyasu and Sinan Tavsan, Ascendant and assertive Turkey creates tough choices for US, *asia.nikkei.com*,https://asia.nikkei.com/politics/international-relations, 28 July 2021.

(13) Rajiv Malhotra, *Artificial Intelligence and the Future of Power* (Rupa Publications, 2021), pp.xviii.

(14) President Xi Jinping emphasises the salience of technological innovation http://english.scio.gov.cn/m/topnews/2021-05/29/content_77535046.htm, 17 October 2022; Central Intelligence Agency, Government of the United States of America, https://www.cia.gov/stories/story/cia-names-first-chief-technology-officer/

(15) In the ensuing technological contest, China leads the US in all emerging technologies to include AI, military autonomy and robotics. In the recent offensive against Hamas, the IDF leveraged facial recognition to eliminate top Hamas commanders as also Big Data to target the weak points in the Hamas tunnel network. The Turk military has invested heavily in drone swarms and electronic warfare to grow its strategic heft and eliminate threats at source. The USA and China are now locked in a battle for supremacy in chips.

Strategic and Tactical Perspectives on Technologies

AI and the Rise of Autonomous Weapons

Ravindra Singh Panwar

At this stage in the evolution of warfare, lethal autonomous weapon systems (LAWS), often sensationally referred to as 'killer robots' or 'slaughterbots', seem set to emerge from the fantasy world of *Terminators* (1) into real-world militaries. Autonomy in civil and military systems has been gradually increasing over the past few decades. However, current excitement in the field of autonomous weapons has essentially been triggered by the spectacular advances in artificial intelligence (AI) and robotics technologies.

AI-based applications and systems pose significant risks, mainly because of the remarkably intelligent behaviour displayed by these systems, leading to a substantial increase in the delegation of cognitive functions to machines. AI-enabled weapon systems are of particular concern because they potentially threaten human lives. This surge has given rise to numerous legal and ethical conundrums, which need to be suitably addressed.

At the same time, if the power of AI is leveraged responsibly, it could prove to be hugely beneficial to humankind, both on and off the battlefield. This double-edged character of AI technologies points to the need for a carefully thought-out strategy for developing AI-enabled weapon systems while concurrently evolving an effective mechanism for regulating this development.

This essay touches upon some fundamental issues related to AI, autonomy, and human control. It then attempts to assess the impact of increased autonomy in weapon systems on the character of warfare in the coming decades. It highlights the immense resources being earmarked by major world powers to develop these autonomous systems. Further, it dwells on the ongoing global efforts to regulate these systems and briefly outlines an innovative risk-based approach which could contribute to this endeavour.

AI: Definition, Characteristics and Concerns

It is hard to find a precise definition of AI. One formal explanation of this term is cited in the proposal for AI regulation recently adopted by the European Commission (2). In this document, an AI system is defined as software that is developed for making predictions, recommendations, or decisions, using some of the following techniques:

- machine learning techniques, such as supervised, unsupervised and reinforcement learning
- knowledge-based approaches, such as logic programming and expert systems
- statistical approaches such as Bayesian estimation and optimisation methods

Notwithstanding the broad scope of AI covered by this definition, most of the spectacular results and foreseeable risks associated with AI-enabled systems stem from certain features of neural network-based machine-learning (ML) techniques.

The distinctive characteristics of AI/ML systems arise fundamentally from their ability to 'learn directly from data', which might continue even after the systems are deployed. These systems also have a 'black-box' character since the process by which inputs translate into outputs is largely opaque, even to the developers. This is often referred to as the 'non-transparency' or 'non-explainability' of AI systems. Finally, the power of neural networks has resulted in a phenomenal increase in the 'intelligence' they confer on AI-enabled systems.

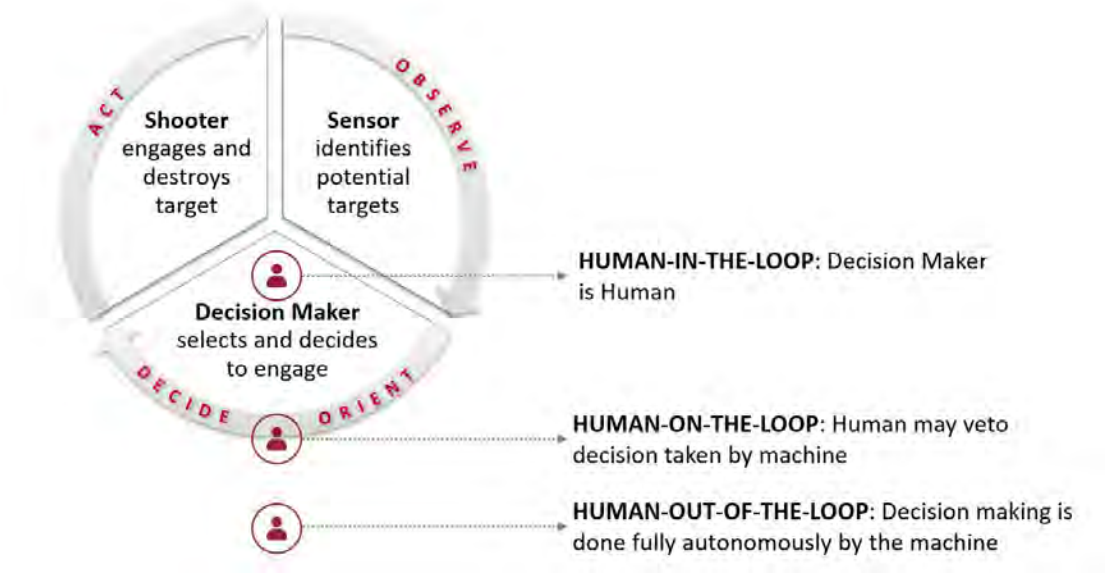
The data-centric character of AI-enabled systems introduces risks that result from unrepresentative, incorrect, biased, or deliberately poisoned data. The fact that a system might continue to learn post-deployment and thus morph into something different from what was intended introduces a degree of unpredictability to its functioning. The non-transparent nature of AI systems also renders them vulnerable to catastrophic failure when confronted with edge cases, a characteristic termed 'brittleness'. Their higher intelligence and the consequent potential for greater autonomy results in an inevitable 'transfer of cognitive functions' from humans to machines, which is itself a cause of great concern, with additional undesirable effects such as 'automation bias' and 'lack of accountability' (3).

Autonomy in Weapon Systems

Autonomy and human control are closely related—where autonomy ends, human control begins. In a weapon system, this is a complex, multifaceted relationship, covering distinct functions—such as take-off and landing, navigation, target identification, selection, tracking, the decision to engage, and actual engagement—each of which may have varying degrees of autonomy. Further, while one can visualise a fully manual weapon system (for instance, a simple spear), a fully autonomous system is harder to envision, as some level of human control over weapon systems is always likely to exist (unless machines take over the human race!). It is also to be noted that AI/ML technologies do not necessarily underpin autonomy in a system.

Scholars William C. Marra and Sonia K. Mcneil have provided an excellent exposition on autonomy in weapon systems, opining that autonomy should be measured on a continuous scale (4). A popular way to classify different degrees of autonomy uses the 'human-in-the-loop', 'human-on-the-loop', and 'human-out-of-the-loop' clauses, the last representing full autonomy (5). It is helpful to consider the 'loop' here as the observe–orient–decide–act, or the OODA loop, which translates to the sensor–decision-maker–shooter loop in the context of weapon systems (see Figure 1).

Figure 1: Degrees of Autonomy



Source: Author's own

In its Directive 3000.09 on autonomy, the US Department of Defense classifies weapon systems as "semi-autonomous", "supervised autonomy", and "fully autonomous" (6). Several other classifications defining different levels and facets of autonomy exist in the literature, some at a more granular level (7), (8).

A careful analysis of existing literature shows that autonomy in weapon systems is a continuum spanning several sub-functions, and any lines drawn to separate weapon systems into sub-classes based on this parameter are, at best, blurred.

Deliberations at the United Nations have broached two alternative frameworks to make headway on the degree of human control in LAWS (9). According to Human Rights Watch, the term meaningful human control (MHC) signifies control over the selection and engagement of targets, which are considered as critical functions in a weapon system. Human rights advocacy groups assert that humans should exercise control over every individual attack, not simply overall operations (10).

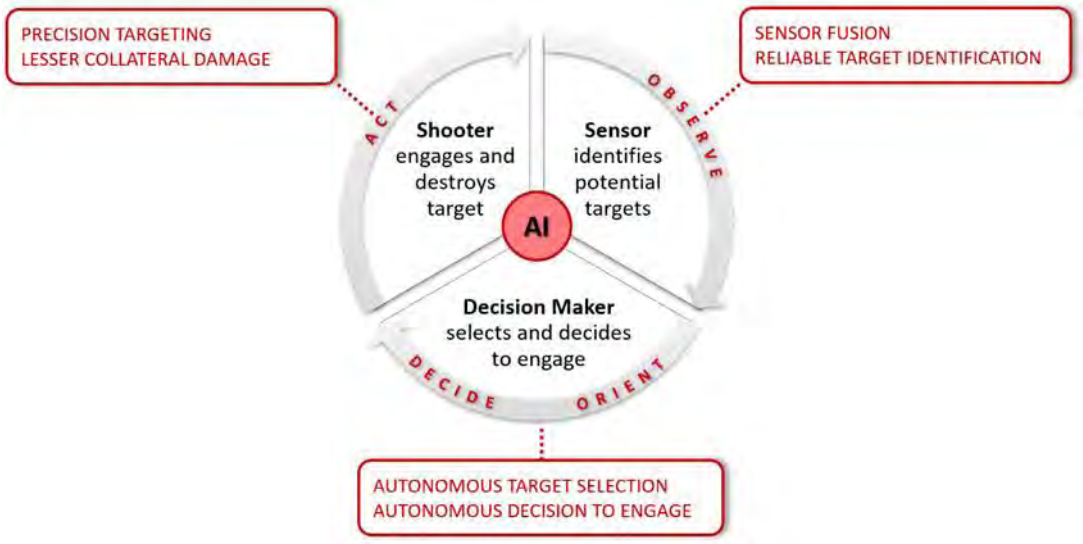
An alternate viewpoint proposed by the US stresses that the human-machine relationship extends throughout the development and employment of the autonomous weapons system and is not limited to the moment of decision to engage a target. Therefore, it is more practical to talk about 'appropriate levels of human judgement' rather than MHC (11).

After nearly eight years of deliberations, a consensus remains elusive on what level of control should be exercised over LAWS. This is perhaps the main stumbling block in the way of a treaty or any other type of binding agreement for regulating their development.

AI and the Changing Character of Warfare

It is widely believed that the combination of AI and robotics technologies will trigger the next revolution in military affairs, which is expected to unfold over the next two decades. AI technologies, being ubiquitous, are expected to seep into every stage of the weapon system OODA loop (see Figure 2).

Figure 2: Infusing Intelligence into the OODA Loop



Source: Author's own

The chief concerns associated with AI-powered weapons hinge on the critical select-and-engage functions. In carrying out target identification, AI-enabled sensors would play a vital role in selection. Next, AI-enabled decision-making would be involved in prioritising targets, followed by the decision to engage. The actual engagement mechanism, such as the fire-and-forget homing missiles, may also be AI-enabled and could significantly increase the precision of weapon systems.

Thus, in the physical realm, AI-powered autonomous weapon systems are expected to greatly speed up, improve the quality of the OODA loop in warfighting, and provide a potent new dimension to non-contact warfare. Concurrently, employing the power of AI for the conduct of cyber, electronic, and psychological operations will also bring about transformative changes in the information and cognitive realms.

Autonomous weapons: Extant systems

Autonomy in weapon systems, including in their critical functions, is not a recent development. Indeed, fully autonomous weapon systems have been in operational use for several decades. Nonetheless, there

is no denying that recent advances in AI and robotics have immensely accelerated the incorporation of autonomous functions into a wider variety of weapon systems.

Some of the notable extant weapon systems with varying degrees of autonomy, either already operational or in an advanced stage of development, and not all of them powered by AI, are:

- Unmanned Aerial Vehicles (Harop (12), Blowfish A3 (13), Bayraktar TB2 (14))
- Unmanned Ground Vehicles (Marker (15), Multi-Utility Tactical Transport (16))
- Unmanned Undersea Vehicles (Posiedon (17), Orca XLUUV (18), HSU001/ Haishen 6000 (19))
- Drone swarms (STM Kargu-2 (20), Israeli Drone Swarm (Israeli-Hamas War) (21), Perdix Drone Swarm (22))
- Manned-Unmanned Teaming (MUMT) systems (XQ-58 Valkyrie (23), Loyal Wingman (24), and
- Defensive systems (Phalanx (25), Iron Dome (26))

A few of these deserve special mention:

- US Phalanx (non-AI, fully autonomous, defensive weapon system): One of the earliest examples of LAWS, in service since 1978, is the US Phalanx, a close-in weapon system for defence against incoming threats such as anti-ship missiles and torpedoes. The Phalanx can automatically search for, detect, track, and engage targets using its computer-controlled radar system.

- Israeli Harop (non-AI, fully autonomous, offensive weapon system): The Harop is a loitering munition designed to attack enemy radars by self-destructing into them. Its predecessor, the Harpy, with similar features, has been operational since at least the early 1990s.

- Turkish Kargu-2 (AI-enabled, fully autonomous, offensive weapon system): According to an April 2021 UN report, the STM Kargu-2, a Turkish unmanned combat aerial vehicle (UCAV), autonomously hunted down Haftar Armed Forces elements in Libya in 2020 (27). If the report is accurate, Kargu-2 is perhaps the first and only fully autonomous weapon system known to be operational that specifically seeks out human targets. The fully autonomous capability of this drone has, however, been refuted by the manufacturer (28)

- Israeli operations against Hamas (first AI war): The Israeli operations against Hamas in the Gaza Strip in May 2021 have been dubbed the first AI war. In addition to using drone swarms in conjunction with mortars and ground-based missiles, AI was leveraged to extract targeting information using data from a variety of sources, including signal intelligence, visual intelligence, human intelligence, and geospatial intelligence.

- Russian Poseidon (autonomous nuclear weapon): The Poseidon is an autonomous, nuclear-powered, and nuclear-armed unmanned underwater vehicle developed by Russia, perhaps the only one of its kind in the world. The extent of autonomy in Poseidon is unclear from the available information, and its operational status is also somewhat ambiguous.

Since the potential benefits of intelligent weapons and applications for enhancing combat capacity is very high, major militaries are spending billions of dollars to harness AI for warfighting.

Harnessing AI for Warfare: US, China, and India

US AI initiatives and the Third Offset Strategy

AI and robotics technologies were central to the US Defense Innovation Initiative, also termed the Third Offset Strategy, issued in 2014 (29) (30). Thereafter, the Department of Defense AI Strategy was circulated in 2018, with the Joint Artificial Intelligence Centre as its focal point, the Defence Advanced Projects Research Agency, and the military service laboratories in the lead (31).

Notably, the US established the National Security Commission on Artificial Intelligence in 2018 to make recommendations on advancing the development of AI and associated technologies for comprehensively addressing national security needs. Its 756-page report submitted in March 2021 (32) stated that the US is not sufficiently prepared to defend or compete against China in the AI era. Some of its recommendations are:

- Double non-defence funding for AI research and development (R&D) annually to reach US$32 billion per year by 2026
- Triple the number of National AI Research Institutes
- Leverage commercially derived AI
- Create a digital service academy and civilian national reserve to grow tech talent
- Retire legacy systems ill-equipped to compete in AI-enabled warfare

China's AI plan: Leading AI power by 2030

The defeat of world champion Lee Sedol by Deepmind's AlphaGo AI-powered software in the game of Go in 2016—the first time a computer programme defeated a human champion— dramatically demonstrated the potential advantages AI could provide in future command decision-making. This win is considered by many to be the 'Sputnik moment' for China to pursue this technology with full vigour (33). China's focus on AI and other technologies such as big data, cloud computing, the Internet of Things, and nanotechnologies, is also perceived as China's response to the US's Third Offset Strategy.

Chinese military strategists envisage the nature of conflict evolving from today's 'informatised' warfare to future 'intelligentised' warfare. China's strategic military guideline for "winning informatised local wars" was first issued via a 2015 defence white paper titled *China's Military Strategy*. In 2017, China released the New Generation AI Development Plan, which envisioned a domestic AI industry worth US$150 billion, and declared China's objective of becoming the leading AI power by 2030 (34). The People's Liberation Army (PLA) plans to integrate AI into its weapon systems as part of its asymmetric 'assassin's mace' warfare strategy (35).

The Science and Technology Commission of China's Central Military Commission has launched well-funded plans for AI research. The PLA is pursuing service-specific AI projects through its captive research institutes, such as the Academy of Military Science and the National University of Defense Technology. AI R&D is vigorously pursued by the China Electronics Technology Group Corporation, the China Aerospace Science and Technology Corporation, and the China Aerospace Science and Industry Corporation (36).

India: Taking baby steps

In February 2018, India's Ministry of Defence set up a task force to prepare the country's future AI roadmap for developing defensive and offensive warfare capabilities (37). Based on its recommendations, a High Level Defence AI Council, chaired by the defence minister, was constituted, with the charter of providing strategic direction for AI-driven transformation in defence, facilitating R&D and technology adaptation, and ensuring ethical use of AI technology in defence applications, amongst others. A Defence AI Project Agency was also established, with the secretary (defence production) as its chairman.

The Defence Research and Development Organisation's Centre for Artificial Intelligence and Robotics (the primary laboratory for AI R&D), Vehicles Research Development Establishment, and the Research & Development Establishment (Engineers) have so far made limited headway in developing some prototype systems, such as the Muntra unmanned ground vehicle, and the Daksh remotely operated vehicle.

At this juncture, the Indian armed forces do not appear to be pursuing the development of AI systems with the urgency it deserves, evidenced by the lack of concept papers and doctrinal literature analysing AI's impact on warfighting in the Indian context. Indeed, the Technology Perspective and Capability Roadmap, 2018, which is meant to make a technology projection for the armed forces for the next 15 years, does not list a single project related to AI and robotics. The information available in the public domain does not provide a very encouraging picture of AI-powered projects being pursued by the armed forces. Clearly, a transformative R&D approach needs to be undertaken by India to harness the potential of AI for military applications.

Mitigating Risks in AI-Enabled Military Systems

For almost nine years now, there has been an ongoing global debate over the ethical and legal concerns generated by the expected emergence of AI-powered LAWS on the battlefield. The Campaign to Stop Killer Robots was initiated in April 2013 under the aegis of Human Rights Watch, aiming to ban LAWS preemptively. Triggered by this campaign, the UN Office of Disarmament Affairs took up this issue for discussion in 2014, initially as informal meetings of experts, and then, since 2017, through meetings of a Group of Government Experts (GGE). The latest meeting of the LAWS GGE was held in Geneva in March 2022 against the backdrop of Russian special operations in Ukraine (38).

Ban advocates argue that autonomy in the critical select-and-engage functions would violate international humanitarian law (IHL) principles of distinction and proportionality, and the Martens Clause (39),(40):

- Principle of Distinction: The basic rule of distinction requires that an attack may only be directed against combatants or military objectives. Ban proponents declare that machines will never be able to distinguish between combatants and civilians/wounded combatants reliably and will also be incapable of exercising empathy.

- Principle of Proportionality: This principle prohibits attacks that might cause incidental loss of life/injury to civilians and/or damage to civilian objects that would be excessive in relation to the anticipated

military advantage. Ban advocates contest that adhering to this principle requires 'value judgement', and machines can never evolve to this level of human prowess.

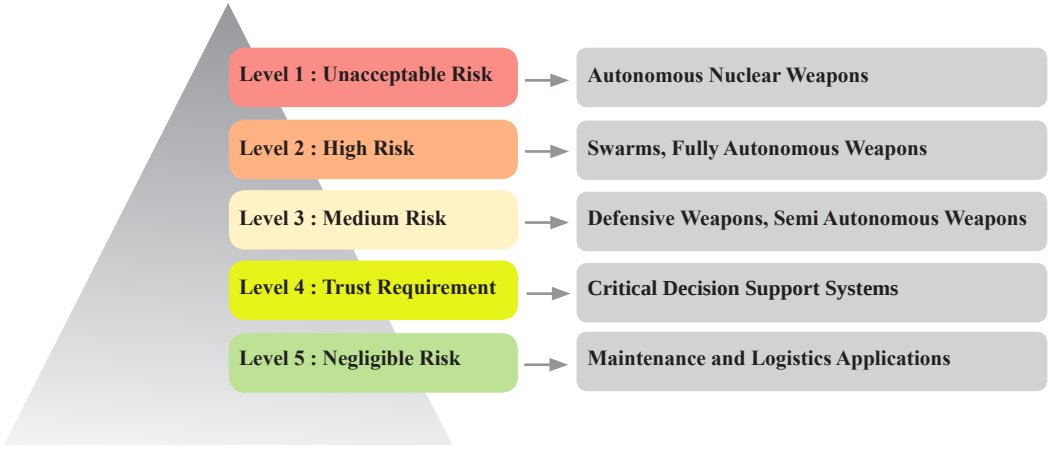
- Martens Clause: Ban advocacy groups raise the ethical/philosophical issue of whether machines should ever be vested with the decision power of 'life and death' and stress that it would be "against the principles of humanity and the dictates of public conscience", a provision reflected in the Martens Clause.

In 2019, the UN GGE achieved limited success by establishing 11 guiding principles for the development of LAWS (41). The US Department of Defense adopted a set of 'Ethical Principles for AI' in February 2020 (42). In addition, China, the European Union (EU), and Russia are amongst major state players who have come up with principles/norms for developing AI technologies, though these may not specifically address military systems (43) (44) (45). Notably, the EU has adopted a risk-based approach for regulating AI, which is applicable for commercial applications.

Adopting a risk-based approach while moving from principles to practice promises clear benefits for mitigating threats in AI-enabled military systems. This is because risks posed by different types of military systems may vary widely, and applying a standard set of risk-mitigation strategies might prove inadequate for high-risk systems while being overly stringent for low-risk systems, and hamper the development of systems that could possibly benefit humans. A risk-based approach has the potential to overcome these disadvantages.

Evolving such a risk-based model involves several steps: various military systems first need to be grouped into categories; risk classes must be defined, guided by the degree of risks posed; military system categories need to be assigned to risk classes; a differentiated risk-mitigation mechanism must be linked to each risk class.

Figure 3: Five-Level Risk Hierarchy



Source: Author's own

As an example, a five-level risk hierarchy, a pioneering model currently being evolved by the Centre for Humanitarian Dialogue, Geneva, is indicated in Figure 3. The top three risk classes relate to weapon systems, while the bottom two map to decision support systems. The highest risk level corresponds to weapons that pose unacceptable risks, such as fully autonomous nuclear weapon systems - this class of weapons must not be developed. All other AI-enabled weapon systems are mapped to either 'High' or 'Medium' risk levels.

Decision support systems that play a role in critical decision-making, such as for force deployments, require trustworthiness and would perhaps dictate the use of Explainable AI (XAI). All other military systems, including, for example, applications in the field of logistics and maintenance, present the lowest level of risk and would fall into the 'Negligible' risk level.

The differentiated risk mitigation measures imposed on these systems could vary from a complete ban at one end of the spectrum to different levels of scrutiny, review, test and evaluation procedures, mandatory use of XAI, and control and oversight during the deployment phase. A risk-based approach, such as the risk hierarchy, can provide states and militaries with an optimal mechanism to exploit AI's power to enhance combat effectiveness while also helping them identify and avoid high-risk weapon systems that might run against IHL.

Conclusion

AI-powered autonomy in weapon systems is expected to revolutionise warfare by transferring the critical functions of selecting and engaging targets from humans to machines. AI-enabled military systems will also substantially speed up the OODA loop at tactical and operational levels. The impact of AI on the twenty-first-century battlespace will be felt not just in the physical realm but also in the information and cognitive domains.

The perceived loss of control by humans on weapon systems, together with certain unique characteristics of AI/ML systems such as unpredictability and brittleness, has given rise to a global movement clamouring for banning or at least regulating the use of AI in weapon systems in conformance with IHL. However, deliberations at the UN and other international fora have achieved limited success in reaching a consensus in this area.

Advances in AI and robotics will continue to fuel the inexorable rise of autonomous weapon systems in the modern battlespace. It would be futile to expect global powers not to leverage AI's potential to enhance their military capabilities. Nonetheless, nation-states that stand by the principles of *jus in bello*—the law governing how warfare is conducted—will hopefully develop intelligent weapon systems responsibly and ethically, eventually translating into evolving a binding international instrument on LAWS.

Endnotes

(1) Eliana Dockterman, "Untangling the Terminator Franchise's Complicated Timeline," *Time*, November 1, 2019, Time.com, https://time.com/5697301/terminator-movies-timeline-explained/

(2) European Commission, *Annexes to Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, Brussels, April 21, 2021, pp. 1, https://www.eumonitor.nl/9353000/1/j4nvgs5kjg27kof_j9vvik7m1c3gyxp/vli87bognun6/f=/8115_21.pdf.

(3) "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach," *International Review of the Red Cross, 102 (913)*, (2020), pp. 463–479, https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ai-and-machine-learning-in-armed-conflict-a-human-centred-approach-913.pdf.

(4) William C Marra and Sonia K McNeil, "Understanding the Loop: Regulating the Next Generation of War Machines," *Harvard Journal of Law and Public Policy, Vol. 36*, No 3, (2013), https://www.harvard-jlpp.com/wp-content/uploads/sites/21/2013/05/36_3_1139_Marra_McNeil.pdf.

(5) Christof Heyns, "Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, United Nations," Geneva, April 09, 2013, https://digitallibrary.un.org/record/755741?ln=en

(6) United States Department of Defence, *Directive 3000.09: Autonomy in Weapon Systems*, Washington DC, November 21, 2012, https://irp.fas.org/doddir/dod/d3000_09.pdf.

(7) United States Department of Defence, *Directive 3000.09: Autonomy in Weapon Systems*

(8) United Kingdom Ministry of Defence, *Joint Doctrine Publication 0-30.2: Unmanned Aircraft Systems*, Wiltshire, August 2017, pp. 13, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/%20attachment_data/file/673940/doctrine_uk_uas_jdp_0_30_2.pdf

(9) United Kingdom Ministry of Defence, *Joint Doctrine Publication 0-30.2: Unmanned Aircraft Systems*

(10) "Killer Robots and the Concept of Meaningful Human Control," *Human Rights Watch*, April 2016, pp. 1-2, https://www.hrw.org/news/2016/04/11/killer-robots-and-concept-meaningful-human-control.

(11) Michael W Meier, *UN CCW Informal Meeting on LAWS: US Delegation Opening Statement*, Geneva, April 11, 2016, https://geneva.usmission.gov/2016/04/11/laws/.

(12) Israel Aerospace Industries, "Harop Loitering Munition System," https://www.iai.co.il/p/harop.

(13) Patrick Tucker, "SecDef: China Is Exporting Killer Robots to the Mideast," *Defence One*, December 5, 2019, https://www.defenseone.com/technology/2019/11/secdef-china-exporting-killer-robots-mideast/161100/.

(14) Stephen Witt, "The Turkish Drone that changed the Nature of Warfare," *The New Yorker*, May 9, 2022, https://www.newyorker.com/magazine/2022/05/16/the-turkish-drone-that-changed-the-nature-of-warfare.

(15) David Hambling, "Russia's Autonomous Robot Tank Passes New Milestone (And Launches Drone Swarm)," *Forbes*, September 2, 2021, https://www.forbes.com/sites/davidhambling/2021/09/02/russias-autonomous-robot-tank-passes-new-milestone-and-launches-drone-swarm/?sh=59342d7021fa.

(16) "Multi-Utility Tactical Transport (MUTT) UGV," *Army Technology*, July 8, 2020, https://www.army-technology.com/projects/multi-utility-tactical-transport-mutt-ugv/.

(17) Natalie Huet, "What is Russia's Poseidon nuclear drone and could it wipe out the UK in a radioactive tsunami?," *EuroNews*, May 5, 2022, https://www.euronews.com/next/2022/05/04/what-is-russia-s-poseidon-nuclear-drone-and-could-it-wipe-out-the-uk-in-a-radioactive-tsun.

(18) "US Navy Designates Future Orca Unmanned Sub Support Facility," *The Defense Post*, 06 Aug 2021, https://www.thedefensepost.com/2021/08/06/us-navy-future-orca/.

(19) Ryan Fedasiuk, "How China is Militarizing Autonomous Underwater Vehicle Technology, *The Maritime Executive*, August 22, 2021, https://www.maritime-executive.com/editorials/how-china-is-militarizing-autonomous-underwater-vehicle-technology#:~:text=As%20early%20as%202013%2C%20the,in%20the%20South%20China%20Sea.

(20) Tactical Mini-UAV Systems, "Kargu: Combat Proven Wing Loitering Munition System," Savunma Teknolojileri ve Mühendislik A.Ş, https://www.stm.com.tr/en/kargu-autonomous-tactical-multi-rotor-attack-uav.

(21) Zak Kallenborn, "Israel's Drone Swarm Over Gaza Should Worry Everyone," *Defense On*e, July 7, 2021, https://www.defenseone.com/ideas/2021/07/israels-drone-swarm-over-gaza-should-worry-everyone/183156/.

(22) US Department of Defence, *Department of Defense Announces Successful Micro-Drone Demonstration*, January 9, 2017, https://www.defense.gov/News/Releases/Release/Article/1044811/department-of-defense-announces-successful-micro-drone-demonstration/.

(23) Kratos Defense & Security Solutions, Inc., "Kratos XQ-58A Valkyrie Successfully Completes Sixth Flight, Including First Payload Release from Internal Weapons Bay," April 5, 2021, https://ir.kratosdefense.com/node/26446/pdf.

(24) Samara Kitchener, "Loyal Wingman project achieves milestones," *Australian Government Defence News*, November 4, 2021, https://news.defence.gov.au/capability/loyal-wingman-project-achieves-milestones.

(25) Robert H Stoner, "R2D2 with Attitude: The Story of the Phalanx Close-In Weapons," *NavWeaps*, October 30, 2009, http://www.navweaps.com/index_tech/tech-103.php.

(26) Seth J Frantzman, "Iron Dome intercepts targets, works with US systems in Army test," *DefenseNews*, August 2, 2022, https://www.defensenews.com/land/2022/08/02/us-army-completes-second-iron-dome-interceptor-test/.

(27) UN Security Council, *Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973 (2011) – S/2021/229*, March 8, 2021, pp. 17/458, https://undocs.org/Home/Mobile?FinalSymbol=S%2F2021%2F229&Language=E&DeviceType=Desktop&LangRequested=False.

(28) Sinan Tavsan, "Turkish defense company says drone unable to go rogue in Libya," *NikkeiAsia*, June 20, 2021, https://asia.nikkei.com/Business/Aerospace-Defense/Turkish-defense-company-says-drone-unable-to-go-rogue-in-Libya.

(29) United States Department of Defence, *The Defence Information Initiative*, Washington DC, November 15, 2014, https://news.usni.org/2014/11/19/document-pentagon-innovation-initiative-memo.

(30) Peter Dombrowski, "America's Third Offset Strategy," *S Rajaratnam School of International Studies*, June 2015, pp. 4, https://www.rsis.edu.sg/wp-content/uploads/2015/06/PR150608_Americas-Third-Offset-Strategy.pdf.

(31) United States Department of Defence, *Summary of the 2018 Department of Defence AI Strategy*, Washington DC, November 8, 2018, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF?source=GovDelivery.

(32) United States National Security Commission on Artificial Intelligence, *Final Report*, Washington DC, March 1, 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

(33) Elsa B Kania, "Chinese Military Innovation in Artificial Intelligence," *Centre for New American Security*, June 7, 2019, pp. 1-5, https://www.cnas.org/publications/congressional-testimony/chinese-military-innovation-in-artificial-intelligence.

(34) "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)," *Digichina, Stanford University*, August 1, 2017, https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

(35) Rick Joe, "China's Growing High-End Military Drone Force," *The Diplomat*, November 27, 2019, https://thediplomat.com/2019/11/chinas-growing-high-end-military-drone-force/.

(36) Elsa B Kania, "Chinese Military Innovation in Artificial Intelligence,"

(37) Lt Gen (Dr) R S Panwar, "Artificial Intelligence in Military Operations: A Raging Debate and Way Forward for the Indian Armed Forces," *USI Monograph*, No 2, (2018), pp. 38, https://www.ibpbooks.com/artificial-intelligence-in-military-operations-a-raging-debate-and-way-forward-for-the-indian-armed-forces/p/36197.

(38) Reaching Critical Will, *We will not weaponize our way out of horror - CCW Report Vol 10 No 2*, March 14, 2022, https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2022/gge/reports/CCWR10.2.pdf.

(39) International Committee of the Red Cross, *International Humanitarian Law: Answers to your Questions*, December 2014, pp. 47, https://www.icrc.org/en/doc/assets/files/other/icrc-002-0703.pdf.

(40) Rupert Ticehurst, "Martens Clause and the Laws of Armed Conflict," *International Review of the Red Cross*, No. 317, April 30, 1997, https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm.

(41) UN Office of Disarmament Affairs, *Guiding Principles affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System, Final Report: Annexure III*, UN CCW GGE on LAWS, December 13, 2019, pp. 10, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/343/64/PDF/G1934364.pdf?OpenElement.

(42) United States Department of Defence, *DOD Adopts Ethical Principles for Artificial Intelligence*, February 24 2020, https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

(43) Ministry of Science and Technology, People's Republic of China, *A New Generation of Artificial Intelligence Ethics Code*, Beijing, September 26, 2021, http://www.most.gov.cn/kjbgz/202109/t20210926_177063.html.

(44) European Commission, *Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, Geneva, April 21, 2021, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF.

(45) "Artificial Intelligence Code of Ethics," Signed during International Forum on *Ethics of AI: The Beginning of Trust*, Moscow, October 26, 2021, https://a-ai.ru/wp-content/uploads/2021/10/Code-of-Ethics.pdf.

The Role of Nuclear Weapons in Future Wars

Manpreet Sethi

Nuclear weapons have been used only twice ever in warfare, in 1945 when two atomic bombs of 15 and 20 kiloton each were dropped over Hiroshima and Nagasaki in Japan. While there has been no other physical detonation or actual use of this weapon of mass destruction since then, nuclear weapons have certainly played a role in wars. Possessors of these weapons have used them for both coercion and deterrence. Indeed, in the nearly eight decades since they have been in existence, it has even come to be assumed that nuclear weapons have kept major powers from large-scale wars. It has been internalised as conventional wisdom that nuclear weapons have kept another world war at bay by "preventing a Cold War from turning into World War III because they induced both Washington and Moscow to be more prudent… and led to the establishment of tools for crisis management to reduce the prospect of the outbreak of unintended warfare, either nuclear or conventional (1)." Nuclear weapons, therefore, are assumed to have played a role in wars, not through their use but by casting a shadow.

In today's nuclear firmament, however, there are nine nuclear-armed states, creating multiple dyads. Each state has its nuclear doctrine, force structure, and force posture. The nuclear warhead numbers have come down from the Cold War peaks of around 60,000 to a soberer approximately 13,000. But their salience remains high, with the ongoing Russia-Ukraine conflict seemingly adding to their value. The way a nuclear Russia has behaved against a non-nuclear, sovereign nation can be expected to cause non-nuclear weapon states to reconsider their security requirements, especially if they face hostile relations with other nuclear-armed states. The Treaty on the Non-Proliferation of Nuclear Weapons and the more recent Treaty on Prohibition of Nuclear Weapons could face turbulent times ahead as nations re-examine the role of nuclear weapons.

The pertinent question to ask in contemporary times is what role nuclear weapons will play in future wars. Are the risks of the actual use of nuclear weapons going to increase due to new doctrinal or technological developments? Or will the weapons continue to cast a constraining influence on wars

in general? While definitive answers are difficult, some intelligent estimates on the likely nuclear developments that could influence future wars can be made; two doctrinal and three technological developments related to nuclear weapons are likely to impact future wars.

Two Doctrinal Developments

The first doctrinal development that could have an impact on future wars is the idea of limited nuclear use in warfighting. A terminology that has reemerged in recent times is 'limited nuclear use for strategic effect'. This is premised on the development and use of "tactical nuclear weapons" (TNWs) as low-yield nuclear weapons to be used against battlefield targets. During the Cold War, TNWs in the form of nuclear artillery shells and torpedoes were popular with the US and Soviet Union. With time, however, it was realised that the use of such weapons could not be divorced from the strategic impact that would lead to a full-blown nuclear conflict. TNWs went out of favour in the 2000s and were slated to be the next item on the US-Russia bilateral arms control agenda around 2010. However, with Washington and Moscow going through a phase of mistrust since 2014, instead of removing TNWs from national arsenals, the emphasis seems to have returned to the projection of using *small* nuclear weapons in *limited* nuclear wars.

The US's 2018 Nuclear Posture Review (NPR) brought this to the fore by suggesting that the country would build the necessary capabilities to fight a limited nuclear war to counter Russian dual-capable, nonstrategic systems that are not accountable under the New START Treaty (2). It mentioned a tailored deterrence strategy based on "a diverse range and mix of US deterrence options, now and in the future" (3). Signalling to Russia and China that "nuclear first use, however limited, will fail to achieve its objectives, fundamentally alter the nature of conflict, and trigger incalculable and intolerable costs", the NPR stated that "the President must have a range of limited and graduated options, including a variety of delivery systems and explosive yields" (4).

Moscow, in turn, has made counter allegations against the US, particularly its missile defence systems, for its own 'escalate to de-escalate' strategy. Irrespective of who started it, this has led to a situation where both are focusing on developing capabilities and options for a roughly similar execution of 'limited' nuclear strikes with diversity in platforms, range, and survivability. Though China has not yet announced any change in its nuclear doctrine, its nuclear advances cater to all contingencies. Meanwhile, Pakistan has been projecting the battlefield use of nuclear weapons, arguably to deter India's conventional might.

So, will future wars see a heightened chance of limited nuclear use? This looks difficult as part of a premeditated national response because nations will always find it difficult to guarantee that their own 'limited' nuclear weapons use would be honoured by the other side with a similar, proportionate response. In any case, what could be proportionate in use of nuclear weapons given that their effects cannot be constrained in time and space? Can it be business as usual after a 'limited nuclear exchange'?

While militaries may believe that a tailored deterrent strategy that offers many options to the leadership enhances the credibility of deterrence, such an approach overlooks the fact that nuclear weapons are not ordinary. In fact, on this dimension, much will depend on whether TNWs are used in the ongoing

Russia-Ukraine conflict. In the remote possibility of Russia using a low-yield nuclear weapon over some military target, it could create the danger of conventionalising nuclear use, and future wars can then be expected to find similar uses for the weapon.

A second doctrinal change that could lend itself to more overt use of nuclear weapons could be acceptance of postures that rely on keeping the weapons on 'launch on warning' or 'launch under attack'. This will be a particularly worrisome development when two nuclear armed states engage in conventional war. The experience until now has been that the US and Russia, who do maintain such postures, have not fought direct conventional wars with each other. So, the risks of inadvertent use of nuclear weapons due to misperception have been low. Meanwhile, in Asia, China, India, and Pakistan's nuclear postures have so far been more relaxed. While these nuclear-armed nations have been caught in direct confrontations, they have taken conscious measures to avoid risks.

The role of nuclear weapons in enforcing nuclear deterrence and constraining the scope of conventional conflicts in the region is clear. The three countries, on different occasions, have shown high tolerance for an adversary's military and political actions, and moderated the use of their own military capability to remain below the other side's perceived nuclear threshold. A former Indian defence minister made this observation after the nuclearisation of Southern Asia, "Nuclear weapons did not make war obsolete; they simply imposed another dimension on the way warfare was conducted…. [C]onventional war remained feasible, though with definite limitations, if escalation across the nuclear threshold was to be avoided" (5). So, the presence of nuclear weapons makes it difficult for countries to declare outright victories and defeats in conflicts. Nations are forced to tailor their politico-military objectives along more and more limited lines. Future wars between nuclear-armed states are likely to be of this nature.

Three Technological Developments

Amongst the many technological advances that are likely to impact nuclear deterrence, three particularly stand out. The first is the development of hypersonic technologies and weapon systems, which is continuing at a rapid pace in the US, Russia, and China (6). The US embarked on this technology to build a capability to hit time-sensitive terrorist targets anywhere in the world and to "counter growing threats to forward deployed forces and bases and ensuring US power projection capabilities (7)." Echoing the same thoughts, the 2018 NPR underscored the need for delivery systems that could strike quickly over long distances while evading early warning radars or ballistic missile defence (BMD).

Russia and China, however, have espied a threat to their nuclear assets from such delivery systems. They perceive hypersonic missiles, even when conventionally armed, as first-strike weapons that could undermine their nuclear deterrent. Indeed, it is not difficult to envisage that Russia or China could mistake the launch of a conventional hypersonic missile as a surprise attack on their nuclear forces or nuclear command, control, and communications (NC3) systems, thereby triggering nuclear retaliation. This could prove highly destabilising.

Hypersonic boost-glide vehicles that can fly at speeds of Mach 5-20 through the upper atmosphere and bring together the attributes of speed, range, manoeuvrability, and accuracy, even when armed with conventional warheads, pose a danger to nuclear deterrence. Manoeuvrability at hypersonic speeds

would help such missiles evade missile defence interceptors. So, while the early warning systems detect a missile launch, once the glide vehicle separates from the missile, it could not be tracked by the system, keeping the adversary guessing on the target. This ambiguity could spark inadvertent escalation by increasing pressures and panic for action.

Such use would blur the distinction between conventional and nuclear weapons in terms of their doctrine, role, and delivery systems. This would particularly increase the unease of a nation with small nuclear forces and could tempt them towards nuclear pre-emption. Therefore, the chances of stumbling into a nuclear war are significantly heightened in the presence of such technologies. The reduction in decision-making time, given the speed of the hypersonic glide vehicles, could compel nations to move towards launch-on-warning or launch-under-attack postures, which would further raise risks of inadvertence. Thus, the mere deployment of such systems could threaten nuclear deterrence of the adversary.

The second technology that could lead to the physical use of nuclear weapons in future wars could be situations created by the digital age that evoke the possibility of loss of control over a situation and so may lead to nuclear escalation even when a side realises that there is no premium in striking first. Cyberattacks could lead to situations that might compromise the negative controls over nuclear command and control (NC2) by instigating pre-emption through false alarms or misinformation fed into the system. At the same time, they could also affect positive controls by not allowing launch activation by jamming/corrupting or fooling the system. The fear of such compromise of NC2 could compel nations to adopt risky nuclear postures, posing a higher order threat of inadvertent nuclear war.

Indeed, any kind of cyber disruption of satellites used for early warning, communication and intelligence, surveillance, reconnaissance (ISR)m or ground-based radars and transmitters, or against recce and communication aircraft could trigger unintentional escalation. It is not surprising, therefore, that the US's NPR warns potential adversaries that Washington would consider using nuclear weapons in the event of "significant non-nuclear strategic attacks… on US or allied nuclear forces, their command and control, or warning and attack assessment capabilities (8)." While nuclear retaliation against a cyberattack does not appear to be a wise move since attribution of a stealthy cyberattack is not easy, and it could also trigger a nuclear response, which would only make the situation more difficult, not easier.

Therefore, efforts at addressing cyber challenges to NC3 network defence, authentication, data integrity, and assurance of secure and reliable information flow are critical. Enhanced resilience of systems to ensure survivability, including through investing in adequate redundancy, is critical. At the same time, there is a need for efforts at bilateral or multilateral fora to establish norms to restrict the use of cyber weapons against nuclear systems. Any agreement that mandates the non-targeting of nuclear systems through cyber disruptions would be for the benefit of all. Similarly, agreements that lower alert levels of nuclear forces from hair-trigger postures will also ease pressures on hasty decision-making.

The third technological development likely to shape future wars can be seen as coming from the growing potential risks and opportunities being presented by military applications of artificial intelligence (AI) in the fields of robotics, autonomous vehicles, supercomputing and quantum computing, all of which are still to fully reveal themselves (9). In some dimensions, it could prove to be a useful enabler. For instance, in the case of ISR, decision support, simulation and modelling, as also for collecting and analysing large volumes of information, AI could be of major help. Better information could lead to

better-informed decisions. AI-guided ISR that provides multi-domain situational awareness or real-time information analysis of the battlefield could have huge implications for precision targeting by AI-led autonomous weapons operating in any medium (land, air, sea, or even space and cyber). This, according to supporters of AI, would enable militaries to conduct more precise and discriminate targeting. This would result in nuclear counterforce targeting and thus reduce risks to civilians.

But for a nation that feels that its adversary has an AI advantage, this could look highly threatening. And, in the nuclear game, an adversary that feels cornered or on the edge because it senses a vulnerability to the survivability of its nuclear forces, can be a greater danger. The ability to target strategic assets with conventional precision strike capabilities, enhanced through AI, may heighten instability in crisis situations. The threat of disarming first strikes without using nuclear weapons, especially if the attacking side also has a ballistic missile defence (which itself may be made more effective through AI technologies), would end up severely undercutting the nuclear deterrence of the other side. This may compel nations to put their nuclear forces on hair-trigger alert or low alert levels and tempt them to use nuclear weapons first and early in a conflict. Therefore, AI could end up magnifying concerns of deterrence stability, escalation management and conflict resolution by leading to a loss of human control over the use of force.

In a crisis, the employment of AI-enabled ISR, autonomous sensor platforms, automated target recognition, or even the perception of availability of such a system with the adversary could lead to inadvertent escalation. As said in a RAND report, "AI may be strategically destabilizing not because it works too well but because *it works just well enough to feed uncertainty*" (10). A nation's sense that the adversary has the theoretical capability to conduct a disarming first strike will cause a security dilemma and lead him to develop countermeasures, including defences against counterforce strikes and hardening and camouflage to evade or confuse the ISR. Lawrence Freedman, a prominent nuclear strategist, had warned in 1991 that "To the extent that AI influences perceptions of intent and capability and alters the calculus of risk and reward, it will inspire new thinking about possible offensive and defensive maneuvers in the evolution of nuclear strategy" (11).

Perceptions of how AI-enabled technologies may alter the battlefield could lead to an arms race as nations take steps to reverse a perceived disadvantage by investing in relevant defences and other countermeasures to enhance the survivability of their nuclear forces. For instance, Russia justifies the use of AI, particularly its doomsday drone or the Oceanic Multipurpose System Status 6, which is supposed to be an autonomous vehicle launched from a submarine and equipped with the intelligence to evade all oceanic defences to carry a nuclear payload to cause damage to the adversary and ensure the credibility of its deterrence against US BMD or anti-submarine warfare capabilities.

Another worrisome dimension of AI comes from its support for decision-making through the compression of timelines. While this may be of help to a commander by assisting him in making sense of the available information, it could also increase pressures for immediate action and may get nations to stumble into further escalation inadvertently. The speed of decision-making, therefore, could be both an asset and a liability. As cautioned by a report, "the speed at which AI-guided ISR could direct and execute kinetic operations could limit options for de-escalation" (12). It could shrink the time for political or diplomatic action to resolve a crisis. It would be imprudent to forget that "in practice, slowing things down can be the key to victory, especially when the options include nuclear weapons (13)."

To the extent that AI increases the speed and precision of targeting, undercuts the sense of mutual vulnerability, and strengthens the sense that one side can overwhelm the other's deterrence, it could prove to be destabilising. Such tendencies could tempt pre-emption to prevent strategic surprise early in the conflict and cause an unwanted nuclear exchange. Therefore, the utilisation of AI on the battlefield needs to be intelligently managed for its benefits with a clear-eyed recognition of the risks.

Conclusion

The two doctrinal developments and three technological advancements discussed above seem to hold the potential to shape the role that nuclear weapons may play in future wars. While these trends appear to offer the lure of managing nuclear escalation, this promise could prove to be ephemeral and even dangerous. The use of nuclear weapons by one country against another that has the same capability will inevitably lead to a nuclear exchange. The consequences of even a modest exchange would reverberate across the immediate ground zero and even for generations.

Nuclear weapons are one kind of weapons whose value may be exploited for political reasons, but whose military use could spoil the game. These weapons have a role only when they do not physically come into play in warfare. They can, and do, shape wars merely by their presence. The shadow of nuclear weapons will continue to play this role in future wars too. In fact, this shadow will grow as deterrence is sought to be maintained by more risky postures encouraged by doctrines and enabled by technologies.

Nuclear deterrence, it appears, will become more risk-tolerant in the short to medium term. There will be a greater projection of bravado related to managing nuclear escalation. However, the flip side is that it could seriously raise the risks of inadvertent use. In the long term, nations may realise the futility of living with such risks. But, for now, the nuclear shadow on future wars between states that possess such a capability can be expected to be more overtly flaunted and palpably signalled to shape adversary's responses. Boundaries could be pushed, and new waters tested. Hopefully, nations will return to understanding the basics of nuclear deterrence without reliving the painful lessons of Hiroshima and Nagasaki.

Endnotes

(1) Richard Falk and David Krieger, *The Path to Zero: Dialogues on Nuclear Dangers* (Boulder and London: Paradigm Publishers, 2012), p. 26

(2) Office of the Secretary of Defence, Nuclear Posture Review,2018, p. 8, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

(3) Office of Secretary of Defence, p. 26

(4) Office of Secretary of Defence, pp. 30–31

(5) George Fernandes, "The Challenges of Limited War: Parameters and Options," Inaugural address at National Seminar organized by IDSA, 05 Jan 2000, http://www.idsa-india.org/defmin5-2000.html

(6) India too is believed to be doing R& D in this direction. So are Japan, Israel and South Korea.

(7) US Department of Defence, *Quadrennial Defence Report*, Washington DC, Feb 2010, pp 32-33

(8) Office of Secretary of Defense, p. 21

(9) Some parts of this argument have been drawn from an earlier piece of the author. See Manpreet Sethi, "Global Nuclear Developments 2017-2020: Implications for India's Nuclear Policy", *National Security*, vol. III, issue 2, Apr-June 2020, pp 232-245.

(10) Edward Geist and Andrew J Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?", *Perspective*, A RAND policy paper, 2018, p. 15. Emphasis added.

(11) Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: St Martin's Press, 1981)

(12) Paige Gasser, Rafael Loss and Andrew Reddie, Summary of workshop on Assessing the Strategic Effects of Artificial Intelligence, held by Centre for Global Security Research, Lawrence Livermore National Laboratory, Sept 20-21, 2018, p. 6.

(13) Zachary Davis, *Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability and Strategic Surprise*, p.10

The Future of Cyber Warfare in the Indo-Pacific

Bart Hogeveen

"(...) cyber war will be to the 21st century what the blitzkrieg was to the 20th century."

General V.P. Malik, Indian Chief of Army Staff (2000) (1)

When Russian forces illegally crossed Ukraine's sovereign borders in February 2022, the world anxiously anticipated a cyber war would unfold. "When countries send code into battle, their weapons move at the speed of light," is how Microsoft President and Vice Chair Brad Smith described the nature of the risk (2). While the world seems to have been spared a digital doomsday, both sides have been fighting one another heavily in the digital domain. Russian security agencies deployed a series of offensive cyber tools for the purpose of reconnaissance and to manipulate, deny, disrupt, degrade, or destroy targeted Ukrainian computers, information systems, and networks (3). On the Ukrainian side, the internet community shored up their defences, seemingly successfully, by rallying global support from various foreign government, industry, and non-government entities in what has come to be known as the IT Army (4).

In this fog of war, the exact details will only reveal themselves after a while, but analysts, officials and government leaders have already started to formulate predictions of the possible security implications in the Indo-Pacific. At the June 2022 NATO summit—which also saw the participation of the grouping's four Asia-Pacific partners Australia, New Zealand, Japan, and South Korea—the heads of governments called out China's systemic challenge to the rules-based international order alongside cyber, space, hybrid and other threats, and its malicious use of emerging and disruptive technologies (5). Evidently, key areas of concern are the lessons Beijing's strategic policy elite may learn from the Russian military's kinetic, hybrid, and digital campaign; the subsequent Euro-Atlantic resolve to reinvest in defence and political solidarity; and the role of cyberwarfare and use of ICT tools in a potential future conflict in the Indo-Pacific region.

Cyber Warfare in the Regional Context

To date, cyber warfare is generally perceived through the lens of state-to-state conflicts where one state uses computer technology to deliberately disrupt, manipulate, degrade, or destroy the information and communications technology (ICT) systems of another state for strategic, political or military purposes (6). Such activities can be conducted by entities within the national security and intelligence community or by third parties acting on behalf of a government.

However, this prism overlooks two other important dimensions. One involves the effort to misinform or manipulate public opinion in a given territory, for instance, through disinformation campaigns. In strategies pursued by countries such as China and Russia, the information environment is an integral part of their broader hybrid and cyber warfare doctrine. It is also an area in which these countries have developed sophisticated capabilities at an industrial scale.

A second overlooked dimension is that of undermining any adversary's economic prosperity. Considering the digital transformation of our economies, the operations of businesses are the first to be affected by any cyber incident. More specifically, targeted efforts to steal intellectual property, business information or trade secrets from entities in foreign economies not only provide aggressors with an unfair competitive advantage, potentially leapfrogging years of research and development investments, but can potentially degenerate a victim nation's long-term prosperity.

The digital domain has made these state practices easier, less costly, largely invisible and highly deniable, and—given China's dominance in IT products and technology infrastructure—made nations in the Indo-Pacific dependent (7).

Acts of cyber warfare, often conflated with the term offensive cyber operations, can come in different shapes and forms. The most prevalent include acts of cyber-enabled espionage, cyber warfare and influence operations as part of a kinetic military campaign, and standalone offensive operations.

The use of cyber capabilities by security and intelligence agencies in a domestic context must be added to this equation. In the current era, conflicts are not purely of an inter-state nature, and any compromises of the internet's technical layers or deployment of malware will have adverse transboundary effects.

Acts of cyber warfare do not occur in isolation and tend to be connected to political tensions, military confrontations, and economic competition. They have been observed in long-time military stand-offs on the Korean Peninsula, coercive actions around the South and East China Seas disputes, around Taiwan, and in the border conflicts between India and Pakistan and India and China. North Korea has also shown a propensity to undertake 'standalone' cyberattacks. For instance, in 2016, North Korean hackers successfully found access to the Central Bank of Bangladesh's messaging system and funnelled away billions of dollars through the Philippines (8).

Cyber-enabled espionage is a significant and widespread phenomenon, particularly in the Indo-Pacific region. The US, China, North Korea, Russia, Australia, Japan, South Korea, and Singapore (9) are among the world's leaders in signals intelligence. But also, in the domestic contexts, the deployment of many concerning acts of cyber warfare tools can be observed.

In efforts to stem discontent, surveil political opposition, demoralise insurgency groups, and control the flow of information and data, security agencies have imposed crude tactics that will easily fit in an inter-state conflict. Examples include frequent internet shutdowns in India, Myanmar, and Indonesia, where governments are abusing their authority over internet service providers; attempts to establish national internet gateways—a system of controlled entry points for internet access—in countries like Myanmar and Cambodia (although the latter has been suspended for now (10)); and the (mis) use of cybersecurity, cybercrime and misinformation laws to stem civil society voices and create an environment of self-censorship (11). These practices severely affect citizens' security, privacy, human rights and fundamental freedom.

Growing Military Cyber Capabilities

The US-China strategic competition is the overriding issue that casts a shadow over many Indo-Pacific regional security issues, including in the cyber domain. China, by now, is seen as an assertive and, at times, aggressive actor using its various advanced cyber capabilities in combination with proxy agents to seek political, military, and economic intelligence advantages, exert coercive influence over foreign government elites, and disrupt social and economic life in opponent states (12).

The global focus on China, however, seems to have offered developing nations in the Indo-Pacific free reign to build and develop their military cyber capabilities without much outside scrutiny. By now, almost all militaries possess some form of cyber capability, and most claim to be able to deploy cyber warfare tools (see Table 1).

Table 1: Overview of Military and National Security Cyber Capabilities of Indo-Pacific Countries

State	Capabilities	Mandate
India	Defence Cyber Agency (est. 2018)	To formulate a cyber warfare doctrine to develop and maintain relevant capabilities to deter, defend and disrupt an opponent's cyber operations.
Australia	Australian Defence Force (ADF) Information Warfare Division (est. 2017)	The ADF's cyber capabilities have two distinct functions: cybersecurity of the ADF and cyber operations.
	Australian Signals Directorate (ASD; cyber capabilities established prior to 2010)	The offensive cyber capability rests with ASD. Offensive cyber capacity in support of military operations is a civil-military partnership (13).
Japan	Self-Defense Forces' (SDF) Cyber Defense Unit (est. 2022)	The unit's primary function is to oversee the cyber defences for the entire SDF. Reportedly, the SDF has no offensive capability or mandate (14).

State	Capabilities	Mandate
China	People's Liberation Army Strategic Support Force (SSF; est. 2015) Ministry of State Security (MSS)	Focused on 'information dominance', the SSF concentrates on information operations, which include synchronisation of cyber, electronic, and psychological warfare components. The SSF aims to develop and deploy significant cyber fires (15). The MSS' activities appear to focus on cyber-enabled intelligence for strategic, political, and economic purposes, typically operating through proxies in the form of advanced persistent threats (16).
Singapore	Digital and Intelligence Service (est. 2022)	A division-sized entity to effectively navigate cyber threats from external aggressors. Its mandate is to provide accurate, relevant, and timely early warning and operational intelligence for the Singapore military to operate as a networked force.
Indonesia	Tentara Nasional Indonesia (TNI) Satuan Siber (est. 2017)	To keep the TNI's information resources safe from interference and misuse or use by other parties; provide protection for strategic data; collect information on threats and disturbances; and be able to build the cyber defence capacity of the TNI in the form of deterrence, prosecution, and recovery capabilities (17).
Malaysia	Cyber Command (est. 2019) Cyber Warfare Signals Regiment (99 RSPS; est. 2021)	To enhance cyber operations by conducting cyber defence operations, cyber exploitation operations, cyber-attack operations and developing cyber expertise, in line with the active defence concept as stipulated in Malaysia's Cyber Security Strategy (18). To strengthen the Malaysian Armed Forces' capacity and preparedness in the face of cybersecurity challenges and cyber threats from various domains, including by considering the acquisition of the latest assets and systems (19).
Philippines	Armed Forces of the Philippines Cyber Group (est. > 2017) Cyber Battalion, Philippine Army (est. 2020)	To defend the country from cyberattacks; gather foreign cyber threat intelligence and determine attribution; secure national security and military systems; support national protection, prevention, mitigation of and recovery from incidents; and investigate cybercrimes under military jurisdiction (20). To support the army's compliance with adopting cyberspace as another domain of operations. It aims to conduct active and defensive cyber operations to protect army cyber assets and defend it from cyberattacks across its different domains of operations.
Vietnam	People's Army of Vietnam, Cyber Operations Command (est. 2018) Force 47 (est. 2017)	To protect the country from cyberattacks, focusing on ensuring national cyberspace security and fighting high-tech crimes, contributing to the defence of national sovereignty over the mainland, airspace, seas, and cyberspace (21). To scour and collect information on social media, participate in online debates to maintain "a healthy cyberspace" and counter any "wrongful opinions" about the regime and protect it and the public from "toxic information" (22).

Arguably, most cyber activities of South and Southeast Asian countries' military focus on the defensive side, concentrated on protecting their ICT networks in peacetime and during armed conflict. But Southeast Asian defence strategists have now started to talk about capabilities to conduct "cyber exploitation operations" and "cyber-attack operations" as well (23).

This cyber warfare discourse goes hand in hand with a surge in the establishment of new institutions. For instance, in March 2022, Singapore announced a plan to establish a Digital and Intelligence Service in the Defence Force as "the digital domain has grown into a full-fledged arena of conflict and contestation" (24), and Japan launched a new cyber defence unit within the Self Defence Forces (25). In April, Indonesia's Chief of Defence reflected on the TNI Cyber Unit's role in mounting cyber defences that can respond to threats from overseas (26).

The US and China have also enhanced their cyber warfare capabilities in recent years. In 2018, under the Trump administration, the US Cyber Command launched the concept of 'persistent engagement', which centres on the idea of seizing and maintaining "the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they manoeuvre" (27). After the reorganisation of the People's Liberation Army Strategic Support Force in 2015, China prioritised boosting its cyber warfare capabilities, in part, by a 'fusion' of military and civilian cyber assets. As a testament, China reportedly managed to enhance its ability to exploit software zero-day vulnerabilities by six-fold in 2021 compared to 2020 (28).

In this competitive environment, other countries may feel compelled to make substantial investments in their indigenous cyber capabilities. For instance, in response to various cyber-enabled intrusions that were attributed to the Chinese state, the Australian government announced an AUD 1.35-billion investment in its defence apparatus' cyber capabilities in 2020 (29).

The establishment of military cyber (defence) entities, in some cases accompanied by significant financial stimulus, illustrate that cyber is a domain of warfare and that more countries are raising their posture and becoming cybersecurity actors.

The Indo-Pacific military cyber posture currently sees a sharp divide between the highly developed and developing nations. For the latter, their stance will, at least for the time being, remain of a defensive nature—in declared policy if not action—and serve a predominantly domestic imperative. Nonetheless, the build-up signals an increasing militarisation of the Indo-Pacific digital domain, which comes with the risk of unintended and immature cyber activities that may spill across borders, particularly from those jurisdictions where political caution and legal scrutiny are less firmly embedded.

Understanding the Cybersecurity Landscape

Most of the developing cyber nations in the Indo-Pacific have been turning a blind eye to the regional security implications of military cyber capabilities, perhaps because they consider such issues the concern of bigger cyber powers. Even within the cybersecurity portfolio of ASEAN, for example, most attention goes to issues like cybercrime, misinformation campaigns, and data security. Other economic and security issues, such as reliable energy, food security, maritime security, and post-Covid-19 economic recovery, take precedence in these countries.

There is also a systemic lack of transparency and willingness to share information in the Indo-Pacific region. Among the advanced cyber nations, China, for instance, does not acknowledge its military cyber capabilities despite overwhelming evidence and does not disclose its policies, doctrine, and command and control mechanisms (30). On the other hand, Canada, Australia, New Zealand, the UK, and the US, which comprise the Five Eyes intelligence alliance, have acknowledged their offensive cyber capabilities and willingness to use these (31), but struggle to form reciprocal and trusted partnerships with others in the region.

Sharing cyber threat information through non-political platforms, such as the Asia-Pacific Computer Emergency Response Team, remains challenging. Not only are national cybersecurity authorities very sparse with their reporting, but disclosed data often lacks methodological rigour and paints a biased picture. Global cybersecurity firms, which fill in part of the puzzle in other parts of the world, face a lack of data points and analytical depth in the Indo-Pacific (32). This weakness in a collective (critical) understanding of the regional cybersecurity threat environment produces a political and policy environment in which cybersecurity risks are either under or overestimated in terms of effects on the economy and regional stability.

International Law and Norms in Cyberspace

The build-up of military capabilities in an area where poor situational awareness pervades is not unique to the cyber domain. To seek reassurance and mitigate the greatest risk, the global community typically relies on existing principles of international law and the responsibility of states to follow agreed norms.

In regard to cybersecurity developments that affect international peace and security, the UN General Assembly recognised in 2013 that international law applies to states' actions in cyberspace. This recognition is part of a normative framework of responsible state behaviour that includes norms of responsible behaviour such as not attacking critical infrastructure, not allowing your territory to be misused for malicious cyber activities, and reporting ICT vulnerabilities responsibly (see Figure 1).

Figure 1: UN Norms of Responsible State Behaviour in Cyberspace

Source: Australian Strategic Policy Institute (33)

The UN Security Council's permanent members have driven this process of establishing legal and normative boundaries since the late 1990s, but other countries have also contributed. For example, ASEAN member states collectively embraced the UN framework in 2018 and are taking steps at the regional level to strengthen cyber stability by enabling a platform for sharing information and good practices and offering capacity-building assistance (34).

While high-level commitments are essential, a gap remains in a shared Indo-Pacific commitment to the outcomes of this UN-centred process. For instance, many states have yet to submit their views on how they see international law being applied to state conduct in cyberspace. Singapore (35), Australia (36), Japan (37), and the US (38) have published their statements, and Malaysia announced an intent to do so (39), but countries such as India, Pakistan, Indonesia, South Korea, the Philippines, Vietnam, and China have not. And most Indo-Pacific nations are yet to attest that they are following agreed UN norms and describe how they observe them.

In the ongoing diplomatic contest of values and interests, the Non-Aligned Movement has aligned around a position that argues against 'the militarisation of cyber space' (40). And India has called on the international community "unilaterally declare to refrain from militarisation or offensive use of ICTs" (41).

Such positions not only look out of touch with the reality of our external environment but also domestic developments; cyberspace has become a national security issue. Furthermore, this position on non-militarisation keeps holding a tendency in place by some countries to refrain from acknowledging and disclosing their capabilities. This undermines the effective application of international law and adherence to norms. Any steps that help take away legal ambiguity and reinforce multilaterally agreed rules should be seen as serving the interests of emerging digital powers and those states intend on acting responsibly.

A Regional Outlook on Cyber Warfare

Geostrategic competition between the US and China will impact the future of cyber warfare in the Indo-Pacific. However, a few distinct regional developments in the region may determine how the use of offensive cyber tools and tactics will play out there.

First, the process of digital transformation of the region's economies and societies is creating a new balance of influence and cyber power. Singapore, Japan, and South Korea are world-leading digital economies; India is a software development powerhouse; China is a global provider of accessible technology and manufacturing resources; and most Southeast Asian countries have embraced ambitious digital economy strategies relying on the Indo-Pacific's burgeoning youth and grassroots tech ecosystems. This trend will continue, albeit at different paces, and digital trade will account for a growing percentage of countries' GDP.

Next, governments in the region are slated to continue to press ahead with reflexive and restrictive regulatory approaches in the cybersecurity, technology and online information environments. The popularity of social media platforms, in combination with the (mobilising) power of the smartphone, is perceived as a challenge to stability by some states and to regime survival or social cohesion by others. Despite a variety in political regimes and levels of prosperity and diverging approaches to internet governance and regulation across the Indo-Pacific, governments in the region, to varying degrees, seem to be on a trajectory where they seek to impose sovereign borders on the different layers that make up the cyber domain.

With the new cyber defence forces that have been formed, discussions of conflicts in Indo-Pacific's cyberspace now enter a new era. The earlier established cyber units have secured a central place in their countries' overall national security posture. The newer cyber defence forces can rely on political interest, and their mandates and influence are more likely to grow. A key determinant of a State's future cyber behaviour will be the extent to which appropriate checks and balances in the context of civilian oversight and control of the cybersecurity agencies can be established.

It is essential to recognise that all three trends can be managed constructively and should concern all stakeholders in the Indo-Pacific equally. Security in the region will remain competitive in the years ahead with suppressed inter-state conflicts and contested national ICT domains. The internet governance communities will have to find an intricate balance between encouraging digital innovation, adequate cybersecurity, a permissive online information environment, and a responsible role for the various security and intelligence services.

The securitisation and militarisation of the cyber domain will continue too. Indo-Pacific governments play their part in this, and the onus of mitigating the risks of misuse or irresponsible use of cyber warfare also lies with them. Nations should be discouraged from entering a 'cyber capabilities arms race'. To achieve this, the multistakeholder community of political leaders, officials, civil society advocates, technicians, and industry experts must keep a close watch on malicious incidents and potentially destabilising trends in capability development, be permitted to call out irresponsible behaviour, and in a position to engage in meaningful and constructive mutual dialogues.

Endnotes

(1) General V.P. Malik, Address at the Indian Defence Services Staff College (2000). Quoted in: Vinod Anand, "Evolution of a Joint Doctrine for Indian Armed Forces", *Strategic Analysis*, July 2000, https://ciaotest.cc.columbia.edu/olj/sa/sa_jul00anv01.html#note1

(2) Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft on the Issues, June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (3) Microsoft, *Defending Ukraine: Early Lessons from the Cyber War*, 22 June 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

(4) Monica Kaminska, James Shires, and Max Smeets, *Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)*, European Cyber Conflict Research Initiative, Tallinn Workshop Report, July 2022, : https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf

(5) NATO, *Madrid Declaration*, paragraph 6, 29 June 2022, https://www.nato.int/cps/en/natohq/official_texts_196951.htm

(6) Australian Cyber Security Centre, *Glossary: cyber warfare*, https://www.cyber.gov.au/acsc/view-all-content/glossary/cyber-warfare. See also: Tom Uren, Bart Hogeveen and Fergus Hanson, Defining offensive cyber capabilities, *Report for the Global Commission for the Stability of Cyberspace*, July 2018, https://www.aspi.org.au/report/defining-offensive-cyber-capabilities

(7) See, for instance: Dirk van der Kley, Benjamin Herscovitch, and Gatra Priyandita, *China Inc. and Indonesia's Technology Future*, ANU National Security College, July 2022, https://nsc.crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2022-07/web_nsc_pop_indonesia_education_no.27_1.pdf

(8) Neha Banka, Explained: The story of how North Korea hackers stole $81 million from Bangladesh Bank, *The Indian Express*, 30 June 2021, https://indianexpress.com/article/explained/bangladesh-bank-robbery-north-korea-lazarus-heist-7375441/

(9) Rory Medcalf, *Contest for the Indo-Pacific: Why China Won't Map the Future*, La Trobe University Press (3 March 2020).

(10) Sebastian Strangio, Cambodia Puts Controversial National Internet Gateway Plan on Hold, *The Diplomat*, 16 February 2022, https://thediplomat.com/2022/02/cambodia-puts-controversial-national-internet-gateway-plan-on-hold/

(11) Janjira Sombatpoonsiri and Sangeeta Mahapatr, *COVID-19 Intensifies Digital Repression in South and Southeast Asia*, Carnegie Endowment for International Peace, 19 October 2022, https://carnegieendowment.org/2021/10/19/covid-19-intensifies-digital-repression-in-south-and-southeast-asia-pub-85507

(12) Institute for International and Strategic Studies, *Asia Pacific Regional Security Assessment 2019,* Chapter Five: China's cyber power in a new era, May 2019, https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5

(13) Fergus Hanson and Tom Uren, *Australia's offensive cyber capability*, Australian Strategic Policy Institute, 2018, https://www.acs.org.au/carousel-pages/policy-brief-australia-offensive-cyber-capability.html

(14) Aimee Chanthadavong, *Japan to bolster national cybersecurity defence with 800 new hires: Report*, ZDNet, 5 July 2021, https://www.zdnet.com/article/japan-to-bolster-national-cybersecurity-defence-with-800-new-hires-report/

(15) The Hague Centre for Strategic Studies, *Cyber Arms Watch: An Analysis of Stated & Perceived Offensive Cyber Capabilities*, May 2022, https://hcss.nl/wp-content/uploads/2022/05/Cyber-Arms-Watch-HCSS-2022-1.pdf

(16) Institute for International and Strategic Studies, *Asia Pacific Regional Security Assessment 2019,* Chapter Five: China's cyber power in a new era, May 2019, https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5

(17) Ministry of Communication, Government of Indonesia, *TNI bentuk Satsiber,* https://m.kominfo.go.id/content/detail/10997/tni-bentuk-satsiber/0/sorotan_media

(18) Ministry of Defence, Government of Malaysia, *Defence White Paper*, paragraph 38, 2020. https://www.mod.gov.my/images/mindef/article/kpp/DWP-3rd-Edition-02112020.pdf para 38.

(19) MalayMail, *Malaysian Armed Forces to set up cyber warfare regiment to strengthen cyber defence, says army chief*, 2 March 2021, https://www.malaymail.com/news/malaysia/2021/03/02/malaysian-armed-forces-to-set-up-cyber-warfare-regiment-to-strengthen-cyber/1954285

(20) Department of ICT, Government of The Philippines, *National Cyber Security Plan 2022*, https://dict.gov.ph/national-cybersecurity-plan-2022/

(21) People's Army Newspaper, *MND debuts Cyberspace Operations Command*, 9 January 2018, https://en.qdnd.vn/military/news/mnd-debuts-cyberspace-operations-command-488684

(22) Dien Nguyen An Luong, "How The Vietnamese State Uses Cyber Troops to Shape Online Discourse"*, ISEAS Perspective 2021/22*, 3 March 2021, https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2021-22-how-the-vietnamese-state-uses-cyber-troops-to-shape-online-discourse-by-dien-nguyen-an-luong/

(23) Ministry of Defence, Government of Malaysia, *Defence White Paper*, paragraph 38, 2020. https://www.mod.gov.my/images/mindef/article/kpp/DWP-3rd-Edition-02112020.pdf; and National Security Council, Government of Malaysia, *Malaysia Cyber Security Strategy, 2020-2024*, https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

(24) Ministry of Defence, Government of Singapore, *Fact Sheet: Timely Establishment of Digital and Intelligence Service*, 2 March 2022,https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2022/March/02mar22_fs

(25) Japan Times, *Japan's Self-Defense Forces launch new cyberdefense unit*, 17 March 2022, https://www.japantimes.co.jp/news/2022/03/17/national/sdf-cyberdefense-unit/

(26) Tempo, *TNI Commander Talks of Future Cyber Threats*, 28 May 2021, https://en.tempo.co/read/1466510/tni-commander-talks-of-future-cyber-threats

(27) Jacqueline Schneider, Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy, *Lawfare*, 10 May 2019, https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy

(28) Patrick Howell O'Neill, How China built a one-of-a-kind cyber-espionage behemoth to last, *MIT Technology Review*, 28 February 2022, https://www.technologyreview.com/2022/02/28/1046575/how-china-built-a-one-of-a-kind-cyber-espionage-behemoth-to-last/

(29) Jane Macmillan, Cybersecurity spending gets $1.35 billion boost in wake of online attacks against Australia, *ABC*, 29 June 2020, https://www.abc.net.au/news/2020-06-29/cyber-security-investment-link-attacks-scott-morrison/12404468

(30) Nigel Inkster, *China's cyber power*, Institute for International and Strategic Studies, 2016.

(31) Josh Gold, *The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'*, NATO Cyber Cooperative Cyberdefence Centre of Excellence, 2020, https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf

(32) Author's conversations.

(33) https://www.aspi.org.au/cybernorms

(34) ASEAN, *ASEAN Leaders' Statement on Cybersecurity Cooperation*, 2018, https://asean.org/asean-leaders-statement-on-cybersecurity-cooperation/

(35) Cyber Law Toolkit, National position of Singapore (2021), https://cyberlaw.ccdcoe.org/wiki/National_position_of_Singapore_(2021)

(36) Cyber Law Toolkit, National position of Australia, https://cyberlaw.ccdcoe.org/wiki/National_position_of_Australia_(2020)

(37) Cyber Law Toolkit, National position of Japan, https://cyberlaw.ccdcoe.org/wiki/National_position_of_Japan_(2021)

(38) Cyber Law Toolkit, National position of US, https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_United_States_of_America_(2021)

(39) National Security Council, Government of Malaysia, *Malaysia Cyber Security Strategy, 2020-2024*, https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

(40) Paul Meyer, *A New Process for an Old Problem: Governing State Behaviour in Cyberspace*, Centre for International Governance and Innovation, 25 November 2019, https://www.cigionline.org/articles/new-process-old-problem-governing-state-behaviour-cyberspace/

(41) Contributions of the Indian delegation to the UN Open-ended Working Group on ICT Security, 2019-2021.

The Use and Potential of Cyber Weapons in Contemporary and Future Conflict

Noëlle van der Waag-Cowling, Brett van Niekerk,
and Trishana Ramluckan

Cyber weapons are subject to much debate and misunderstanding. Their intangible nature and the secrecy that surrounds their development and existence make it difficult for laypeople and military analysts alike to understand their usage and potential and indeed their very existence. Unlike the traditional order of battle that details a given state's conventional assets and forces, cyber weapons and capabilities are more difficult to gauge due to the opaque nature of the cyber domain (1).

Cyber weapons pose a multitude of challenges to both those who possess them and those who aspire to do so. From a developmental perspective, they are profoundly resource- and time-intensive, with an accompanying and persistent risk of obsolescence. From a norms perspective, they pose the risk of offensive cyber capability (OCC) proliferation amongst states and malign non-state actors, a situation aggravated by the dual-use nature of digital technologies (2). However, unlike kinetic weapons, properly purposed cyber weapons offer the proposition of varying options for states, which can be stealthy, extremely precise, and even de-escalatory (3). Conversely, a poorly reconnoitred and constructed cyber exploit can be blunt and cause considerable collateral damage with far-reaching disruption and damage.

For armed forces, the development and ownership of cyber weapons necessitates a wide process of doctrinal and operational evolution that is highly predicated on significant funding and deep scientific and human capital resources. Consequently, offensive cyber capabilities are beyond the reach of many states. How this will shape the geostrategic responses of such states going forward is a vital question (4). This article seeks to provide an overview of cyber weapons, their usage to date, and their potential and drawbacks as elements of conflict and inter-state relations.

Conceptual Perspectives on Cyber Weapons

The term 'cyber weapon' is often used rather loosely, thereby creating substantial confusion. In the purest sense, cyber weapons are specifically purposed offensive exploits that aim to achieve a desired tangible strategic or tactical effect. There are several prevailing views on cyber weapons and what they are—one approaches them from a system capability angle, while another, arguably older, view is narrower and focuses on the exploits and their code.

The US Strategic Command's Cyber Warfare Lexicon defines a cyber weapon system (CWS) as "A combination of one or more weaponised offensive cyber capabilities with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency" (5). The term 'system' is core to this discussion as, unlike most conventional military materiel, a cyber weapon is the sum of all parts of an ecosystem that is required to imagine, design, render, and deploy it. Scholar Max Smeets' explanation is instructive in this regard: "Instead of a weapon, an offensive cyber capability in fact refers to the ability of an actor to undertake cyber operations. Cyber operations are a set of linked activities—bringing together technology, skill, and organizational processes—spanning from target acquisition to payload delivery and consequent operations which follow the successful breach of the target. To perform cyber operations, an actor may rely on certain tools or infrastructure to conduct the activity effectively" (6). Smeets thus avoids defining cyber weapons and rather focuses on offensive cyber operations, claiming that an offensive cyber operation can be conducted without a cyber weapon.

Thomas Rid and Peter McBurney provide a more functional definition of the objectives of a cyber weapon: "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings" (7). The Tallinn Manual 2.0 provides a broader yet more outcomes-driven definition, including more tools outside of computer code, but limits the consequences to physical impacts, namely damage, destruction, death or injury, based on the legal definition of an armed attack (8). For the sake of clarity, this article will utilise the terms cyber weapons, cyber operations, and cyber capabilities as part of an interrelated whole.

Cyber Operations in Armed Conflict

Instances where cyber operations have been used during times of armed conflict between countries include the Georgia conflict in 2008, the annexation of Crimea in 2014, up to and including the ongoing Russian-Ukraine conflict of 2022. In Georgia, the primary cyber tool was distributed denial-of-service (DDoS) attacks and website defacements, which disrupted official websites and communication and appeared to be used to limit the narratives on the conflict (i.e., they overwhelmed the Georgian networks so only the Russian narrative was available) (9). This was the first recorded case of cyber operations being used in conjunction with a major military operation (10), seemingly employed for a particular strategic purpose and did not necessarily directly affect the tactical military situation.

During the annexation of Crimea, cyber operations appeared to have been used in coordination with other methods to disrupt communication networks during the initial incursion into Crimea. However,

DDoS attacks and website defacements had been occurring prior to and after the annexation of Crimea (11). In the period between the annexation of Crimea and the 2022 Russian-Ukraine conflict, while low-intensity conflict was occurring in the East of Ukraine, malware attributed to Russia disrupted power grids in Ukraine in December 2015 and 2016 (12). In 2017, the Not Petya malware, a ransomware worm, became one of the most disruptive and expensive cyber incidents globally, but appears to have initially been targeted at Ukraine (13). This incident illustrates the issue of controlling cyber weapons, resulting in them escaping the confines of their intended target(s) and causing significant digital collateral damage. In addition, it was reported that Ukrainian Android mobile phones were infected with malware linked to Russian state actors, enabling them to track Ukrainian artillery units between 2014 and 2016 (14). Such cyber operations, while not an attack per se, can potentially give a military advantage for targeting purposes. Other attempted cyberattacks include one on a chlorine distillation plant and on the Ukrainian Security Service website (15).

In 2022, numerous cyber operations and incidents have been reported in relation to the Russia-Ukraine conflict, but few appeared to have a specific impact on military operations. However, some notable cyberattacks have occurred, such as a satellite Internet provider (ViaSat) experienced a cyberattack (occurring in conjunction with the Russian military operation) that disrupted networks in Ukraine and other European countries; the hack of Ukrainian media with a fake message to surrender; a deepfake of Ukrainian President Volodymyr Zelenskyy calling for his troops to surrender; claims of cyberattacks by hacktivist collectives on trains to disrupt Russian troop movements; and reports of a coordinated Russian cyberattack and missile strike (see Table 1 for cyber incidents related to the Russia-Ukraine conflict) (16). Of these, only the disruption of trains carrying troops would have a direct tactical military consequence, but fake calls to surrender, if successful, could also present an advantage on the battlefield. Two tactics not prevalent in previous conflicts are the use of wiper malware and hack and leak operations, with the wiper malware potentially signifying an ‘evolution’ of cyber weapons. As researcher Erin Harding indicates, Russian cyber activity appears to be tailored towards reducing the effectiveness or diminishing confidence in the Ukrainian government, and a different selection of strategic targets may have proved to be more effective (17). In addition, support from other nations and the volunteers probably aided the holistic defence of Ukraine, and private sector attribution of cyber operations to Russia did not deter the operations but, along with publicly exposed plans, allowed for a coordinated defence and quicker assistance (18). The tactics demonstrated in Russian cyber operations appeared consistent with those in Georgia and related to the annexation of Crimea, indicating that there was also a greater degree of preparation for cyber defence, limiting the effectiveness of the operations. Cybersecurity journalist Sean Lyngaas reported opinions providing reasoning for the apparent limited cyber operations, including that in an overt conflict, kinetic weapons can be used, and cyber tools can be kept for periods outside of open armed conflict (19).

Table 1: Recorded Cyber Incidents During the Russia-Ukraine Conflict (as of July 2022)

Attack type	Target		
	Ukraine	Russia	Another country/ organisation
Cyber-enabled information operations/disinformation	5	6	2
Cyberespionage	17	1	2
DDoS	12	9	33
Defacement	5	3	3
Hack and leak	1	52	5
Malware	7	2	1
Phishing	7	1	5
Ransomware	0	4	3
Wiper	14	2	1
Other	2	0	0
Total	**88**	**83**	**64**

Source: CyberPeace Institute (20)

Additionally, Israel allegedly used cyber operations to affect Syrian radar systems in 2018 and to support an airstrike in 2007 (21). Such cyber operations can potentially have a tactical impact on military operations, providing additional protection for aircraft due to the degraded ability to detect them on the radar. The Stuxnet worm that targeted the Iranian nuclear programme is also sometimes considered a cyberweapon, although it was not used in an open armed conflict. It is also an example of a cyberattack that broke out of its original target, resulting in its detection (22).

Limitations and Affordances of Cyber Weapons

As the above historical synopsis illustrates, advanced cyber weapons or exploits can be deployed to degrade and disrupt an adversary rather effectively with the significant advantage of plausible deniability on the part of the offensive force. It is important to note that not all the cases discussed involve cyber weapons per se but rather malware that has been weaponised for a specific strategic purpose. To date, most known targets have primarily been critical national infrastructure or high-profile civil entities rather than military targets. This raises the spectre of a potential differentiator between cyber operations and other military operations. Cyber operations may have a far more direct impact on civil society and state stability, particularly during peacetime, than physical military operations. This is compounded by the capacity for contagion and the resultant damage to unintended targets when a cyber exploit is deployed; "a cyber operation could have consequences that are unintended by the initiator, either because the initiator is reckless as to such a risk or because there has been a failure of mission and risk analysis" (23). Conversely, "Cyber weapons also offer the potential of exquisite precision because, if well designed, they may affect only specific targets and inflict carefully tailored effects" (24). Scholar Ben Buchanan discusses the challenges of cyber operations within international relations, particularly where defensive cyber operations in a 'defend forward' or intelligence context

may be indistinguishable from offensive cyber operations, resulting in an escalatory cycle of systems intrusions for defensive purposes (25).

It is through the precision and tailored effects of strategic cyber operations that states seek to achieve security and foreign policy objectives without engaging in physical combat or, indeed, even acknowledged conflict. The desired strategic effect of such operations is usually to degrade an adversary's capability, as in the Stuxnet episode, or to coerce an adversary into backing down or changing course. It is these properties of cyber operations that are valued for their ability to assist in neutralising threats without resorting to kinetic conflict in what Brandon Valeriano and Benjamin Jensen term 'de-escalation pathways' (26). George Perkovich and Ariel Levite stress the 'stand-off potential' of CWS: "They can be operated from a distance to achieve global reach, sparing the conductors from friction with intermediaries and from risks of interdiction, capture, or death" (27).

On the negative side, there are the unknown effects of increasingly 'high-end spectrum' cyber weapons with kinetic potential and the possibility of systemic damage and the subsequent cascading effects on civilian populations in particular (28). Owning cyber weapons poses some unique challenges and risks. The stockpiling or suspected stockpiling of weapons creates mistrust and tensions between adversaries, and confidence-building measures will be especially challenging due to the invisible nature of digital entities. The secure storage of cyber exploits is a further significant issue. This problem is closely followed by the harvesting of a weapons code once it has been launched in the wild. There is sufficient evidence of the re-engineering of cyber weapons by nefarious actors for further usage—the case of the Shadow Brokers and the US National Security Agency hacking tools is a case in point (29). A major consideration when deploying a cyber weapon is the risk of strategic miscalculation as military understandings of cyber conflict and its escalation dynamics are still at a nascent stage, with states tending to push and test boundaries without necessarily understanding the exact limitations of the escalation threshold (30)."

Cyber Disequilibrium and Offensive Cyber Proliferation

An important factor in cyberspace stability lies in the 'haves and have-nots' of the cyber world or 'cyberspace disequilibrium'. In a somewhat similar fashion to nuclear weapons, where only a limited number of states possess nuclear capabilities, the number of countries with significant offensive cyber capabilities is also limited. This largely reflects the underlying requirement of a technologically and scientifically advanced society, which is essential for developing a cyber weapons programme. Creating a cyber exploit is only part of the process; nations still need to develop a strategic capacity to effectively leverage a sustainable offensive cyber operations capability and integrate it with other operations capabilities. Therefore, the initial technical capability can be easily learnt or proliferated, however, the finesse of what to do with that capability and how to grow it may still be beyond the reach of many nations.

Winnona Desombre et al. outline the tooling chain that underpins cyber weapons systems and identify five pillars of activity in the chain: vulnerability research and exploit development, malware payload generation, technical command and control, operational management, and training and support (31). This approach to understanding the entirety of the CWS interfaces well with Smeets' emphasis on cyber

operations as a "set of linked activities – bringing together technology, skill, and organizational processes – spanning target acquisition to payload delivery and beyond" (32). It is, however, the emphasis of both approaches on the importance of human capital that is of particular note. This is potentially the single largest factor that will drive persistent inequalities in cyber capabilities between states. Creating the pipeline that will provide high-end cyber related skills is a decades-long enterprise requiring a whole-of-society approach that focuses on national systems of education, science and innovation. For many countries, the skills gap is widening, not closing. Given the small number of states that are currently assessed to constitute top-tier cyber powers (33), we cannot yet accurately fully understand or predict how cyber means will be deployed during military operations and against critical national infrastructure targets when more states have access to such capabilities in the future.

What then are the ramifications for national security and vulnerable populations in such states? Even in the most digitally underdeveloped regions of the globe, there are areas of critical cyber dependency (34). Increasingly, these dependencies are linked to energy and supply chain security and, by extension, to food and health security. It is postulated that this capability disparity will, alongside the utility of proxy operations, be one of the drivers of cyber mercenaryism and OCC Access as a Service (AaaS). AaaS groups are already widely believed to assist states that lack the necessary skills and resources in developing OCC. The proliferation of AaaS actors means that at least some form of 'turnkey' offensive cyber means is within reach of almost all states and many non-state actors. For those who can afford their services, "Access-as-a-Service firms offer government-level capabilities at private sector speeds (35)." However, OCC proliferation may also drive the genesis of less sophisticated cyber weapons with limited precision and containment as well as no regulatory visibility. Countering the proliferation of such actors and their services is a far more complex proposition than monitoring physical arms shipments and transactions (36). The necessary code or tools to function as a cyber weapon can be delivered via the cloud or a small memory device or on consumer electronics such as a laptop or smart phone.

The creation and proliferation of a cyber weapon, however, is different from developing a mature state capability to conduct coherent offensive cyber operations (37). We postulate that a key outcome of this may be the development of an irregular guerilla-style cyber conflict that focuses on randomised raids on soft targets, such as civilian infrastructure. This would be a more sustainable strategy for immature cyber states and insurgent or terrorist groups. This would negate the requirement of building and maintaining persistent, mature cyber capabilities that are, in part, designed to complement conventional capabilities in a progression towards network-centric warfare. To this end, the key attributes of deception and surprise will be important factors in irregular cyber operations, as this will assist in mitigating other shortfalls in cyber-related resources (38).

A key point here is that as the threat probability multiplies and the number of potential protagonists expands, the need to work towards a global normative arrangement for the regulation and stability of cyberspace increases.

Cyber Weapons and International Law

In 2013, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security released a report, adopted as a resolution

by the UN General Assembly, that international law, the UN Charter, and principles of state sovereignty all apply in cyberspace, and the need for states to meet their international obligations concerning internationally wrongful acts occurring in cyberspace that may be attributed to them (39). As indicated by Francois Delerue, there are diverse opinions on whether a cyber operation by a state against another will constitute a breach of sovereignty on the injured state (40). For example, the Tallinn Manual 2.0 focuses on the severity of a cyber operation or system intrusion, whereas Delerue considers any intrusion on a State's information and communication technology (ICT) infrastructure by another state as a breach of sovereignty (41). As only an action by a State can breach another State's sovereignty (42), the use of proxies further complicates the determination of a breach of sovereignty due to possible difficulties in attribution. Attribution of a cyber operation has technical, political, and legal aspects, and is complex due to the ability to reuse code, the use of intermediary infrastructure, and the possibility of false flags for deception. When a sub-state entity or proxy is involved, there also needs to be an assessment of the control a State has over those proxies. Alternatively, a state may be held accountable for failure of due diligence if insufficient effort is made to mitigate sub-state cyber operations from within its territory (43). The concept of 'volunteer cyber armies', such as seen in the 2022 Russia-Ukraine conflict, and the involvement of other non-state groups, whether encouraged or not, further complicates the environment. The volunteers supporting Ukraine in cyberspace, even if encouraged, are unlikely to be under the direct control of the state, and therefore their actions are not attributable to the state. However, this does raise the question of civilian and mercenary involvement in online conflicts, which is outside the scope of this article

The Wassenaar Arrangement is applicable to the control of cyber weapons as defined in this article. The Arrangement was created to contribute to regional and international security and stability through the promotion of transparency and responsibility to a larger extent concerning the transfer of standard arms and goods and technologies for dual use, thereby preventing destabilising stockpiling of cyber weapons. Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities that undermine these goals and are not diverted to support such capabilities (44). However, cyber weapons and related information required to develop cyber weapons are often used for defensive purposes, for example, to test the security of ICT infrastructure or to develop patches. There were apparent misunderstandings regarding the nature of cybersecurity that may have resulted in the degradation of cybersecurity practitioners' ability to protect networks, eventually resulting in updates to the Agreement (45).

Increasingly, the discussion has begun to shift from measures to control cyber weapons to seeking international agreement on what constitutes legitimate targets or objectives of a cyber operation instead. Proponents of this approach point to the obvious difficulties of cyber arms control (46). In addition, an equivalent effect may be achieved through abusing insecure access rather than through a cyber weapon.

Conclusion

Offensive cyber capabilities will continue to become more mainstream as part of larger military combined operations as warfighting moves towards a network-centric future. Cyber weapons will continue to evolve and pose greater threats to societies due to greater interconnectedness and smart societies.

A fundamental property of cyber weapons that is unlikely to change is their highly transitory nature when compared to most kinetic weapons. The utility of cyber weapons is restricted by the rapid rate of decline in their ability to cause harm (47). This gives rise to the proposition that advanced and sovereign offensive cyber capabilities will remain the preserve of advanced and economically stable states. To counteract this problem and the accompanying sense of susceptibility, less 'cyber-capable' states and non-state actors may potentially lean towards a pay-as-you-go approach and leverage OCC via AaaS providers and brokers. Less capable nations are unlikely to move beyond such a mode unless there is a persistent and targeted cyber threat that necessitates the development of a standing cyber force to counter the threat.

The civilian nature of digital infrastructure means that strategic cyber threats have a high likelihood of causing collateral damage or are directly targeted at civilian infrastructure to degrade a population's will to fight; the examples discussed in this article illustrate both. While cyber operations have been used in conjunction with kinetic attacks, these had limited direct military benefits beyond disrupting civilian communication and media. Cyber weapons are likely to remain as military assets best used outside of direct armed conflict for the foreseeable future but will continue to play a significant role in strategic interference. The planning required for cyber operations renders them largely unsuitable for directly targeting military equipment at present. However, commercial civilian equipment used in infrastructures can be easily obtained for testing and developing targeted cyber weapons, provided there is a sufficient financial and intellectual investment.

The difficulties in defining cyber weapons, hindering proliferation, and conceptualising their implications within international law (particularly related to thresholds) is resulting in a shift towards normative processes emerging out of the UN Group of Governmental Experts, and a focus on defining legitimate targets and effects. Until adequate consensus at an international level can be achieved, cyber operations will continue to pose both a strategic and societal threat due to the uncertainty of how to address them.

Endnotes

(1) Jason Healey., "Preparing for the Inevitable Cyber Surprise," War on the Rocks, *Texas National Security Review*, January 22, 2022, https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/

(2) Noelle Van der Waag-Cowling., "Stepping into the Breach Stepping: Military responses to global cyber insecurity,", *ICRC Law and Policy Blog,* June, 2021, https://blogs.icrc.org/law-and-policy/2021/06/17/military-cyber-insecurity/

(3) Brandon Valeriano and Benjamin Jensen, "De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War," in *Cyber Peace: Charting a Path Towards a Sustainable, Stable, and Secure Cyberspace*, ed Scott Shackelford et al. (Cambridge University Press, 2020).

(4) T. Maurer, "Cyberspace and International Relations: Rising Powers, Proxies, and Norms" (PhD Diss., Freien Universität Berlin, 2019), pp. 8-10.

(5) A.F. Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision- Making*, (Athens, GA: University of Georgia Press, 2016), pp.15.

(6) Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, (London: Hurst & Co, 2022), Kindle.

(7) Thomas Rid and Peter McBurney, "Cyber-Weapons", *The RUSI Journal,* 157, no. 1 (2012): 6-13.

(8) Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017)

(9) Kim Hart, "Longtime Battle Lines are Recast in Russia and Georgia's Cyberwar", *The Washington Post*, August 14, 2008, https://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html; David Hollis, "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, (2011), https://web.archive.org/web/20220304223742/https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf; Joseph Menn, "Expert: Cyber-attacks on Georgia websites tied to mob, Russian government", *Los Angeles Times*, August 13, 2008, https://www.latimes.com/archives/blogs/technology-blog/story/2008-08-13/expert-cyber-attacks-on-georgia-websites-tied-to-mob-russian-government

(10) Hollis, "Cyberwar Case Study.

(11) Brett van Niekerk, "Information Warfare in the 2013-2014 Ukraine Crisis," in *Cybersecurity Policies and Strategies for Cyberwarfare Prevention*, ed. Jean-Loup Richet (Hershey: IGI Global, 2015), 307-339.

(12) Laurens Cerulus, "How Ukraine became a test bed for cyberweaponry," *Politico*, February 14, 2022. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/; Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, E-ISAC and SAN ICS Defence Use Case, March 18, 2016, https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf; Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

(13) European Parliament, *Briefing: Russia's war on Ukraine: Timeline of cyber-attacks*, European Union, June 12, 2022, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549

(14) Dustin Voltz, "Russian hackers tracked Ukrainian artillery units using Android implant: report," *Reuters*, December 22, 2016, https://www.reuters.com/article/us-cyber-ukraine-idUSKBN14B0CU

(15) European Parliament, *Briefing: Russia's war on Ukraine.*

(16) CyberPeace Institute, *Timeline: How have cyberattacks and operations evolved over time since the military invasion of Ukraine?* (2022), https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline; European Parliament, *Briefing: Russia's war on Ukraine;* Matthew Holroyd Fola Olorunselu, "Deepfake Zelenskyy surrender video is the 'first intentionally used' in Ukraine war," *Euronews*, March 16, 2022, https://www.euronews.com/my-europe/2022/03/16/deepfake-zelenskyy-surrender-video-is-the-first-intentionally-used-in-ukraine-war; Vilius Petkauskas, "Ukraine says Russia coordinated cyber and missile attacks," *Cybernews*, July 4, 2022, https://cybernews.com/cyber-war/ukraine-says-russia-coordinates-cyber-and-missile-attacks/; Joe Uchill, "New narrative forms on Russia-Ukraine cyberwar as Viasat outage investigated," *SC Magazine*, March 14, 2022, https://www.scmagazine.com/analysis/cyberespionage/new-narrative-forms-on-russia-ukraine-cyberwar-as-viasat-outage-investigated.

(17) Erin Harding, "The Hidden War in Ukraine," Centre for Strategic and International Studies, June 15, 2022, https://www.csis.org/analysis/hidden-war-ukraine

(18) Harding, "The Hidden War in Ukraine".

(19) Sean Lyngaas, "Russia's cyber offensive against Ukraine has been limited so far. Experts are divided on why," *CNN*, March 12, 2002, https://edition.cnn.com/2022/03/12/europe/russia-ukraine-war-cyber-attacks/index.html

(20) CyberPeace Institute, *Timeline*.

(21) L. Tabansky, "Israel Defense Forces and National Cyber Defense", *Connections* 19, no. 1 (2020): 45-62.; Sharon Weinberger, "How Israel Spoofed Syria's Air Defense System", *Wired*, October 4, 2007, https://www.wired.com/2007/10/how-israel-spoo/

(22) Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, (New York: Broadway Books, 2015).

(23) Kubo Macak and Ewan Lawson, "Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts," 2021, 12.

(24) James. M. Acton, "Cyber Weapons and Precision-Guided Munitions," in *Understanding Cyber Conflict 14 Analogies,* ed George Perkovich and Ariel E. Levite (Georgetown University Press, 2017), 45.

(25) Ben Buchanan, *The Cyber Security Dilemma: Hacking, Trust and Fear between Nations*, (Oxford, UK: Oxford University Press, 2017), Kindle.

(26) Valeriano and Jensen, "De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War".

(27) George Perkovich and Ariel Levite, "Conclusions," in *Understanding Cyber Conflict 14 Analogies*, 2017, 257.

(28) Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal* 157, no. 1 (2012), 7, https://doi.org/10.1080/03071847.2012.664354

(29) P.J. Mallick, Cyber Weapons a Weapon of War? Vivekananda International Foundation, 13, 2021. https://indianstrategicknowledgeonline.com/web/Cyber-Weapons-A-Weapon-of-War.pdf

(30) Van der Waag-Cowling, "Stepping into the Breach".

(31) Winnona Desombre et al, "A Primer on the Proliferation of Offensive Cyber Capabilities," Atlantic Council Snowcroft Centre for Strategy and Security, Issue Brief March 2021, 4. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/

(32) Max Smeets, "What it Takes to Develop a Military Cyber-Force," Policy Perspectives, CSS ETH Zurich, Vol. 10/7, June 2022.

(33) International Institute for Strategic Studies, "Cyber Capabilities and National Power - A Net Assessment," 2021, 9-12. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

(34) Van der Waag-Cowling, "Stepping into the Breach".

(35) Winnona Desombre et al, "A Primer on the Proliferation of Offensive Cyber Capabilities," Atlantic Council Snowcroft Centre for Strategy and Security, Issue Brief March 2021, 5-6. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/

(36) Heidi Swart, "Pegasus and the NSO Group: The dark world of cyber mercenaries," *The Daily Maverick,* August 4, 2021, https://www.dailymaverick.co.za/article/2021-08-04-pegasus-and-the-nso-group-the-dark-world-of-cyber-mercenaries/

(37) Smeets, *No Shortcuts.*

(38) Healey, "Preparing for the Inevitable Cyber Surprise".

(39) United Nations General Assembly, Resolution A/68/98* Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013).

(40) Francois Delerue, *Cyber Operations and International Law*, (Cambridge: Cambridge University Press, 2020).

(41) Schmitt, *Tallinn Manual 2.0*; Delerue, *Cyber Operations and International Law.*

(42) Delerue, *Cyber Operations and International Law*.

(43) Delerue, *Cyber Operations and International Law*; Schmitt, *Tallinn Manual 2.0*; Florian J. Egloff and Max Smeets, "Publicly Attributing Cyber Attacks: A Framework," *Journal of Strategic Studies*, (2021), https://doi.org/10.1080/01402390.2021.1895117; Amir Lupovici, "The 'Attribution Problem' and the Social Construction of 'Violence': Taking Cyber Deterrence Literature a Step Forward", *International Studies Perspectives* 17, no. 3, (2016):322-342.

(44) Wassenaar Arrangement Secretariat, *Public Documents Volume 1: Founding Documents*, (December 2016). https://www.wassenaar.org/app/uploads/2015/06/WA-DOC-17-PUB-001-Public-Docs-Vol-I-Founding-Documents.pdf

(45) Tom Cross, "New Changes To Wassenaar Arrangement Export Controls Will Benefit Cybersecurity", *Forbes,* January 16, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/01/16/new-changes-to-wassenaar-arrangement-export-controls-will-benefit-cybersecurity/

(46) Andrew Futter, "What does cyber arms control look like? Four principles for managing cyber risk," June 2020, 7. https://www.europeanleadershipnetwork.org/policy-brief/what-does-cyber-arms-control-look-like-four-principles-for-managing-cyber-risk/

(47) Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies* 41, no. 1-2 (2018): 7.

Quantum Technology in Future Warfare: What is on the Horizon?

Michal Křelina

NATO refers to quantum technology as an emerging and disruptive technology (1), while the European Union (EU) sees it as an emerging technology of global strategic importance (2). Quantum technology has also been recognised as being of strategic significance with the potential to provide China with "a decisive advantage in future peacetime and wartime competition alike" (3). It is a prime example of dual-use technology, with relevant applications in both civil and military use, and widespread impacts on society and security. For example, there is already a shift in the cybersecurity paradigm due to the quantum threat, and in the long term, quantum computing can tremendously benefit the pharmaceutical and chemical industries and make society more sustainable (4). Therefore, it is highly pertinent to address the question of what impact quantum technologies can have on future conflicts and wars.

The term quantum technology encompasses various technologies that make use of different quantum-mechanical properties (for instance, quantum superposition (5), quantum entanglement (6), or no-cloning theorem (7)) at the level of individual quanta, such as electron, atom, molecule or quasiparticle. Ultimately, quantum technology allows for the realisation of computations reaching up to exponential speedup, highly secure communication, and unprecedentedly sensitive sensors, among others.

At the same time, the overall level of technological readiness of quantum technologies is rather low (8). While some commercially available technologies exist, such as quantum key distribution and atomic clocks, most quantum technologies are at the laboratory level. As such, there is a long transfer period from the laboratory to actual deployment.

The military applications of quantum technology are a subject of active research (9). However, assessing what impact these applications will have in future warfare is difficult. This is due to the combination of

high expectations and quantum hype, the low level of technological readiness (which corresponds to the technology being at the laboratory stage), and, the consequent complicated estimation of future realistic capabilities. For example, in theory, quantum magnetometry has the potential to discover submarines. However, the final capability of sensitivity and resolution is uncertain outside of laboratory performance. To what extent will it be practically deployable, and from which platform: ship, drone, or satellite?

Overview of Quantum Technology

For greater clarity in the discussion of different quantum technologies (10), the following taxonomy is used:

- **Quantum computing** represents universal programmable quantum computers, quantum annealers, and quantum simulators, which all tend to provide some computational advantage (up to exponential speedup) over classical computers. It is important to note that quantum computers will only be efficient and provide some advantages for limited computational problems, typically those with high complexity.

Examples of such problems are quantum simulations (molecule simulation for chemical and pharmaceutical research, new material development), quantum cryptoanalysis (breaking of most of the asymmetric encryption schemes), faster searching, faster solving of linear or differential equations, quantum optimisations (for instance, the travelling salesman or so called NP problems (11) in supply chains, logistics, portfolio or medicaments optimisation), or quantum machine learning.

At the moment, the biggest obstacle to having a powerful and capable quantum computer is the quality and amount of quantum bits, commonly termed qubits. The qubit is a quantum analogy of a bit, a basic computational unit with a value of 0 or 1. Qubits acquire states, which can also be analogously referred to as 0 or 1. Moreover, utilising quantum features such as quantum superposition, the qubit can also be a linear combination of the states 0 and 1, and quantum entanglement causes a strong correlation between two and more qubits that have no classical analogy. A qubit can be realised by various physical systems, such as the spin of an electron or ion, the polarisation of a photon, or the oscillating modes of transmon in a superconductor. Several physical types of qubits have been developed with different progress (12).

The qubit, in principle, is very sensitive and easily disrupted by random interaction with the surroundings, leading to the loss of quantum information before the computation is finished. Therefore, complex quantum error correction schemes are being developed. This task is all the more difficult because quantum information cannot be copied. Consequently, a logical qubit that is fault-tolerant is being introduced and can consist of tens to thousands of physical qubits. Hundreds and thousands of logical qubits will be needed for practical quantum computations. For example, about 6,000 logical or 20 million physical qubits are needed to break RSA-2048 encryption (13). Currently, the best universal quantum processor has 127 physical (superconducting) qubits (14), and several companies (such as PsiQuantum, IBM, and Google) claim they will have a million physical qubits in 2030.

From a military and security perspective, one imminent application of quantum computing will be in cyber operations, to break the present asymmetric encryptions (15). The so-called ‘Q-Day’—a day

when a quantum computer will be able to break RSA-2048 encryption—is expected to occur in 10 to 15 years (16). However, by that time, such an application of quantum computing will not pose much of a danger as other quantum-resistant encryption schemes (see Quantum Cryptography below) will be in use. The risk is present for current and near-future data; China, and perhaps other nations and actors, has employed the strategy of 'harvest now, decrypt later' (17), which refers to the current practice of gathering sensitive encrypted data that will be valuable in the years to come, and waiting to address their decryption when the necessary quantum computer is available. Such data includes intelligence data, trade secrets, biometric identification markers, social security numbers, criminal records, weapon designs, and research and development around pharmaceuticals, biology, materials science and chemistry.

Other military applications will include quantum-enhanced machine learning for intelligence, surveillance and reconnaissance (ISR), and situational awareness, faster and better wargame simulations (leading to better decision-making), optimisation of military logistics and supply chains for missions, and enhanced analysis of radio-frequency spectrum, among others (18). Simply put, one can imagine using quantum computers for most computationally complex and slow tasks. It is also important to note that the deployment of quantum computers will not be immediate or surprising; their deployment and use will gradually increase with their increased capabilities.

- Quantum networks and communication aim to transmit quantum information (qubits) via numerous technologies across various channels, such as the optical fibres of free-space communication. A quantum network in its first generation is used practically only for quantum key distribution (QKD). QKD is a method of mitigating the threat posed by quantum computers through the distribution of cryptographical keys via quantum networks. The significant advantage of QKD is that an interception or eavesdropping attempt would be noticed immediately. QKD is commercially available for use with optical fibres, and many commercial free-space QKD services should be launched in the following two to five years. QKD is often described as being unhackable. However, this is only true for properly implemented quantum information transmissions. The endpoints, controlled by classical computers, can be considered the main target of future offensive cyber operations.

The next-generation quantum network, called quantum information networks (QIN) or quantum internet (19), differs in its ability to distribute entangled qubits. QIN will offer more services, also related to security, such as secure identification, position verification and distributed quantum computing. Significant technical applications will also be in high-precision clock synchronisation or networked quantum sensors (20). On the other hand, the biggest obstacle in this area of quantum technology is the absence of reliable quantum memory to store quantum information for synchronisation and distribution across the network with many intermediated nodes.

- Quantum cryptography is a term representing the methods of mitigating quantum computing threats (21). Apart from the QKD mentioned above, the other methods are based on post-quantum cryptography (PQC). PQC does not involve quantum physics. It is a classical technology and relies on mathematical problems that are highly difficult to compute, even for quantum computers. As such, PQC can be imagined simply as software/hardware updates, though usually more computationally demanding. However, in principle, it can never be proven that PQC is completely secure, and new classical or quantum attacks can appear.

The military applications here are evident (22). Today's battlefield depends heavily on communication, which is also often the target of enemy actions. In this sense, both quantum networks and cryptography offer a new, secure method of communication with a smaller chance of interference, jamming or eavesdropping. Moreover, additional QIN security protocols can improve communication security far beyond just QKD. Precise clock synchronisation will also be important. Quantum or optical clocks are so precise that the present method of clock synchronisation is insufficient. More precise timing is crucial for the quantum sensing applications described below as well as the new generation of satellite navigation systems, such as GPS, and various military applications, such as in electronic warfare or radars.

- Quantum sensing aims for the more precise measurements of various physical variables such as magnetic or electric fields, gravity gradients, acceleration rotations and time. This can be used for more precise clocks (used by many current technologies), quantum inertial navigation, underground and undersea exploration, more effective radio frequency communication receiving, etc. Quantum sensors use various quantum-mechanical principles and are associated with the greatest uncertainty in terms of how well they will work when deployed. For example, quantum magnetometry measures magnetic fields with high sensitivity, which can be used for detecting local magnetic anomalies or weak biological magnetic signals (e.g. for magnetoencephalography). In general, quantum sensors are the most developed among the various quantum technologies. However, military applications will require a portable or mobile solution with low SWaP (size, weight and power). At the same time, quantum sensors need to improve spatial resolution, as it is often anticorrelated with sensitivity. This means that detecting a submarine from space using a quantum sensor is rather unlikely. On the other hand, some quantum sensors are expected to be tested in the relevant environment in the next two to five years.

The military applications of quantum sensing can be seen in many areas, for example, quantum inertial navigation for submarines and ships, and later for spaceships and airborne vehicles; submarine and mine detection; underground structure mapping; wideband radio-frequency (RF) receivers; chemical detectors; precise time measurement that can also improve present radar, electronic warfare, and navigation systems; and Earth magnetic anomalies and gravity mapping for augmented navigation (23).

- Quantum imaging is a subfield of quantum optics that is, in comparison to quantum sensors, active in terms of some signal being emitted, with its reflection needing to be detected. However, using quantum entanglement, a significantly higher signal-to-noise ratio can be reached, so the signal itself may be unrecognisable in the background noise without additional knowledge on entanglement. Quantum imaging can provide technology such as quantum radars, 3D cameras, around-the-corner cameras, gas leakage cameras, and low-visibility vision devices. All these technologies would have direct applications in the military. However, quantum radar in the microwave regime is currently considered as unfeasible (24).

Many countries invest in quantum research and many have a national quantum strategy or plan (25). Currently, the US is the leader in quantum computing, while China is ahead in quantum communication. The UK, EU, Australia, Israel, Canada, India, and Japan are also strong in quantum research and development. China's investment in quantum technology accounts for about 50 percent of global quantum technology funding (26), and its primary motivation is the dual-use nature of quantum

technology. Similarly, military-oriented quantum activities can be seen in the US (27), Australia (28), India (29), and Israel (30).

Military Quantum Technology from Different Perspectives

There are many factors of uncertainty when attempting to predict the military applications of quantum technologies. Nevertheless, the basic possible applications can be projected, which allow for the military deployment of quantum technology to be seen from different perspectives.

Quantum enhancement

From this perspective, quantum technology can be seen as just a simple improvement of the present technologies, for example, to have better range and sensitivity (quantum magnetometry), better security (PQC), better pattern resolution by quantum-enhanced machine learning, or better (faster and cheaper) logistic optimisation. Especially in the case of quantum sensing, it can be simply imagined as the replacement of a classical sensor with a quantum one. From this perspective, it does not matter that the technology is quantum; what matters is that it provides better performance, such as a better signal-to-noise ratio, higher sensitivity or resolution, more effective data processing, or preserving data security.

New capabilities

Another perspective considers the new capabilities that are unreachable with current technology. These quantum technologies are due to come alongside current technologies and provide new possibilities, such as asymmetric encryption breaking, wideband RF sensing with a fixed-size small quantum antenna, exponentially faster linear equation solving relevant for many simulations, non-eavesdropping communication or unprecedentedly precise inertial navigation. However, whether the final product will meet expectations is highly uncertain, even more so for military applications than civil use.

Combination of technologies

The next question may be how much advantage we can gain by combining several technologies together. From this perspective, one line of thinking is the combination of several quantum technologies, i.e. combining two or more quantum technologies. For instance, imagine a quantum-enhanced drone that will have several quantum sensors, such as an RF receiver, magnetometer, chemical detector on board, with its GPS navigation backed up by quantum inertial navigation and its communication secured by the QKD. Such a combination of quantum systems within one platform can greatly increase the disruptive potential.

Another line of thinking is the combination of quantum technologies with other emerging and disruptive technologies, as the fusion of quantum technologies and machine learning/artificial intelligence (ML/AI) is progressing daily (for instance, no Barren plateaus in quantum neural networks (31), exponential speedup of quantum ML (32), or quantum ML will need less training data (33)). For example, ML/AI for better understanding and interpretation of quantum sensor data is under development (34). This will further improve the efficiency of quantum sensing and, consequently, its uses for military

applications. Furthermore, ML/AI can help overcome the imperfections of the first generation of quantum technologies, making them more useful from the start (35). Another example could be future autonomous vehicles combining classical and quantum sensors and classical AI with quantum neural networks or hypersonic weapons using quantum inertial navigation and quantum sensing, etc.

Abuse and misuse of quantum technologies

The next line of research will focus on the possible abuse and misuse of quantum technologies. Presently, the most assessed topic is that of quantum crypto analytical capabilities and how to mitigate the threat. But other questions arise: What if a malevolent actor takes full control of end nodes in a quantum network? What could they do and what would be the consequences? When low-cost quantum technologies are available, could non-state actors use them? If so, how? As quantum technology matures, these and many other similar questions will need to be answered.

In this research, only known technologies have been considered, even if only in theoretical terms. New quantum technologies or their new applications can still emerge. For example, a new quantum computing feature can lead to the emergence of new and surprising quantum algorithms with near-exponential speedup that will exploit, for example, a hidden structure in some symmetric encryption.

Quantum Technology in Future Warfare

Quantum technologies can significantly improve situational awareness, ISR or, more generally, the whole domain of C4ISTAR (command, control, communications, computing, intelligence, surveillance, target acquisition, and reconnaissance). In these areas, quantum sensing and quantum imaging will gather additional data, quantum communication will secure these data and achieve better precision and quantum computing, together with classical computing, will process all these data from quantum and classical sensing and provide situational awareness for more effective command and control. However, quantum-enhanced updates of ISR or C4ISTAR will be gradual. It can be expected that the first impact on warfare domains will be from quantum sensing and imaging, then from quantum communications and, finally, from quantum computing, which will need the most time to scale up to be useful.

Many discussions pertain to the future of the cybernetic domain and quantum computing, mainly in regard to the crypto analytical capabilities or quantum-enhanced ML/AI for automated cyber operations. However, this is only relevant in the approaching next decade, (2030 onwards). In the meantime, the cyber domain can significantly evolve only by classical ML/AI and edge computing. The current relevant topic in the cyber domain is the replacement of asymmetric encryptions that will not be secure with quantum computers in the future. It should be seen as an urgent need (36) as well as an opportunity to implement new, stronger security schemes. Nevertheless, there is also a risk of implementing new bugs and loopholes that will be exploited in the future.

Quantum technologies will also affect other existing warfare domains. For example, if quantum magnetometers prove to be much more powerful than the current classical ones, they could significantly modify anti-submarine warfare, and new technology, tactics and strategy will need to be employed to react to this new capability enabled by quantum sensors. Such a consideration can be

applied to many other warfare domains. Another example could be the future extensive integration of quantum inertial navigation into missiles, making electronic warfare acting against GPS-, radar-, or infra-navigated missiles obsolete. Such a situation will require the employment of new anti-missile capabilities and technologies. Similarly, quantum technologies can also have a significant role in the space ecosystem (37).

In connection with quantum technologies, new areas will emerge, such as quantum electronic warfare, where new countermeasures against quantum communications and imaging systems will need to be developed.

Conclusion

Quantum technologies exploit quantum mechanics to provide better sensing, safer communication, and faster computation. They are typical dual-use technologies with high potential for military and security applications. It is important to highlight the great uncertainty of whether all proposed quantum technology military applications will mature and meet higher military requirements, which is also connected with a significant general hype around quantum technologies, especially quantum computing.

Although quantum computers are highly discussed, realistically, they are, at best, over 10 years away from being in use. On the other hand, some quantum sensors and imaging systems can be expected to be deployed for military testing purposes in the next two or so years. Moreover, in many cases, the first generation of quantum sensing can provide similar or only slightly better performance than the best present classical sensors, but performance can also be expected to improve with each generation. Also, quantum networks and communication can be expected to be operational before 2030. In principle, post-quantum encryption should be the first to be deployed now. A few big services like OpenSSH (38) have even begun to implement it.

To prevent unpleasant surprises, we need to build awareness of quantum technology and study their direct and indirect consequences, which could have even deeper implications. Quantum technologies could also have a huge impact on society itself (39) and, consequently, on the security aspects of society that can create changes in international security (40).

Endnotes

(1) NATO, *Emerging and Disruptive Technologies*, NATO, 18 June 2021, http://www.nato.int/cps/en/natohq/topics_184303.htm

(2) European Commission, *Horizon Europe - Work Programme 2021-2022 - 7. Digital, Industry and Space*, 23 August 2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-7-digital-industry-and-space_horizon-2021-2022_en.pdf

(3) Elsa Kania and John Costello, 'Quantum Leap (Part 1): China's Advances in Quantum Information Science', *China Brief* 16, no. 18 (5 December 2016), https://jamestown.org/program/quantum-leap-part-1-chinas-advances-quantum-information-science-elsa-kania-john-costello/; Elsa Kania and John Costello, 'Quantum Leap (Part 2): The Strategic Implications of Quantum Technologies', *China Brief* 16, no. 19 (21 December 2016),the subsequent article will evaluate the military and strategic implications of quantum technologies. In August 2016, the launch of the world's first quantum …","container-title":"The Jamestown Foundation China Brief","issue":"18","language":"en-US","title":"Quantum Leap (Part 1 https://jamestown.org/program/quantum-leap-part-2-strategic-implications-quantum-technologies/

(4) Peter Cooper et al., *Quantum Computing Just Might Save the Planet*, McKinsey & Company, May 2022, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-just-might-save-the-planet

(5) In classical information science, the elementary carrier of information is a bit that can be only 0 or 1. The quantum information elementary carrier of information is the quantum bit, qubit in short. A qubit can be or , or an arbitrary complex linear combination of states and called the *quantum superposition*. This feature is responsible, e.g., for up to exponential speed up in quantum computing.

(6) *Quantum entanglement* refers to a strong correlation between two or more qubits (or two or more quantum systems in general) with no classical analogue. Quantum entanglement is responsible for many quantum surprises.

(7) The *no-cloning theorem* says that quantum information (qubit) cannot be copied. This theorem has profound consequences for qubit error correction as well as for quantum communication security.

(8) Michal Krelina, 'Quantum Technology for Military Applications', *EPJ Quantum Technology* 8, no. 1 (2021): 1–53; D.F. Reding and J. Eaton, *Science & Technology Trends 2020-2040*, NATO Science & Technology Organization, 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf The Australian Army, *Army Quantum Technology Roadmap*, April 2021, https://researchcentre.army.gov.au/sites/default/files/RD5734_Quantum%20Roadmap%20WEB.pdf

(9) Krelina, 'Quantum Technology for Military Applications'; Andrew Davies and Patrick Kennedy, 'From Little Things: Quantum Technologies and Their Application to Defence', *ASPI Special report*, November 2017; Stuart A. Wolf et al., *Overview of the Status of Quantum Science and Technology and Recommendations for the DoD*, The Institute for Defense Analyses, 2019, https://apps.dtic.mil/sti/pdfs/AD1098553.pdf; Kelley M Sayler, *Defense Primer: Quantum Technology*, Congressional Research Service, 24 May 2021, https://crsreports.congress.gov/product/pdf/IF/IF11836

(10) Olivier Ezratty, 'Understanding Quantum Technologies', *ArXiv:2111.15352 [Quant-Ph]*, 2021.

(11) NP is a complexity class characterised by the fact that it cannot be solved in polynomial time but can be verified in polynomial time. Specifically, the NP-hard problems are not only hard to solve but are difficult to verify as well. Examples of NP-hard problems are the Travelling Salesman problem and Graph Colouring problems.

(12) Emily Grumbling and Mark Horowitz, *Quantum Computing: Progress and Prospects*, US National Academy of Sciences, 2018.

(13) Craig Gidney and Martin Ekerå, 'How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits', *Quantum* 5 (2021): 433.

(14) IBM, 'IBM Unveils Breakthrough 127-Qubit Quantum Processor', *IBM Newsroom*, 16 November 2021, https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor

(15) Public-key cryptography or asymmetric cryptography uses a scheme (e.g. RSA) with a pair of keys: a public and a private key. The public key can then be used for encrypting a message that can be decrypted only by the private key. The public key can be distributed openly because classical computers are not able to obtain the private key from the public one within a reasonable timeframe. However, this is not true for several asymmetric cryptographical schemes in the case of quantum computing.

(16) Michele Mosca and Marco Piani, *Quantum Threat Timeline Report 2020*, Global Risk Institute, January 2021, https://globalriskinstitute.org/download/quantum-threat-timeline-report-2020/

(17) Booz Allen Hamilton, *Chinese Threats in the Quantum Era*, November 2021, https://www.boozallen.com/expertise/analytics/quantum-computing/chinese-cyber-threats-in-the-quantum-era.html

(18) Krelina, 'Quantum Technology for Military Applications'; ATARC, *Applied Quantum Computing for Today's Military*, Advanced Technology Academic Research Center, 2021, https://atarc.org/wp-content/uploads/2021/05/ATARC-Military-Paper-by-Quantum-Working-Group.pdf

(19) Stephanie Wehner, David Elkouss, and Ronald Hanson, 'Quantum Internet: A Vision for the Road Ahead', *Science* 362, no. 6412 (2018).it still has many shortcomings, not least of which is that communication can be intercepted and information stolen. If, however, the internet attained the capability of transmitting quantum information—qubits—many of these security concerns would be addressed. Wehner et al. review what it will take to achieve this so-called quantum internet and propose stages of development that each correspond to increasingly powerful applications. Although a full-blown quantum internet, with functional quantum computers as nodes connected through quantum communication channels, is still some ways away, the first long-range quantum networks are already being planned.\nScience, this issue p. eaam9288\nStructured Abstract\nBACKGROUNDThe internet has had a revolutionary impact on our world. The vision of a quantum internet is to provide fundamentally new internet technology by enabling quantum communication between any two points on Earth. Such a quantum internet will—in synergy with the "classical" internet that we have today—connect quantum information processors in order to achieve unparalleled capabilities that are provably impossible by using only classical information.As with any radically new technology, it is hard to predict all uses of the future quantum internet. However, several major applications have already been identified, including secure communication, clock synchronization, extending the baseline of telescopes, secure identification, achieving efficient agreement on distributed data, exponential savings in communication, quantum sensor networks, as well as secure access to remote quantum computers in the cloud.Central to all these applications is the ability of a quantum internet to transmit quantum bits (qubits

(20) Krelina, 'Quantum Technology for Military Applications'.

(21) Prachi Mishra, 'Cybersecurity in the Quantum Age', *ORF Digital Frontiers*, 28 March 2022, https://www.orfonline.org/expert-speak/cybersecurity-in-the-quantum-age/

(22) Krelina, 'Quantum Technology for Military Applications'.

(23) Krelina.

(24) F. Daum, 'Quantum Radar Cost and Practical Issues', *IEEE Aerospace and Electronic Systems Magazine* 35, no. 11 (2020): 8–20.

(25) McKinsey & Company, *The Quantum Technology Monitor - September 2021*, September 2021, https://www.mckinsey.de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2021/2021-09-22%20quantum%20technology%20monitor/mckinsey_quantum_technology_monitor_2021_vf.pdf

(26) McKinsey & Company.

(27) Wolf et al., 'Overview of the Status of Quantum Science and Technology and Recommendations for the DoD'; DARPA, 'Quantum Sensing and Computing', 2020, https://www.darpa.mil/attachments/QuantumSensingLayout2.pdf

(28) The Australian Army, 'Army Quantum Technology Roadmap'.

(29) Arjun Gargeyas, 'With Eye on China, India Joins Race To Weaponise Quantum Tech in Future Military Conflicts', *News18*, 28 February 2022, https://www.news18.com/news/opinion/eye-on-china-india-joins-race-to-weaponise-quantum-technology-in-military-conflicts-4818032.html

(30) Yonah J. Bob, 'Will Israel Build Its First Quantum Computer?', *The Jerusalem Post*, 15 February 2022, https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-696554

(31) Arthur Pesah et al., 'Absence of Barren Plateaus in Quantum Convolutional Neural Networks', *Physical Review X* 11, no. 4 (2021): 041011.known as barren plateau landscapes, for many QNN architectures. Recently, quantum convolutional neural networks (QCNNs

(32) Hsin-Yuan Huang et al., 'Quantum Advantage in Learning from Experiments', *Science* 376, no. 6598 (2022): 1182–86.

(33) Matthias C. Caro et al., 'Generalization in Quantum Machine Learning from Few Training Data', *Nature Communications* 13, no. 1 (2022): 4919.{\\i{}Nature Communications} 13, no. 1 (22 August 2022

(34) Dough Finke, 'SandboxAQ's Product Strategies', *Quantum Computing Report* (blog), 26 March 2022, https://quantumcomputingreport.com/sandboxaqs-product-strategies/

(35) Q-Ctrl, 'Q-CTRL Leverages Quantum Control to Improve Quantum Sensor Performance', Q-CTRL, 9 June 2021, https://q-ctrl.com/blog/q-ctrl-leverages-quantum-control-to-improve-quantum-sensor-performance/

(36) Davide Castelvecchi, 'The Race to Save the Internet from Quantum Hackers', *Nature* 602, no. 7896 (2022): 198–201.

(37) Michal Krelina, 'The Prospect of Quantum Technologies in Space for Defence, Security, and Sustainable Presence', *In Preparation*, 2022.

(38) Duncan Jones, 'OpenSSH Bravely Addresses the Quantum Threat', *Cambridge Quantum* (blog), 11 April 2022, https://medium.com/cambridge-quantum-computing/openssh-bravely-addresses-the-quantum-threat-86b03e38c2ba

(39) Pieter E. Vermaas, 'The Societal Impact of the Emerging Quantum Technologies: A Renewed Urgency to Make Quantum Theory Understandable', *Ethics and Information Technology* 19, no. 4 (2017): 241–46; Ronald de Wolf, 'The Potential Impact of Quantum Computers on Society', *Ethics and Information Technology* 19, no. 4 (2017): 271–76.

(40) Michal Krelina and Jürgen Altmann, 'Quantum Technologies – a New Field That Needs Assessment', *Accepted to Die Friedenswarte / Journal of International Peace and Organization (JIPO)*, 2022.

Gene Editing and the Need to Reevaluate Bioweapons

Shambhavi Naik

Genetic material provides the fundamental building blocks for most physical characteristics. The colour of our eyes, the length of a grain of rice, the horns of the cattle are all governed by genes. Recently, the importance of genes in influencing the infectivity of pathogens has been highlighted by the rapid spread of Sars-CoV-2, the infectious agent causing COVID-19. Sars-CoV-2 differs from other coronaviruses in a few genetic regions, conferring on it the ability to interact strongly with the human ACE2 receptor (1). This strong interaction, among other factors, has facilitated the rapid spread of COVID-19 worldwide. Further changes in the genetic material of emerging variants have led to subsequent waves of COVID-19 (2). Conversely, the study of Sars-CoV-2 genes have resulted in rapid diagnostic kits and created avenues to engineer successful vaccines that could target its infection.

The role of genes in our daily life does not need any emphasis. Techniques such as polymerase chain reaction, cloning, Sanger sequencing, and next-generation sequencing have provided the ability to read, edit, and synthesise genetic material. Using these techniques, we can unravel genes' functions in health and disease. For instance, we can now conclusively demonstrate that certain mutations can increase cancer risk or cause congenital diseases such as thalassemia. By understanding the interactions of proteins that genes encode, we can create vaccines against infectious diseases. Using computational biology, we can predict potential mutations in new variants and be prepared with vaccines before the variants manifest. Scientists use gene editing technologies such as Zinc Finger Nucleases and Transcription Activator-Like Effector Nucleases to edit genes and study their impact on microorganisms. Newer technologies, such as Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR), have extended this capacity to edit human cells with unprecedented precision.

The last few decades have conferred onto humans the tremendous power of altering the very fundamental blocks of biology. This power can be used for alleviating disease, but similarly can also be used to design newer biological weapons, leading to new diseases. COVID-19 has shown the devastation—of

life and economy—that new diseases, whatever their origin, can cause. In addition, COVID-19 has also demonstrated the weak nature of key multinational agencies, such as the World Health Organization (WHO), in quickly responding to an emerging threat. In this backdrop, the current turmoil in international relations and political instability across various countries have created a stage that could facilitate the deployment of bioweapons. This combined biotechnological progress and fragile political systems warrant a serious study of bioweapons, how they may be potentially used, and how India can protect against this emerging threat.

New-Age Biowarfare: Setting the Stage

The conversation around biowarfare has thus far mostly been limited to the use of biological weapons as a weapon of mass destruction. In this context, bioweapons are banned by the Biological Weapons Convention (BWC), a multilateral arms control measure in force since 1975 (3). The fear of bioweapons stems from the resulting uncontrolled spread of disease, unlike the relatively more limited fallouts of other weapons. State actors, including the US, that once experimented with creating bioweapons, are wary of a rival stealing these technologies. This fear was so apparent that, in a first in the arms control and disarmament sphere, countries agreed to disband their existing bioweapons programme and destroy any stockpiles. While the treaty can be said to be a major victory for international diplomacy, the lack of a verification mechanism means that there is no real way to check if all signatory countries continue to adhere to its provisions (4). Further, even the investigation of a potential bioweapon attack can only be started upon a country's request and routed through the United Nations Security Council, rendering the BWC toothless. However, the lack of any major incident involving bioweapons has lulled the international community into ignoring the bioweapons threat and the weaknesses in the BWC. Despite serious attempts, including a verification mechanism within the BWC, it has failed. Unlike the Chemicals Weapons Convention (CWC), the BWC lacks a scientific board that can advise it on emerging technologies that could impact bioweapons. Even more importantly, the BWC is poorly funded, with the implementation support unit only having three employees as compared with the CWC's 500 or so employees (5), (6). While the lack of use of bioweapons in the interim is promising, it is important to remember that new-age bioweapons may overcome some of the challenges associated with acquiring and using traditional bioweapons.

Indeed, since the treaty was signed in 1975, the nature of warfare and the technologies to engineer biological weapons have changed. New-age technologies are changing both the kind of biological weapons that can be used and the delivery mechanisms to deploy these. The use of biological weapons can be covert, with attribution to a particular source obscured by limits of scientific detection and political mechanisms. This may make biological weapons appealing to state or non-state actors interested in subverting a rival authority without necessarily having to engage in a full-blown military intervention. Thus, the theatres where biowarfare could be engaged may differ from the traditional battlefield.

In addition, bioweapons may confer the advantage of selective destruction of agriculture or animal livestock. A state or non-state actor who wishes to use biowarfare might not be interested in directly killing human populations. Instead, they may target agriculture or animal husbandry, leading to starvation, heavy economic losses, or the artificial creation of dependence on a provider country. Such selective destruction cannot be achieved using other means of warfare. The emergence of new diseases,

the changed patterns of predator movements and the unpredictable nature of agricultural outputs driven by climate change and globalisation can obfuscate any investigation of an unusual biological event. Thus, new-age bioweapons bred to cause economic devastation without directly hurting human populations are a category that needs to be assessed.

Moreover, new technologies are being developed to deliver gene editing components into humans for medical purposes. Delivery mechanisms, such as genetically modified viruses, do not cause any harm and carry medical payloads that can cause the necessary gene edits inside a human body. Such *in vivo* delivery mechanisms are envisioned to revolutionise medical therapy for diseases of genetic origin, such as certain cancers, thalassemia, and haemophilia. However, these same medical tools could also be used to carry malicious payloads. These mechanisms could, in effect, ease delivery, which remains one of the major challenges of deploying bioweapons. As the technologies improve—which they will and must for medical purposes—we will see further simplification of the delivery of gene editing components.

Finally, the experience with COVID-19 has demonstrated the difficulties in identifying the origins of novel diseases. Notwithstanding the nature of the virus' origin, the first WHO investigation into the origin happened only after the World Health Assembly passed a motion in May 2020. Subsequent investigations by various institutions have come under criticism for the conflict of interests of the investigators (7). The controversies fuelled by these delayed and opaque investigations on social media has led to the spread of further misinformation. The fallout of the political games surrounding the scientific investigation is that we are no closer to understanding the virus's origin and identifying ways to prevent a pandemic of this scale from breaking out again.

Thus, the advantages of using novel technologies such as gene editing coupled with the quagmire created by weak multinational institutions means that a cleverly designed bioweapons attack may never be identified. On a global stage, where war-related state actions are often met with economic sanctions or other consequences, biowarfare may provide an interesting avenue to even state actors, who seem to have been averse to their use. Below are some new approaches in which bioweapons might be used.

Targeting individuals for attack

The use of bioweapons for personal attacks is not novel. The 1978 assassination of Bulgarian dissident Georgi Markov using a ricin pellet fired from an umbrella brought attention to the use of this biotoxin (8). In 2020, letters containing Ricin were sent to the US White House and various law enforcement agencies in Texas (9). Ricin has also been recovered from individuals in Indonesia and Germany. Ricin, which is banned under both the BWC and CWC, has been used for limited attacks but does not offer any avenue for personalisation. However, with new technologies and a better understanding of human biology, it may become possible to design new-age bioweapons that can be tailored for a specific human target.

The advances in sequencing technology have significantly reduced the cost of sequencing. The first human genome sequencing effort took 13 years (1990-2003) and cost about US$1 billion, but it currently costs anywhere between US$300 to US$1000, with prices expected to reduce further soon (10), (11). Further, the ability to sequence from smaller amounts of starting materials or ancient samples has also improved. Consequently, genetic sequencing for both medical and non-medical purposes has

mushroomed. Genetic sequencing can inform on health, risk of disease, and even ancestry of individuals. In research, genetic sequencing is useful in characterising genes and unravelling their functions.

As our knowledge of the human body improves, we may be able to target individual weaknesses in our biology. It may even become possible to target individuals using their genes (12). Getting deoxyribose nucleic acid (DNA) for sequencing genes is easy—DNA can be obtained from fingerprints, saliva or other bodily matter. Even building potential DNA sequences using DNA obtained from samples of close relatives is becoming possible. Finally, various countries, including India, are moving to create forensic and medical DNA databases, and private companies such as 23andMe and Ancestry.com are building databases that could act as repositories of DNA.

Given this context, tailored weapons to target individuals may become a convenient option for an interested State or non-State actor. For example, genome sequencing may reveal an individual has a higher risk of a particular disease. Then CRISPR-based tools may be created to cause further mutations to increase this risk or expedite disease causation. Such designer diseases may remain untraceable and may be treated as normal disease progression, allowing the perpetrating party to remain anonymous.

Targeting population subgroups

Building on the premise of tailored weapons, it is likely that weapons meant to target particular population subgroups based on ethnicity may be designed. Ethnic groups, particularly those that practice endogamy, may carry common genetic signatures. These signatures can be used as a targeting mechanism for bioweapons. A hypothetical scenario can be as follows: a delivery vector, such as a virus, is created to deliver a lethal genetic payload. The switch to turn on the transcription of this payload is engineered to respond to the unique signature present in the ethnic group. A more plausible scenario is the development of new diseases that can be used to target populations while the perpetrator develops vaccines or antidotes to protect their forces and people.

Targeting agriculture

Agriculture is an easy target for bioweapons, with the ripple effect likely to be felt worldwide. Over the past few decades, changes in predator patterns have been observed. In 2020, for example, swarms of desert locusts damaged crops across multiple states in India. Some of these regions have not seen locusts' swarms since the 1970s. Such changes are to be expected and can be attributed to climate change (13). However, the obscurity provided by climate change can also cloak any deliberate effort at sabotaging agriculture.

The US Defense Advanced Research Projections Agency runs a programme called 'Insect Allies' to use insects to deliver genetically-modified viruses to plantations. These viruses will then genetically modify the target plants. This programme aims to respond to any emerging threats to agricultural produce quickly. As noble as that goal is, any technology developed to deliver beneficial payloads can be usurped to deliver harmful payloads. Questions have been raised about the relative utility of this programme, and it remains to be seen how scientists can ensure that the system is not misused (14).

Similarly, scientists are also working on a molecular technique called 'gene drives'. Gene drives is a system that circumvents the natural method of an offspring inheriting genes from either parent through a random choice. Gene drives introduce a new gene in insects, which is always inherited by the offspring and future generations. Such systems are being developed to combat vector-borne diseases such as malaria and dengue. However, this system could also be used to deliver a toxin or pathogens to a target population, sparking fears of it becoming a tool for biowarfare (15).

Should These Technologies be Banned?

Emerging technologies based on natural processes such as CRISPR and gene drives give humans unprecedented control over our genetic foundations. There is no point denying that this control could be used to achieve malicious outcomes. However, there are tremendous benefits to allowing these technologies to blossom. The lowest hanging fruit is the alleviation of human disease and suffering, particularly those diseases of genetic origin. Other benefits include improvement of agricultural outputs, conservation of endangered species and increased human productivity. The risk of bioweapon engineering is relatively low compared to the thousands of laboratories involved in performing research on the beneficial applications of gene editing. Hence, the spread of these technologies needs to be promoted so that their beneficial applications continue to prosper. Though these technologies are becoming rapidly available, there is still expertise and infrastructure requirements for successfully building a bioweapon using gene editing. At the same time, these technologies need to be regulated to prevent their use for malicious purposes.

What India Can do to Improve Biosecurity

Over the past decades, multiple disease outbreaks have happened in India's neighbourhood. The second COVID-19 wave demonstrated how ill-prepared India's health system is to face an emerging disease.

A national policy governing supply chains of biological products, access to biological reagents, and ethical training of researchers would help promote biosafety and legitimate uses of emerging technologies. This can prevent laboratory accidents and leakages of biological material that could be used as a basis to create biological weapons. However, if a biosecurity risk is comprehended, its origin as a bioweapon or a natural occurrence is a secondary question. The primary challenge is to detect the threat early and limit its spread. In this context, India needs to take four steps to prevent and prepare for a possible biosecurity risk.

Set up a biosecurity threat identification system

There is a need to set up a surveillance hub to identify emerging threats to India's biosecurity (16). This hub can support India's intelligence agencies and work with the appropriate ministries to ensure the country is prepared to tackle any risks or threats. The surveillance hub should incorporate digital monitoring systems to monitor digital content related to biological events. This information would be analysed by a team of agricultural experts, public health professionals, statisticians, epidemiologists,

and analysts trained in strategic studies. Finally, trained officers could acquire field samples for further analysis if required. Such a system would be essential for India to remain ahead of emerging threats.

Universal healthcare

Any threat to human biosecurity can be encountered with a robust healthcare system. This includes access to primary healthcare, testing facilities, and research on designing new vaccines and medicines. All biosecurity threats—whether a bioweapon or natural pathogen—qualify as a threat if they can cause serious damage to human life. A responsive healthcare system, geared to detect, respond, and communicate on health threats, would reduce the threat to India.

Renegotiating BWC

COVID-19 has shown that biosecurity cannot be the concern of any one nation. Similarly, India cannot tackle bioweapons on its own. Hence, it needs to take a leadership position at the BWC and negotiate a treaty more appropriate for the new technologies (17). The BWC immediately requires substantial funding sources and a scientific board capable of advising the Convention on emerging threats. The board could also prescribe a common minimum programme for biosafety policies and healthcare responses. The Convention should create a threat matrix for emerging technological applications and pathogens and design proportionate evasive measures. Further, the Convention should consider actively monitoring unusual disease patterns and maintain a database of evolving pathogen genetics.

Funding more gene editing research

While this may seem counterintuitive, the best biodefence against an engineered pathogen may be understanding its pathogenicity and designing vaccines or therapies. Gene editing may play a critical role in both characterising the pathogen quickly and even creating therapies. However, for this to happen, India needs to actively fund gene editing research so that the expertise and infrastructure are available locally. For example, if a new plant pathogen is destroying rice plants, gene editing may be able to deliver an antidote to protect the plants quickly.

Conclusion

Bioweapons have long been considered uncontrollable weapons of mass destruction, leading to them being shunned by the international community. However, new technologies and a fragile international political scenario have created a situation where targetable bioweapons may be created and used without attribution. This situation warrants a revisit of the BWC and how the world views bioweapons. Stricter regulation, global cooperation, and better healthcare and agricultural practices are a must to prevent any untoward event.

Endnotes

(1) Ana Sandoiu, "Why does SARS-CoV-2 spread so easily?," *Medical News Today*, March 17, 2020, https://www.medicalnewstoday.com/articles/why-does-sars-cov-2-spread-so-easily#Key-receptor-on-human-cells

(2) Rehan M El-Shabasy et al., "Three waves changes, new variant strains, and vaccination effect against COVID-19 pandemic," *International Journal of Biological Macromolecules*, 204 (2022):161-168 https://pubmed.ncbi.nlm.nih.gov/35074332/

(3) Arms Control Association, "The Biological Weapons Convention (BWC) At A Glance," https://www.armscontrol.org/factsheets/bwc

(4) Jonathan B. Tucker, "Putting Teeth in the Biological Weapons Convention," *Issues in Science and Technology*, XVIII(2002):3 https://issues.org/tucker/.

(5) Annual Report of the Implementation Support Unit, Meeting of the States Parties to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, 2019, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/300/74/PDF/G1930074.pdf?OpenElement

(6) Arms Control Association, "The Chemical Weapons Convention (CWC) At A Glance," https://www.armscontrol.org/factsheets/cwcglance

(7) Paul D. Thacker, "Covid-19: *Lancet* investigation into origin of pandemic shuts down over bias risk," *BMJ*, 375(2021), https://www.bmj.com/content/375/bmj.n2414

(8) Christopher Nehring. "Umbrella or pen? The murder of Georgi Markov. New facts and old questions". *Journal of Intelligence History*, 16(2017):1, 47-58, https://tandfonline.com/action/showCitFormats?doi=10.1080%2F16161262.2016.125824.

(9) Katie Benner, "Ricin Is Said to Have Been Sent to White House," *New York Times*, September 19, 2020, https://www.nytimes.com/2020/09/19/us/politics/ricin-white-house-postal-service.html.

(10) GlobalData Healthcare, "Personalised medicine set to surge as gene sequencing costs fall," Pharmaceutical Technology, November 30, 2018, https://www.pharmaceutical-technology.com/comment/genome-sequencing-price-drop/

(11) Brandon Colby, "Whole Genome Sequencing Cost," Sequencing Education Center, Sequencing Outsmart Your Genes®, https://sequencing.com/education-center/whole-genome-sequencing/whole-genome-sequencing-cost

(12) John Sotos, "There are things worse than death': can a cancer cure lead to brutal bioweapons?" *The Guardian*, July 31, 2017, https://www.theguardian.com/science/2017/jul/31/bioweapons-cancer-moonshot-gene-editing

(13) Kabir Agarwal and Shruti Jain, "Climate Change Brings the Worst Locust Attack in Decades to India," *Science The Wire*, May 27, 2020, https://science.thewire.in/environment/locust-attack-india-jaipur-climate-change/

(14) RG Reeves et al., "Agricultural research, or a new bioweapon system?," *Science*, 362(2018):6410, 35-37, https://science.sciencemag.org/content/362/6410/35.summary.

(15) Sharon Begley, "Why the FBI and Pentagon are afraid of this new genetic technology" *STAT*, November 12, 2015, https://www.statnews.com/2015/11/12/gene-drive-bioterror-risk/#:~:text=The%20possibilities%20for%20%E2%80%9Cweaponizing%E2%80%9D%20gene,who%20briefed%20the%20bioweapons%20office

(16) Shambhavi Naik and Ruturaj Gowaikar, "A National Epidemic Service for India," Takshashila Institution, 2022, https://takshashila.org.in/research/takshashila-discussion-document-a-national-epidemic-intelligence-service-for-india No 2): Bioweapons Peril,"osafet(2017)cromolecules, ay impinge on tradesecrets. e regulation of supply chain, policy on biosafet

(17) Shambhavi Naik and Aditya Ramanathan, "The New Bioweapons Peril," *Indian Public Policy Review*, 3(2022):1 https://ippr.in/index.php/ippr/article/view/94

War on the High Frontier

Malcolm Davis

The space domain is vital in the use of military force in the modern era. Its central role in supporting the use of force means that space is now seen as a contested operational domain, to which access must be gained and then sustained in the face of rising counterspace threats. Space warfare will involve a struggle for control of space between opposing forces. The ongoing development of counterspace capabilities, as noted in the Secure World Foundation's annual counterspace report, highlights on-going developments by Russia and China and demonstrated by the US in 2008 and India in 2019, suggests that space could quickly become a warfighting domain in any future major power crisis (1).

It is a common refrain within the strategic policy community to suggest that space is 'contested, congested and competitive', but it is an accurate perspective on this crucial environment that is essential to the conduct of modern joint and integrated military operations (2). Space is no longer seen as a sanctuary that sits serene and untouched by increasing terrestrial rivalries below, and the idea of war in space is no longer confined to the realms of science fiction. Space has never been a global common used for peaceful purposes only, despite the well-intentioned rhetoric promoted by diplomats. Space has certainly been militarised since the dawn of the space age in the 1960s, with early American and Soviet satellites providing intelligence, surveillance, and reconnaissance (ISR), satellite communications, and, most importantly, nuclear command, communications, and control, and missile early warning services (3). The modern equivalents of these early capabilities, such as the US space-based infrared system (SBIRs), remain essential to ensuring a stable nuclear balance and the continued efficacy of nuclear deterrence (4). The 1970s and 1980s saw the development of global navigation satellite systems as a new role for space systems, with the US global positioning system (GPS) as the leading example that has become vital for modern military operations and a wide range of services for civil use, including banking systems, supply chains, and financial trading (5).

The role of space continued to expand in the 1990s to support a broader range of military and civil tasks. For example, space capabilities were a key component of coalition military operations during the 1991 Gulf War, with GPS, intelligence collection satellites and sophisticated digital satellite communications enabling a range of new military technologies, including the provision of 'blue force tracker', as part of the networked command and control of coalition forces during Operations Desert

Storm and Desert Sabre. In the 21st Century, space capabilities will continue to expand in importance to enable networked multidomain operations and support new types of military capabilities, including ever-more sophisticated autonomous systems in the air, on land, and on and under the waves. For example, the positioning, navigation, and timing (PNT) services provided by global navigation satellite systems such as the GPS, Europe's Galileo, China's Beidou, and Russia's Glonass, are not just essential for navigation or the precision-targeting of weapons. The timing signals generated by such satellites are vital in network centric warfare. Advanced digital satellite communications allow for global military operations and long-range power projection, including the facilitation of more sophisticated autonomous systems (6). The control of armed unmanned autonomous vehicles, such as Predator and Reaper drones, over conflicts in Afghanistan were controlled from ground facilities in Nevada via sophisticated satellite systems such as the US Advanced Extremely High Frequency and Wideband Global Satcom, of which Australia controls one of 10 satellites in geosynchronous orbit (GEO).

The importance of space in warfare will only continue to grow, particularly as autonomous systems expand to become prolific over future battlespaces and a key component of the force structures of militaries. As western liberal democracies begin to acquire lethal autonomous weapons systems, the principles of *jus in bello*—that are the laws of war in terms of discrimination, proportionality, and necessary—and international humanitarian law in shaping rules of engagement when using autonomous systems to deliver lethal force will demand a human 'on the loop' to give broad oversight and direction to an autonomous system and, in some cases (such as with the delivery of lethal effect), 'in the loop' to allow direct control, or at the very least, authority to release a weapon. For operations in an Indo-Pacific context, where the likely range of operations is hemispheric in nature, satellite support will be essential.

Whilst there is an aspiration towards developing trusted autonomy for these systems, whereby the human remains on the loop, against a need for positive control depending on tactical and political requirements, western traditions of warfare make it more difficult to envisage circumstances whereby a human will be 'off the loop', with the autonomous system making its own choices about delivery of lethal effect. The reality of a 'western way of war' that is consistent with jus in bello, international humanitarian law, and the requirements of discrimination, necessity and proportionality in the delivery of lethal effect will demand access to resilient space capabilities for sustaining positive and survivable command and control through a network of space- and non-space-based ISR platforms and will demand assured access to PNT services. This makes space capabilities a potential Achilles heel for western military forces as they will increasingly rely on autonomous capabilities, if satellites can be attacked by their authoritarian peers who do not need to address such constraints in their use of force (7).

The role of space sensors for missile early warning has been a crucial component of nuclear deterrence and is now set to expand into non-nuclear operations. Already, key missile early warning satellites of the SBIRs constellation provides missile launch detection and tracking of even conventional ballistic missile systems to cue missile defence capabilities (8). That role is likely to dramatically expand as next generation overhead persistent infrared surveillance is developed to cover early warning and tracking of both ballistic missile-delivered hypersonic glide vehicles and scramjet-based hypersonic cruise missile systems operating within earth's atmosphere (9). The use of low-earth orbit (LEO) based sensors on satellites will be a crucial component of any defence against future hypersonic weapons (10).

The dependency of western terrestrial military forces on space support to undertake joint and integrated military operations means that the space domain could quickly become a warfighting domain prior to or at the outset of any future major power conflict. Adversaries recognize the crucial role that space plays in facilitating the projection of precision military effect at long range and battlespace awareness to deliver a 'knowledge edge' for the US and its allies. Adversaries could employ counterspace capabilities, in concert with offensive cyber and electronic warfare attacks, in what former US Secretary of Defense Donald Rumsfeld called a "space pearl harbour" in January 2001 (in what is referred to as the Rumsfeld Commission report), to deny access to vital space support, leaving the US and its allies effectively deaf, mute, and blind at the outset of any future conflict (11). In the over 20 years since the release of the Rumsfeld Commission report, the growing risk posed by adversary counterspace threats demands that the US and its allies consider the important task of 'space control'—ensuring access to resilient space capabilities even in the face of direct threats posed by adversary counterspace systems (12). This requirement for resilience and assured access demands greater use of distributed networks of small satellites that is supported by responsive space launch in a crisis.

In particular, the potential impact of reusable launch technologies—best epitomized by SpaceX's Falcon 9, Falcon Heavy and, in the future, Starship Super Heavy launch vehicles that offer fast, responsive, and low-cost launch for satellites—offers a potential disruptive effect on the economics of space operations as the cost of space launch falls, and the ability for regular access increases. New technologies have enabled reusable launch vehicles operating at considerably less cost than traditional expendable launch vehicles, or even partially reusable launch capabilities such as the Space Shuttle. Fully reusable launch vehicles like Starship Super Heavy may generate new approaches to accessing space and utilizing space for military purposes, but the trend towards falling launch cost is likely to continue in the coming decades. The potential for true single-stage-to-orbit reusable launch, based on hypersonic aerospace plane technologies, is on the horizon. In the coming decades, if realised, this technology could see space access operating in a manner akin to commercial air travel, and at dramatically lower cost per kilogram of payload to LEO.

For warfighting, such new technologies opens the potential for dramatically different ways to employ space power, by projecting military effect from earth into space, through space, and from space against the earth, in a manner much more rapidly than would be possible with traditional expendable multistage rockets (13). Speed, high operational tempo, and low-cost space access could transform thinking on the nature and application of space power, akin to the effect on airpower of the emergence of jet propulsion in the 1940s and 1950s. More broadly, it could expand potential horizons of civil and commercial purposes, especially if linked with the establishment of a space economy built on space resource utilisation on and around the Moon. With commercial activity comes the potential for competition in an environment that remains managed through regulatory structures that date back to the 1960s, and which were written for a different era in human space activities.

The importance of the space domain is driving greater attention towards space situational awareness, or what is now termed as space domain awareness (SDA). A combination of ground-based radar and optical sensors, combined with emerging space-based situational awareness capabilities, provides an ability to monitor potential counterspace threats, ensure attribution to any party employing such capabilities, take mitigating measures to defeat counterspace attacks, and manage the ever-growing challenge of space debris. Developing more comprehensive and pervasive SDA will be essential to

avoid an opponent using 'dual-role' technologies to undertake grey zone operations in orbit, in which a counterspace capability is masked as a commercial system, for on-orbit repair and refueling, or satellite inspection. Such a satellite could be employed covertly to undertake close-approach rendezvous and proximity operations (RPOs) against a target satellite to gather intelligence or undertake a hostile action as a co-orbital antisatellite weapon. By ensuring attribution of hostile or irresponsible actions in space, there is a greater possibility that diplomatic, political, and economic pressure can be applied to prevent or respond to the use of counterspace capabilities, either overtly or as part of a grey zone activity.

The growing risk posed by counterspace capabilities is generating a dual-track approach in most western states towards mitigating risks and reducing the potential for space to become a warfighting domain. These approaches involve international diplomacy to establish new norms of responsible behaviour in space, update regulatory structures, and strengthen space law, and the development of resilient space capabilities that reinforce deterrence in space. The two approaches complement each other, and the success of one does not negate the requirement for the other.

Firstly, as a result of the establishment of a United Nations (UN) Open Ended Working Group, following the tabling by the UK of the UN General Assembly Resolution 75-36 on 7 December 2020, international diplomatic, regulatory, and legal efforts are underway to establish norms of responsible behaviour in space (14). These efforts are gathering pace, and discussions on space arms control are ongoing at the UN in the hopes of constraining the pace and scope of weaponisation in space. Moreover, the Biden administration in the US has announced a unilateral ban on testing of 'kinetic kill' anti-satellite (ASAT) weapons, and efforts are underway to bring China, Russia and other states into talks towards establishing norms of responsible behaviour in space (15).

At the same time, and while efforts towards diplomatic and legal solutions are worthy and should continue, the recognition that such efforts could fail to bring about new norms of responsible behaviour, especially from authoritarian adversaries such as China and Russia, demand that a means to build deterrence against the use of counterspace capabilities is prioritised. The objective of the US and its western liberal democratic allies is to strengthen resilience in space as a path towards deterrence by denial. The objective of such a strategy would be to weaken the effectiveness of adversaries' counterspace systems, reducing their prospect of success in pursuing the objective of undertaking a decisive counterspace campaign and unleashing a 'pearl harbour in space' at the outset of a military conflict. If the potential cost in military, diplomatic, and political terms of using offensive counterspace capabilities is increased at the same time, in particular by denying an adversary anonymity and ensuring attribution through SDA, space deterrence by denial could see an adversary choose not to escalate a conflict by employing such capabilities.

The two paths—international diplomatic, regulatory, and legal efforts, backed by effective deterrence by denial in space—might strengthen the prospects of the space domain not becoming a warfighting environment in a future crisis. But neither path is guaranteed to succeed, and so the prospect of warfighting in space must be considered. How that occurs and what effects such a conflict would generate must be addressed.

War in Space

Modern counterspace weapons, or ASATs, are broadly based on three types of capability (16). The first is direct-ascent ASATs (DA-ASAT) that uses kinetic kill to physically destroy a target. This type of weapon was demonstrated by China in 2007, the US in 2008, India in 2019, and, most recently, by Russia in 2021 (17). The second type is a co-orbital ASAT that could either use kinetic kill or 'soft kill' methods, such as directed energy, electronic or cyber warfare or physical interference, to disable or damage a satellite, without creating a space debris field that are associated with kinetic kill systems. The third type are ground-based counterspace systems such as uplink and downlink jamming, laser dazzling and cyberattack, including spoofing, to disable or deny access to satellites or to attack ground stations. The use of kinetic kill ASATs is likely to become increasingly self-deterring, given the aftereffects of the physical destruction of satellites in the form of large debris fields, which then affect other orbits and satellites, and, in extremis, deny access to space as an outcome of a Kessler Syndrome event or due to the use of large numbers of DA-ASATs in a wartime situation. Instead, the future of space warfare may increasingly become dominated by soft-kill systems that are either co-orbital or ground based, which can generate scalable and even reversible effects, exploit a degree of anonymity, and operate more effectively within the grey zone in orbit.

Space warfare occurs in accordance with the laws of physics and orbital mechanics, at least within the region between LEO and GEO, and within the timeframe of the present through to the next two decades. Speculation about the distant future of military space capabilities opens possibilities regarding the nature of weapons, platforms and tactical engagements, but it is more useful to focus on the immediate challenge of space warfare occurring along what academic Bleddyn Bowen calls the "cosmic coastline" (18). It is this near-earth region between LEO and GEO that must be the immediate focus of thinking on space warfare, and until a ban on the development, testing and deployment of kinetic kill ASATs can be negotiated, the aftereffect of their use raises the risk of space debris that must be managed.

A key development that is now shaping space capabilities is the growing use of small satellite 'mega-constellations' that have the advantage of a large numbers of small satellites up to 1,000 kgs in mass to enhance resilience. Rather than concentrate critical space support on small numbers of large, complex satellites that are vulnerable to the threat posed by ASATs, the benefits in terms of survivability, resilience, and persistence are more apparent by relying on large numbers of low cost, small satellites, with a mega-constellation being much more difficult to attack. In space, quantity has a quality of its own, as even the loss of a few satellites will not appreciably degrade the performance of a mega constellation for satellite communications or earth observation.

When the impact of orbital dynamics is considered, the benefits of relying on larger numbers of small satellites becomes even more apparent. The nature of space manoeuvres, as explained in Rebecca Reesman and James R. Wilson's 2020 paper titled 'The Physics of Space War: How Orbital Dynamics Constrain Space to Space Engagement', makes clear that positioning co-orbital ASATs for RPOs with a target satellite is complex and time consuming (19). As the paper notes, there are five key concepts that define space warfare in the LEO to GEO realm: "…satellites move quickly, satellites move predictably, space is big, timing is everything, and satellites manoeuvre slowly (20)."

Expanding on the application of these concepts into how space warfare would unfold, Reeseman and Wilson argue that "Space to space engagements would be deliberate, and likely to unfold slowly because space is big, and spacecraft can escape their predictable paths only with great effort…. Attacks on space assets would require precision because spacecraft and even ground based space weapons can engage targets in space only after complex calculations are determined in a highly engineered domain (21)."

The paper considers the practical aspects of space warfare in the context of an ASAT, either direct-ascent or co-orbital, attacking a target satellite in various orbits within the LEO to GEO region, and the analysis correctly applies the laws of physics, including the constraints imposed by limited ΔV ('Delta-V', the ability of a spacecraft to manoeuvre in orbital plane and altitude between orbits) and orbital dynamics to provide a clear and convincing picture of the complexities of space to space engagement, be it for a kinetic kill or for a co-orbital soft kill. However, the complexities of such operations are bound to increase if mega-constellations are applied to the analysis. If a state's space support is augmented through large numbers of small satellites that operate in a complementary manner to traditional large satellites in a 'high-low' mix, simply destroying the large satellite does not necessarily remove critical space support to an opponent. Instead of a catastrophic collapse of space capabilities, there is a graceful degradation as small satellites provide additional space support across the range of tasks. Furthermore, small satellites are more easily launched to reconstitute lost space capabilities, especially if a state builds a sovereign launch capability, as is now emerging in Australia.

Therefore, to avoid a potential 'space pearl harbour' as a result of an adversary counterspace attack, the risks can be mitigated in part through greater reliance on small satellites that augment space support away from total reliance on a small number of large satellites to exploit the benefits of the small and the many. Even with the development of soft kill technologies such as uplink and downlink jamming, spoofing, electronic warfare, cyberattack, and directed energy weapons by generating far more targets than an offensive counterspace capability can manage, the ability of an opponent to launch a decisive counterspace attack is reduced. The rapid reconstitution of small satellites that are lost, together with effective SDA, also further reduces the effectiveness of offensive counterspace capabilities in an environment where the laws of physics and the principles of orbital dynamics rule.

The development of soft-kill capabilities for ASATs may add options for the attacker over single-use kinetic kill ASATS. Cyberattacks for disruption, spoofing, and uplink and downlink jamming are multi-use capabilities. They have 'deep magazines' in that that can be employed repeatedly due to the non-kinetic nature of the weapon system. Cyberattacks could potentially generate more effects across a wider range of targets than a single kinetic-kill ASAT, even given the potential uncertainty posed by debris field generated after a target satellite was destroyed by such an ASAT. Furthermore, unlike kinetic kill ASATs, which do create chaotic debris fields that threaten third parties, soft-kill systems invariably leave the target intact, and are thus more 'usable' than kinetic kill systems (22). The added complexity of mega-constellations comprising thousands or even tens of thousands of small satellites means that kinetic kill ASATs are simply ineffective in threatening such an orbital capability, whereas cyberattack, jamming, or even directed-energy weapons are likely to be far more flexible in their use and open up the 'grey zone' in orbit for exploitation by dual-role space capabilities (23).

However, as noted in the Reeseman and Wilson analysis, all forms of electromagnetic energy lose energy over distance, so to attack a target satellite, or multiple satellites as part of a mega-constellation,

still demands a rendezvous and proximity operation by an attacking co-orbital ASAT against a target, or alternatively, a lot of power if the counterspace capability is ground based, such as for uplink and downlink jamming. Ground-based jamming and the use of high-power microwave or high-energy laser to damage a satellite in orbit can exploit large power sources, but then can only target satellites that are crossing above the visual horizon, within the line of sight of the ground-based facility. For a mega-constellation, orbiting in LEO every 45 to 90 minutes, the potential for ground-based soft-kill capabilities to attack small satellites in significant numbers could provide a means for an aggressor to quickly erode satellite capabilities.

In summary, the attacker's advantage is enhanced if their opponent relies purely on traditional large satellites, deployed in limited numbers due to their complexity and expense and located in the LEO to GEO region, as there are fewer targets needed to be attacked to bring about a catastrophic collapse of space support during a 'space pearl harbour'. The physics of space warfare suggests that even with reliance on only a small number of satellites, a space war engagement would occur over a prolonged period as co-orbital ASATs employing soft-kill mechanisms manoeuvre to intercept their targets in a rendezvous and proximity operation, and then employ jamming, electronic warfare, directed energy weapons, or even cyberattacks to strike at an opponent's key space support. Complementing small numbers of large satellites with large numbers of small satellites in a 'high-low' mix degrades the ability of an aggressor to use counterspace capabilities to conduct a decisive attack, because space support is augmented and disaggregated, across the small, cheap and many rather than concentrated in a few large, expensive and vulnerable satellites. There is greater ease of rapid reconstitution of lost space capability through relying on small satellites and rapid sovereign launch capabilities that can quickly deploy satellites to plug gaps in space support where needed. Small satellites and satellite mega-constellations make the use of kinetic kill direct-ascent ASATs far less effective in attacking an opponent's space capabilities, given the sheer number of targets, the complexities of orbital dynamics to manage such a campaign, and the generation of massive amounts of space debris that would deny space to the aggressor, the defender, and third parties. Greater focus on developing soft-kill technologies for both co-orbital and ground-based counterspace offers a means to attack a greater number of satellites without generating large space debris clouds, but even these technologies will struggle to erode the potential offered by satellite megaconstellations.

Conclusion

Although there are earnest efforts within the diplomatic and international legal communities to strengthen regulatory arrangements on the use of space for peaceful purposes and preclude a slide towards space weaponisation, there are no guarantees that these efforts will succeed in preventing a war in space. Counterspace weapons development continues apace, particularly in China and Russia, and in a future major power military conflict, there would be every incentive for an aggressor to use counterspace capabilities to leave the US and its allies deaf, mute and blind. However, the actual mechanics of space war are complex, constrained by the laws of physics and orbital mechanics, and so the notion of a decisive blow in the form of a 'pearl harbour in space' must be tempered with recognition of the challenges of using such weapons effectively. A threat may emerge that can be detected by ground and space-based SDA, and the nature of orbital dynamics means that the threat can be averted through manoeuvre and timely attribution to deny anonymity, and thus prevent potential grey zone actions in orbit. In an outright

conflict, the use of counterspace weapons is likely to occur, and so the objective of the defender must be to ensure maximum resilience of space capabilities. Investment in large numbers of small satellites and the use of mega-constellations to provide critical space support in combination with traditional large satellites, and investment in responsive space launch capabilities for rapid reconstitution, reduces the potential effectiveness of offensive counterspace capabilities.

Ultimately, the best solution to meeting the threat posed by adversary counterspace capabilities is to promote a dual-track solution by enhancing and strengthening space law and regulation to establish new norms of responsible behaviour in space, and working to get all major space powers to agree to these new arrangements alongside investment in resilient space capabilities as a means to ensure effective space control that strengthens space deterrence. However, if it becomes clear that adversary states will not accept new norms of responsible behaviour in space and continue to develop their counterspace capabilities, then the 'space deterrence' and 'space resilience' element must take precedence to raise the cost of aggressive use of counterspace capabilities to unacceptable levels.

Endnotes

(1) Brian Weeden, Victoria Sampson, *Global Counterspace Capabilities – an Open Source Assessment*, 2022, at www.swfound.org/counterspace/

(2) Todd Harrison, Zack Cooper, Kaitlyn Johnson, Thomas Roberts, 'The evolution of space as a contested domain', *Space News*, October 9, 2017, https://aerospace.csis.org/wp-content/uploads/2018/01/Harrison_SpaceNews.pdf

(3) Craig Boucher, 'On Space War', *Modern War Institute at West Point*, June 1, 2022, https://mwi.usma.edu/on-space-war/ (accessed June 13, 2022)

(4) Missile Threat, 'Space-based Infrared System (SBIRS), CSIS Missile Defence Project, https://missilethreat.csis.org/defsys/sbirs/

(5) The Aerospace Corporation, 'A brief history of GPS', https://aerospace.org/article/brief-history-gps

(6) Ulas Yildirim, Malcolm Davis, 'Understanding the military's role in space'. *The Strategist*, 17 May, 2022, https://www.aspistrategist.org.au/understanding-the-militarys-role-in-space/

(7) 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/

(8) US Department of Defense, *Missile Defense Review*, 2019, https://media.defense.gov/2019/Jan/17/2002080666/-1/-1/1/2019-MISSILE-DEFENSE-REVIEW.PDF

(9) Nathan Strout, 'Space Force, Lockheed are ready to start making the nation's new satellites to watch for missiles', *C4ISRNET*, August 25, 2021, https://www.c4isrnet.com/smr/space-competition/2021/08/24/space-forces-next-generation-of-missile-warning-satellites-passes-major-design-milestone/

(10) Malcolm Davis, 'Australia needs new early warning capability to counter threat from China's new missiles', *The Strategist*, 21 December 2021, https://www.aspistrategist.org.au/australia-needs-new-early-warning-capability-to-counter-threat-from-chinas-new-missiles/

(11) Report of the US Commission to Assess United States National Security Space Management and Organization ('The Rumsfeld Commission', https://aerospace.csis.org/wp-content/uploads/2018/09/RumsfeldCommission.pdf , January 11, 2001

(12) Australian Department of Defence, *Space Power eManual*, and *Australia's Defence Space Strategy,* Defence Space Command, March 2022,

(13) Malcolm Davis, 'SpaceX's reusable rocket technology will have implications for Australia', *The Strategist,* 18 May 2021, https://www.aspistrategist.org.au/spacexs-reusable-rocket-technology-will-have-implications-for-australia/

(14) United Nations, 'Reducing space threats through norms, rules and principles of responsible behaviours : resolution / adopted by the General Assembly', file:///C:/Users/User/Dropbox/PC/Downloads/A_RES_75_36-EN.pdf see also United Nations, 'Open-ended working group on reducing space threats', https://meetings.unoda.org/section/oewg-space-2022_info-on-participation_17541/

(15) Daryl G. Kimball, 'U.S. Commits to ASAT Ban', *Arms Control Association*, May 2022, https://www.armscontrol.org/act/2022-05/news/us-commits-asat-ban

(16) Brian Weeden, Victoria Sampson, *Global Counterspace Capabilities – an Open Source Assessment*, 2022, https://swfound.org/counterspace/

(17) Malcolm Davis, 'The ramifications of Russia's reckless anti-satellite test', *The Strategist*, 18 November, 2021, https://www.aspistrategist.org.au/the-ramifications-of-russias-reckless-anti-satellite-test/

(18) Bleddyn Bowen, War in Space – Strategy, Spacepower, Geopolitics, Edinburgh University Press, 2020, p. 7.

(19) Rebecca Reesman, James R. Wilson, *The Physics of Space War: How orbital dynamics constrain space-to-space engagement*, The Aerospace Corporation, October 2020, https://csps.aerospace.org/papers/physics-war-space-how-orbital-dynamics-constrain-space-space-engagements; see also Reesman and Wilson, 'Physics gets a vote: No starcruisers for space force', *War on the Rocks*, June 28, 2021, https://warontherocks.com/2021/06/physics-gets-a-vote-no-starcruisers-for-space-force/

(20) Reesman and Wilson, *The Physics of Space War*, 2

(21) Reeseman and Wilson, 2

(22) Kaitlyn Johnson, Todd Harrison, Makena Young, Nicholas Wood, Aluyssa Goessler, *Space Threat Assessment 2022*, CSIS Aerospace Security, April 4 2022, https://aerospace.csis.org/space-threat-assessment-2022/

(23) Malcolm Davis, 'The commercial advantage in space's grey zone', *The Strategist*, June 16, 2021, https://www.aspistrategist.org.au/the-commercial-advantage-in-spaces-grey-zone/

Space and Future Warfare: Are We Heading Towards 'Star Wars'?

Almudena Azcárate Ortega

When placed in the same sentence, the words 'space' and 'war' evoke images of science fiction movies, even more so if the word 'future' is added to the mix. However, space technology has been a part of warfare for several years, especially since the Gulf War in 1990 (1). In recent decades, it has become the norm for military operations, and even military conflict, to involve space infrastructure, and it is likely that it will continue to be so in the future (2). But with the advancement of space technology and the continued development of counterspace assets (3), the question of how conflicts involving space systems will look in the future arises. This question is particularly relevant as the international community works towards preserving space security.

Given how essential space infrastructure has become, this essay will look at how existing applicable laws and regulations do not entirely mitigate current threats to space systems. In the face of these limitations, the international community must find a way to address space security concerns effectively. If it fails in this task, the future of warfare will be one where space could become a new theatre of conflict, with devastating consequences for humankind. However, if the international community succeeds in reaching a common understanding on space security issues, this bleak future could be avoided.

The Importance of Space Infrastructure

Space technology is critical for humankind (4). This is particularly true for service-oriented infrastructures such as the Global Navigation Satellite System (GNSS), Earth observation satellites, and communication satellites (SatComs). These technologies can carry out various tasks (for instance, positioning, navigation and timing signals, space imagery, and orbital signal relay amplification),

providing access to many of the services we rely on daily. For example, satellites make safe navigation possible in the air, on land, and at sea. Satellite services also allow people to access high-speed internet, carry out electronic financial transactions, and control and manage certain critical infrastructures and services, such as energy grids, water, and transportation (5). The development and use of these services by private companies, public authorities, households, and individuals that make up the global economy highlight the significant reliance on space assets (6).

This is also the case when it comes to the use of space assets by the defence and security apparatus, particularly in warfighting scenarios (7) Remote sensing satellites, for example, provide militaries with intelligence, surveillance and reconnaissance (ISR) data that allow them to identify their adversary's capabilities, track troop movements, and locate potential targets. ISR data also provides information to facilitate disaster relief and humanitarian assistance operations. SatComs can provide encrypted communications and improve situational awareness, which allows military forces greater mobility. Similarly, positioning, navigation and timing satellite data allows for more precise and discriminate targeting for munitions and air, land, and sea navigation (8).

Given humankind's dependence on space infrastructure, its security is undoubtedly of paramount importance (9), yet, it faces numerous threats.

Dangers and Threats to Space Security

There are multiple dangers that jeopardise peace and sustainability in space, ranging from unintentional safety hazards (such as geomagnetic storms or the accidental malfunctioning of a satellite) to intentional actions to damage another actor's space technology that threaten space security (10). The latter is particularly tragic due to its preventable nature and, if not checked, can forecast a grim future.

The international community agrees that outer space should be kept peaceful and secure. In 1958, only one year after the launch of Sputnik I (the first artificial satellite to complete an orbit around the Earth), the UN General Assembly expressed the need "to avoid the extension of present national rivalries into this new field" (11). Years later, in 1978, the notion of the Prevention of an Arms Race in Outer Space (PAROS) emerged during the Tenth Special Session of the UN General Assembly (the first special session devoted to disarmament) with a view to contributing to space security by preventing the escalation of tensions. Since then, every year, several resolutions are passed at the UN General Assembly on the topic (12). Despite this, it seems that now more than ever before, space security is in jeopardy, with an increasing number of states developing numerous forms of counterspace technology (13). In addition, some countries are establishing policies that explicitly consider the space domain an operational or even a warfighting domain (14).

The use of kinetic anti-satellite technologies (ASAT), such as direct-ascent missiles against objects in orbit, is often cited by stakeholders—states and non-governmental entities alike—as a major concern. This is primarily due to the debris-creating effects of kinetic ASAT weapons, and stakeholders have been particularly vocal on this issue in recent years. For example, the report by the UN Secretary-General published in 2021 pursuant to UN General Assembly Resolution 75/36 on 'Reducing space threats through norms, rules and principles of responsible behaviours' (15), expressed how, for many of the

states that submitted their views to the Secretary-General (16), space debris is the most significant threat to the space environment (17). The intentional use of kinetic force in space is generally recognised as dangerous and irresponsible, but States have so far shied away from condemning it as an illegal action (18). Countries, therefore, continue to be able to test these technologies on their own assets in a way that further increases tensions and puts the sustainability of space at risk.

Recognising the danger of intentional debris creation, the US (19), Canada (20), New Zealand (21), Japan (22), Germany (23), the UK (24), South Korea (25), Australia (26), and Switzerland (27) have made unilateral commitments not to test direct-ascent anti-satellite missiles, and have encouraged other countries to follow their example. While many have praised this as a positive step towards a more sustainable space domain, others have refrained from undertaking similar commitments. The US also sponsored a resolution on "Destructive direct-ascent anti-satellite missile testing" (28), which calls on states to "commit not to conduct destructive direct-ascent anti-satellite missile tests", highlighting the importance of such commitment to protect the space environment and to contribute to the prevention of an arms race in outer space. The First Committee adopted this resolution with 154 votes in favour, 8 against, and 10 abstentions (29), thus highlighting that kinetic ASAT testing is an issue of great concern for the international community.

But kinetic ASAT threats are not the only concern. Non-kinetic counterspace technologies, such as the use of electromagnetic pulses, electronic means of attack like jamming and spoofing, and cyberattacks, are also a threat. These can interfere with the regular operations of a satellite system and can have dangerous effects on the services these satellite systems provide (30). Such forms of attack are often harder to predict, prevent, and attribute.

The development and testing of these technologies, even when not used against other states, contributes to the escalation of tensions, and if left unchecked, could eventually lead to a destabilising arms race that could lead to conflict (31). This could have devastating consequences for humankind, as the disabling or destruction of space systems will have reverberating effects deeply felt by all (32).

The Reach and Limitations of Outer Space Law

The fear of escalating tensions in space emerged in the early days of human space exploration. Consequently, the international community chose to preserve the space domain for "peaceful purposes" (33) by negotiating the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (OST) (34).

The desire to maintain peace in space led the drafters of the OST to determine, under Article III, that international law, including the Charter of the United Nations (35), would apply to outer space. This includes Article 2(4) of the UN Charter, which prohibits the use of force. Under Article IV, the OST also prohibits the placement, installation, or stationing of nuclear weapons or other weapons of mass destruction in orbit, on the Moon, or on other celestial bodies. However, beyond this, the OST does not elaborate on space security issues but instead focuses on establishing principles to govern the peaceful uses of outer space. Subsequent treaties, regulations, and guidelines specific to outer space

have expanded on the principles set out by the OST, thus also focusing on the peaceful uses of outer space, and only addressing space security tangentially (36).

International outer space law is characterised by a permissive and open-ended language, which has allowed the emergence of different interpretations regarding the use and exploration of space. In this sense, the aforementioned concept of "peaceful purposes" has been generally understood to mean non-aggressive or non-hostile use, rather than non-military (37). Moreover, the prohibition of Article IV of the Outer Space Treaty does not extend to the use of conventional weapons. As long as those weapons are not used against another actor—in what would be a breach of the use of force prohibition enshrined in Article 2(4) of the UN Charter—states are free to develop and test any counterspace technologies they deem fit.

International space treaties evidence that the international community had great aspirations of peace and inclusivity, but the emphasis on freedom of action at the centre of these instruments has facilitated turning outer space into a domain where military activities are accelerating and geopolitical tensions are escalating at a rapid and dangerous pace. Unless these growing tensions are diffused, and a common understanding on space security matters is reached, humankind risks suffering the devastating consequences of a space-based conflict (38).

Reaching Common Understanding on Space Security: Impact on Future of Warfare

Since its emergence, PAROS has been the primary objective of multilateral discussions on space security within the UN and is a regular feature in resolutions and in the mandates of working groups. Awareness of growing concerns over space security and the limitations in existing regulations has led to multiple attempts to bolster space security by the international community. These attempts have, however, had limited success. Political and technical obstacles have stifled progress, but states have not yet given up on advancing space security.

Achieving a common understanding may be difficult because of the complexity of space systems, the multiple uses and users of such systems, and the lack of space-specific regulations that focus on space security. Existing international law, particularly international humanitarian law (IHL), can provide helpful guidance on achieving this. Most countries agree that IHL should apply to outer space under Article III of the OST, as it is part of general international law. Such an approach recognises the catastrophic consequences of future war in space and seeks to diminish the evils of war by protecting combatants—and perhaps more importantly, also non-combatants—from its effects (39). However, some states have expressed concerns about discussing the applicability of IHL to outer space (40). They have argued that space should not be a domain of conflict, and therefore the international community should focus on prevention instead of on regulating the possibility of conflict. In the view of these States, discussing the applicability of IHL only increases the likelihood of space becoming a domain of warfare (41). Even if discussing the applicability of IHL was not an issue of concern for some states, there is no uniform interpretation of how IHL principles apply to space systems.

This is further complicated by the inherent complexity of space systems: they comprise different components. Firstly, the space segment, which includes satellites and space launch vehicles. Secondly, the ground segment, including satellite dishes and receiving stations. And thirdly, the data links in between (42). Therefore, warfare involving space systems and counterspace technology is not limited to the space domain. It is important to take into account that any component of a space system can be targeted with counterspace technology, and the entire space system would be affected as a result.

Moreover, there are many different users of one single space system, which further compounds the issue's complexity. As such, the use of counterspace technology against a space system, or a component of one, could affect not just the intended target but others that also benefit from its services (43). In the context of an armed conflict, this raises questions about targeting and neutrality. Under IHL, only military objectives are targetable (44), and belligerents are obligated to respect a neutral's inviolability and can only direct attacks against other belligerents (45). While this may seem like an obvious rule to follow when a space object provides services to many parties, often located in other countries, the lines become blurred. Should the belligerent base its decision on who the state of registry is (46)? Who the launching states are (47)? Who the satellite users are?

States have also expressed concern about the dual nature of many space objects and how this characteristic can make it difficult to ascertain when a space object could present a threat (48). States use the term "dual-use" to refer to two categories of objects. On the one hand, actual dual-use objects have a military and security function, as well as a civilian or commercial one (either simultaneously or alternating. Alternate use is sometimes known as dual-capable (49)). An example of this would be GNSS satellites. On the other hand, dual-purpose objects are those that are designed to fulfil a benign objective (such as debris removal or on-orbit servicing), but they could potentially be repurposed to harm other space objects (50).

The lack of clarity surrounding dual-use and dual-purpose objects—not just in terms of the concept but also in terms of their functions—fosters mistrust among states. Their perceived operational ambiguity could lead certain actors to consider them targetable (51). Dual-use objects see the integration of military and civilian functions as one sole object, which some have argued constitutes a violation (52) of the principle of passive precautions (53), by which belligerents must ensure their military objectives are distinguishable from those that are not, to ensure that their enemies can comply with their obligation of distinction and limit their attacks to targetable objectives (54). Dual-purpose objects are, in principle, not intended to perform military functions directly (although they may provide some form of support to military satellites through on-orbit servicing, for example (55)) or aggressive and hostile actions against other satellites. The lack of understanding of these objects, coupled with the possibility that they could be repurposed for such aggressive actions, raises concerns among states, who have increasingly called for more transparency to avoid the risk of miscalculation and misunderstandings that could heighten tensions in the context of the utilisation of these objects.

Lack of trust and transparency inevitably leads states to assume worst-case scenarios that equate the development of new capabilities to threats. This space technology development leads to a constant tussle to prove technological one-upmanship among countries perceiving each other as competitors, fostering the continuation of the development of counterspace technologies (56). Therefore, efforts to reach common understandings on space security matters are essential for the international community.

Recent Efforts to Keep 'Star Wars' at Bay

Despite the limited success of the previous initiatives to tackle space security concerns, the international community is committed to finding a solution. In recent years, there has been an increased demand for regulations that focus on behaviour in outer space (57).

Moreover, some within the diplomatic community have proposed an approach that focuses on norms, rules, and principles as a mechanism that could effectively break the existing stalemate and reduce the geopolitical tensions, misperceptions, and competition in space that have not allowed past proposals to succeed (58). The most recent iteration is the UN General Assembly Resolution 75/36 on "Reducing space threats through norms, rules and principles of responsible behaviours," adopted in December 2020. This was followed by Resolution 76/231 of the same name, adopted in December 2021, which convened an open-ended working group (OEWG) with the mission of "mak[ing] recommendations on possible norms, rules and principles of responsible behaviours relating to threats by States to space systems, including, as appropriate, how they would contribute to the negotiation of legally binding instruments, including on the prevention of an arms race in outer space" (59).

This process has encouraged a renewal of the discussion on ensuring space security and mitigating and stopping what threatens it. The results have so far been positive, with a high degree of engagement from states on all sides of the geopolitical spectrum. The process has even encouraged unilateral commitments by the US, Canada, New Zealand, Japan, Germany, the UK, South Korea, Australia, and Switzerland to foster norm-creation and state practice relating to testing direct-ascent kinetic ASATs. These developments have stimulated cautious optimism around the progress towards achieving the goals of PAROS. Ultimately, even though states have differing ideas on how to reach these goals, they share many common concerns and a common interest in finding solutions to them (60).

Conclusion

If the spirit of cooperation and willingness to exchange views that have characterised the OEWG's discussions perseveres, states may soon have a set of norms, rules, and principles to reduce threats to space systems. This could, in turn, lay the foundation for a legally binding agreement. However, it is also important to recognise that any regime—whether based on legally binding or non-binding mechanisms—is only as effective as states' willingness to comply with it. While recent developments in the diplomatic sphere are encouraging, the hope for cooperation that they bring can easily be eclipsed by some states' continued insistence on developing and testing counterspace technologies, as well as the broader challenge posed by the lack of transparency and trust surrounding activities in the space domain (61).

The future of warfare in relation to space will look vastly different if the international community takes the opportunity the OEWG provides to reach common understanding on space security concerns. Military operations and even armed conflict on Earth will likely always entail the use of space systems to provide some form of support, but if diplomacy fails and tensions continue to escalate, outer space could become a theatre for conflict. Reaching common understanding on space security issues is of the

utmost importance, as it would provide the foundation the international community needs to establish clear rules and regulations on conducting activities in space to keep the domain peaceful and secure, thus ensuring that *Star Wars* remains science fiction.

Endnotes

(1) Dale Stephens and Cassandra Steer, "Conflicts in Space: International Humanitarian Law and Its Application to Space Warfare" in *War and Peace in Outer Space: Law, Policy, and Ethics*, Eds. Cassandra Steer and Matthew Hersch (Oxford University Press, 2020) 23.

(2) Robert A. Ramey, "Armed Conflict on the Final Frontier: the Law of War in Space", *48 A.F. L. Rev. 1*, 121 (2000); Stephens and Steer, "Conflicts in Space: International Humanitarian Law and Its Application to Space Warfare."

(3) Brian Weeden and Victoria Samson eds., "Global Counterspace Report", *Secure World Foundation*, April 2022, https://swfound.org/counterspace/

(4) Jessica West and Almudena Azcárate Ortega, "Norms for Outer Space: A Small Step or a Giant Leap for Policymaking?", *UNIDIR*, 2022, https://unidir.org/publication/space_dossier_7_norms_outer_space.

(5) James Black, "Our reliance on space tech means we should prepare for the worst", *Defense News*, 12 March 2018, https://www.defensenews.com/space/2018/03/12/our-reliance-on-space-tech-means-we-should-prepare-for-the-worst/

(6) International Committee of the Red Cross, *Constraints under International Law on Military Operations in, or in Relation to, Outer Space during Armed Conflicts*, 2022, https://www.icrc.org/en/document/constraints-under-international-law-military-space-operations

(7) European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, *Dependence of the European economy on space infrastructures: Potential impacts of space assets loss*, Publications Office of the European Union, 2018, https://data.europa.eu/doi/10.2873/81127

(8) Defense Intelligence Agency, *Challenges to Security in Space. Space Reliance in an Era of Competition and Expansion*, 2022, https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf

(9) Nivedita Raju, "Diluted disarmament in space: Towards a culture for responsible behaviour", *SIPRI*, 17 November 2020, https://www.sipri.org/commentary/essay/2020/diluted-disarmament-space-towards-culture-responsible-behaviour

(10) Laetitia Cesari Zarkan, "What's in a word? Notions of 'security' and 'safety' in the space context", *UNIDIR*, 2021, https://www.unidir.org/commentary/whats-word-notions-security-and-safety-space-context

(11) UN GAOR, *GA Res. 1348 (XIII), 13th Sess., Supp. No. 18b UN Doc. A/4090*, 13 December 1958, https://www.unoosa.org/oosa/oosadoc/data/resolutions/1958/general_assembly_13th_session/res_1348_xiii.html

(12) In 2021, five resolutions were passed:

GA Res. 76/22, 76th Sess., *Prevention of an Arms Race in Outer Space*, 6 December 2021, https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F76%2F22&Language=E&DeviceType=Desktop; GA Res. 76/23, 76th Sess., "*No First Placement of Weapons in Outer Space*", 6 December 2021, https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F76%2F23&Language=E&DeviceType=Desktop; GA Res. 76/230, 76th Sess., "*Further Practical Measures for the Prevention of an Arms Race in Outer Space*", 30 December 2021, https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F76%2F230&Language=E&DeviceType=Desktop;

GA Res. 76/55, 76th Sess., "*Transparency and Confidence-building Measures in Outer Space Activities*", 13 December 2021, https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F76%2F55&Language=E&DeviceType=Desktop;

GA Res. 76/231, *76th "Sess. on Reducing space threats through norms, rules and principles of responsible behaviours"*, 30 December 2021, https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F76%2F231&Language=E&DeviceType=Desktop.

(13) Todd Harrison, Kaitlyn Johnson, Makena Young, Nicholas Wood and Alyssa Goessler, "Space Threat Assessment 2022*", CSIS Aerospace Security Project*, April 2022, https://www.csis.org/analysis/space-threat-assessment-2022

(14) NATO, *Overarching Space Policy*, 2019, https://www.nato.int/cps/en/natohq/official_texts_190862.htm?utm_source=linkedin&utm_medium=nato&utm_campaign=20220117_space; Dominic Nicholls, "Space is now a 'warfighting domain' says Chief of the Air Staff", *The Telegraph*, 15 September 2020, https://www.telegraph.co.uk/news/2020/09/15/space-now-warfighting-domain-says-chief-air-staff/

(15) GA Res. 75/36, 75th Sess., *Reducing space threats through norms, rules and principles of responsible behaviours*, 16 December 2020, https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F75%2F36&Language=E&DeviceType=Desktop

(16) Thirty States, the European Union, and nine non-State actors submitted substantive comments. The details of each submission are available online on the UN Office of Disarmament Affairs website, available at https://www.un.org/disarmament/topics/outerspace-sg-report-outer-space-2021/.

(17) Report of the Secretary-General A/76/77, *Reducing space threats through norms, rules and principles of responsible behaviours,* 12-13 July 2021, https://undocs.org/en/A/76/77.

(18) Almudena Azcárate Ortega, "Return of ASATs and counterspace technologies: A slippery slope to weaponisation?" *ORF*, 19 October 2021, https://www.orfonline.org/expert-speak/return-of-asats-and-counterspace-technologies/

(19) The White House, *Remarks by Vice President Harris on the Ongoing Work to Establish Norms in Space,* 18 April 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/04/18/remarks-by-vice-president-harris-on-the-ongoing-work-to-establish-norms-in-space/

(20) Statement of Canada, *Open-ended working group on reducing space threats – Agenda item 5. General exchange of views on all matters*, May 2022, https://documents.unoda.org/wp-content/uploads/2022/05/Canada-General-Statement-for-Translators-OEWG-Space-Threats-Session-bilingual.pdf

(21) Mike Houlahan, "Mahuta's satellite test pledge launches policy school", *Otago Daily Times*, 2 July 2022, https://www.odt.co.nz/news/dunedin/campus/mahuta's-satellite-test-pledge-launches-policy-school

(22) Ministry of Foreign Affairs of Japan, *Decision not to conduct Destructive, Direct-Ascent Anti-Satellite Missile Testing*, 13 September 2022, https://www.mofa.go.jp/press/release/press3e_000451.html

(23) Statement of Germany, *Open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours*, 13 September 2022, https://documents.unoda.org/wp-content/uploads/2022/09/220913-Statement-by-Germany-on-13-September.pdf

(24) Foreign, Commonwealth & Development Office and UK Space Agency, *Responsible space behaviours: the UK commits not to destructively test direct ascent anti-satellite missiles*, 3 October 2022, https://www.gov.uk/government/news/responsible-space-behaviours-the-uk-commits-not-to-destructively-test-direct-ascent-anti-satellite-missiles

(25) Hwang Joon-kook, South Korea's permanent representative to the United Nations, UN Web TV at 01:09:15, 4 October 2022, https://media.un.org/en/asset/k11/k11cb8lhld?fbclid=IwAR2GAA-Y5G_v1VqiC5vesqLco4j8tbZWQhFidGZTFJ-KjO-jloz0mIRl5hw

(26) Defense Ministers Government of Australia, *Australia advances responsible action in space*, 27 October 2022, https://www.minister.defence.gov.au/statements/2022-10-27/australia-advances-responsible-action-space

(27) Statement of Switzerland, *77ème session de l'Assemblée Générale Première Commission Débat thématique sur l'espace extra-atmosphérique New York, le 26 octobre 2022 Déclaration prononcée par la Suisse*, 26 October 2022, https://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com22/statements/26Oct_Switzerland.pdf

(28) 1C Res. A/C.1/77/L.62, 77th Sess., *Destructive direct-ascent anti-satellite missile testing*, 13 October 2022, https://documents-dds-ny.un.org/doc/UNDOC/LTD/N22/630/36/PDF/N2263036.pdf?OpenElement

(29) 1C Res. A/C.1/77/L.62, 77th Sess., *Destructive direct-ascent anti-satellite missile testing*, 13 October 2022 – voting results, https://www.reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com22/votes/L62.pdf

(30) West and Azcárate Ortega, "Norms for Outer Space: A Small Step or a Giant Leap for Policymaking?*"*

(31) Ludmila V. Pankova, Olga V. Gusarova, Dmitry V. Stefanovich, "International Cooperation in Space Activities amid Great Power Competition*", 19 Russia in Global Affairs*, 97, 99, 2021.

(32) International Committee of the Red Cross, *The Potential Human Cost of the Use of Weapons in Outer Space and the Protection Afforded by International Humanitarian Law*, 7 April 2021, https://www.icrc.org/en/document/potential-human-cost-outer-space-weaponization-ihl-protection; International Committee of the Red Cross, *Constraints under International Law on Military Operations in, or in Relation to, Outer Space during Armed Conflicts*, 3 May 2022, https://www.icrc.org/en/document/constraints-under-international-law-military-space-operations

(33) See preamble of the 1967 Outer Space Treaty: *Recognizing the common interest of all mankind in the progress of the exploration and use of outer space for peaceful purposes.* Reference to peaceful purposes or the peaceful exploration of outer space is also made in articles IV and IX OST, as well as article 3 Moon Agreement. The preambles of the Agreement on the Rescue of Astronauts, the Return of Astronauts and Return of Objects Launched into Outer Space, the Convention on International Liability for Damage Caused by Space Objects and the Convention on Registration of Objects Launched into Outer Space also highlight this core principle. It is generally accepted that this principle has achieved the status of customary international law.

(34) Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 27 January 1967, 18 UST 2410; 610 UNTS 205; 6 ILM 386

(35) Charter of the United Nations and Statute of the International Court of Justice, 26 June 1945, 59 Stat. 1031; T.S. No. 993; 3 Bevans 1153

(36) For an overview of current legal and regulatory frameworks that address space security issues, see UNIDIR, *Existing Legal and Regulatory Frameworks concerning threats arising from State behaviours with respect to outer space*, 5 May 2022, https://documents.unoda.org/wp-content/uploads/2022/05/20220509-WP-UNIDIR-FINAL-UN-Format.pdf

(37) Shannon Orr, "Peace And Conflict In Outer Space*", 30 Peace Research 52, 58*, (1998); Bhupendra Jasani and Maria A. Lunderius, "Peaceful Uses of Outer Space-Legal Fiction and Military Reality*", 11 Security Dialogue 57, 58*, (1980).

(38) West and Azcárate Ortega, "Norms for Outer Space: A Small Step or a Giant Leap for Policymaking?*"*

(39) Geoffrey S. Corn, Victor Hansen, Richard Jackson, Christopher Jenks, Eric Talbot Jensen, James A. Schoettler, "The Law of Armed Conflict. An Operational Approach," 39 (2nd ed. Aspen Casebook Series, 2019).

(40) Theresa Hitchens, "UN talks on space norms surprisingly collegial, but fireworks to come: Sources", *Breaking Defense*, 31 May 2022, https://breakingdefense.com/2022/05/un-talks-on-space-norms-surprisingly-collegial-but-fireworks-to-come-sources/

(41) A/AC/294/2022/WP.3, *Document of the Russian Federation on the scope of work of the UN Open-Ended Working Group (OEWG) established pursuant to UN GA resolution 76/231*, https://documents.unoda.org/wp-content/uploads/2022/04/ENG-Позиционный-документ-по-ответственному-поведению-в-космосе.pdf.

(42) A/AC.294/2022/WP.10, *Submission of China Pursuant to United Nations General Assembly Resolution 76/230*, https://documents.unoda.org/wp-content/uploads/2022/05/A_AC294_2022_WP10_E_China.pdf

(43) Matt Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine", *Wired*, 23 March 2022, https://www.wired.com/story/viasat-internet-hack-ukraine-russia/

(44) Article 48 of the Protocol (I) Additional to the Geneva Conventions of August 12, 1949, Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977, 1125 UNTS. 3.

(45) Article 1 of the Hague Convention No. V respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 18 October 1907, 36 Stat. 2310, and article 1 Hague Convention No. XIII concerning the Rights and Duties of Neutral Powers in Naval War, 18 October 1907, 36 Stat. 2415

(46) Article I.c) of the Convention on Registration of Objects Launched into Outer Space, 14 January 1975, 1023 UNTS 15.: "The term "State of registry" means a launching State on whose registry a space object is carried in accordance with article II."

(47) Article I.a) of the Registration Convention. The term is also defined in article I(c) of the Convention on International Liability for Damage Caused by Space Objects, 29 March 1972, 961 UNTS 187: "The term "launching State" means: (i) A State which launches or procures the launching of a space object; (ii) A state from whose territory or facility a space object is launched."

(48) Report of the Secretary-General A/76/77, *Reducing space threats through norms, rules and principles of responsible behaviours*, 13 July 2021, https://undocs.org/en/A/76/77.

(49) David A. Koplow, "Reverse Distinction: A U.S. Violation of the Law of Armed Conflict in Space*", 13 Harv. Nat'l Sec. J. 25*, 46 2022.

(50) Almudena Azcárate Ortega, "Statement to the Open-Ended Working Group on 'Reducing space threats through norms, rules and principles of responsible behaviours' - Topic 3: Current and future space-to-space threats

by States to space systems", 14 September 2022, https://documents.unoda.org/wp-content/uploads/2022/09/Azcarate-Ortega-Almudena-OEWG-dual-use-presentation-FINAL.pdf

(51) Almudena Azcárate Ortega and Laetitia Cesari Zarkan, "The road to a moratorium on kinetic ASAT testing is paved with good intentions, but is it feasible?", *Fondation pour la recherche stratégique*, 23 May 2022, https://www.frstrategie.org/en/publications/notes/road-moratorium-kinetic-asat-testing-paved-good-intentions-it-feasible-2022

(52) Koplow, "Reverse Distinction: A U.S. Violation of the Law of Armed Conflict in Space"

(53) Article 58 Additional Protocol I.

(54) Article 48 Additional Protocol I.

(55) Hannah Duke, "On-Orbit Servicing – Opportunities for U.S. Military Satellite Resiliency", *CSIS*, 15 September 2021, http://aerospace.csis.org/wp-content/uploads/2021/09/20210914_Duke_OSAM.pdf

(56) Joan Johnson-Freese and David Burbach, "The Outer Space Treaty and the weaponization of space", *75 Bulletin of the Atomic Scientists 138*, (2019).

(57) Brian Weeden and Victoria Samson, "India's ASAT Test is Wake-Up Call for Norms of Behavior in Space", *Space News*, 8 April 2019, https://spacenews.com/op-ed-indias-asat-test-is-wake-up-call-for-norms-of-behavior-in-space.

(58) Comm. on the Peaceful Uses of Outer Space, *Operating in Space: Towards Developing Protocols on the Norms of Behaviour*, U.N. Doc A/AC.105/2019/CRP.12, 2019

(59) GA Res. 76/231, 76th Sess. 5 c), 2021, https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F76%2F231&Language=E&DeviceType=Desktop.

(60) Jessica West, "The UK Process On Norms And Space Security", Project Ploughshares, July 2021.

(61) Azcárate Ortega, "Return of ASATs and counterspace technologies: A slippery slope to weaponisation?"

Implications Perspectives

The Legal Constraints of Cyber Operations in Armed Conflicts

Kubo Mačák and Laurent Gisel

The use of cyber operations during armed conflicts is now a reality. While only a few states have publicly acknowledged using such operations, an increasing number are developing military cyber capabilities, and their use is only likely to rise in the future. The international community recognises that just as any other means and methods of warfare, cyber operations may seriously affect civilian infrastructure and result in "devastating…humanitarian consequences" (1).

These words of caution are supported by the growing evidence of particularly concerning cyber incidents over the past few years (primarily outside armed conflicts), including cyber operations against hospitals, water and electrical infrastructure, and nuclear and petrochemical facilities (2). The increasing use of military cyber capabilities and the related humanitarian concerns underscore the urgency of reaching a shared understanding of the legal constraints that apply to the use of cyber operations during armed conflicts.

This essay sets the scene by defining the notion of cyber operations during armed conflicts and by presenting a summary of the current military use of cyber operations and their potential human cost. It then discusses the threshold question of whether international humanitarian law (IHL) applies to cyber operations and zooms in on three specific issues related to how IHL principles and rules apply to cyber operations during an armed conflict (3).

Cyberspace and Cyber Operations: Setting the Scene

IHL does not contain a definition of cyber operations, cyber warfare, or cyber war, nor do other international law fields. Definitions used by states vary from those that narrowly focus on the use of

cyber capabilities to achieve goals in cyberspace (4), to broader approaches that refer to information war and define this notion in a manner that includes at least some aspects of what is often understood as cyber warfare (5). The International Committee of the Red Cross (ICRC) understands cyber operations during an armed conflict as "operations against a computer system or network, or another connected device, through a data stream, when used as means or method of warfare in the context of an armed conflict" (6).

In recent years, societies have become largely dependent on information and communication technologies (ICTs), a process that was accelerated by the COVID-19 pandemic. While there are numerous benefits and opportunities offered by growing interconnectivity, increased dependency also implies increased vulnerability. Whereas the emergent proliferation of cyber tools and their use as a means or method of warfare may offer belligerents the possibility of achieving their objectives without necessarily causing direct harm to civilians or physical damage to civilian infrastructure, the potential human cost of cyber operations must not be neglected.

Using cyber operations, processes controlled by computer systems can be triggered, altered, or otherwise manipulated, and essential civilian data, including medical data, can be tampered with, with the potential to cause significant harmful effects for civilians. Moreover, cyber operations can harm infrastructure in at least two ways. First, they can affect the delivery of essential services to civilians, as has been the case in several cyber operations against electrical grids, water supply facilities, or the healthcare sector. Second, they can cause physical damage, as was the case with the Stuxnet attack against a nuclear enrichment facility in Iran in 2010, and an attack on a German steel mill in 2014 (7).

These risks are compounded by the interconnectivity that characterises cyberspace, which means that whatever has an interface with the Internet can be affected by cyber operations conducted from anywhere in the world. A cyber operation against a specific system may have repercussions on various other systems, regardless of where those systems are located. Cyber operations conducted over recent years (primarily outside armed conflicts) have shown that malware can spread instantly around the globe and affect civilian infrastructure and the provision of essential services (8). There is a real risk that cyber tools—either deliberately or by mistake—may cause large-scale and diverse effects on critical civilian infrastructures, such as essential industries, telecommunications, transport, governmental, and financial systems. As one cybersecurity expert put it, such military operations constitute a "humanitarian crisis in the making" (9).

The characteristics of cyberspace raise other concerns as well. For example, cyber operations entail a risk of escalation and related human harm because it may be difficult for the targeted party to know whether the attacker's aim is intelligence collection (computer network exploitation) or more harmful effects (computer network attack). The target may thereby react with greater force than necessary in anticipation of a worst-case scenario, leading to an unexpected escalation of competition and conflict (10).

Cyber tools also proliferate in a unique manner. Once used, they can be repurposed or re-engineered and thus widely used by actors other than the one that initially developed or used them. A further concern is the difficulty of reliably attributing cyber operations, which hampers the identification of the authors of such operations, holding them accountable, and determining the applicable legal framework (11). The perception that it will be easier to deny responsibility for such operations may also weaken

the taboo against their use and may make actors less scrupulous about using them in violation of international law (12).

Overall, these concerns underscore the need to understand the potentially harmful impact of cyber operations on the civilian population and, accordingly, the protections afforded to civilians and civilian infrastructure by the applicable international law. In this regard, IHL plays a central protective function as a 'legal firewall' to limit the effects of cyber operations in armed conflicts (13).

Does IHL Apply to Cyber Operations During Armed Conflicts?

States have repeatedly reaffirmed that international law applies to the use of ICTs, most recently in last year's reports of the UN Open-Ended Working Group (OEWG) (14). and the UN Group of Governmental Experts (GGE) (15). The GGE report also expressly referred to IHL in the cyber context (a historical first for UN-based processes), noting that this branch of international law "applies only in situations of armed conflict" (16). Commentators have interpreted this reference as amounting to a consensus among the participating states on the applicability of IHL to cyber operations (17).

In our view, there is no question that IHL applies to, and therefore limits, cyber operations during armed conflict, just as it regulates the use of any other weapon, means, and methods of warfare in an armed conflict, whether new or old. In doing so, IHL seeks to minimise the humanitarian consequences of armed conflict, whether caused by kinetic or cyber means. This holds true irrespective of whether cyberspace is considered as a new domain of warfare similar to air, land, sea, and outer space; a different type of domain because it is man-made while the former is natural, or not a domain as such (18).

In line with this view, an increasing number of states and international organisations have publicly asserted that IHL applies to cyber operations during an armed conflict (19). At the same time, some states have expressed opposition to the militarisation of cyberspace or a cyber arms race and have expressed concerns regarding a possible legitimisation of the use of military cyber operations (20). While these are important considerations, they are not necessarily incompatible with the application of IHL to cyber operations during armed conflict.

In particular, acknowledging that IHL applies to cyber operations during an armed conflict is not an encouragement to militarise cyberspace and should not be understood as legitimising cyberwarfare (21). As underscored in the 2021 GGE report, "recalling [IHL] principles by no means legitimises or encourages conflict" (22). In fact, IHL imposes substantial limits on the militarisation of cyberspace by prohibiting the development of military cyber capabilities that would violate IHL (23).

Finally, it must be noted that any use of force by states—cyber or kinetic—remains governed by the UN Charter and the relevant rules of customary international law, in particular, the prohibition against the use of force (24). International disputes must be settled by peaceful means (25), as recently reaffirmed in the cyber context in both the OEWG and the GGE processes (26).

How IHL Applies to Cyber Operations During Armed Conflicts: Specific Challenges

While affirming that IHL applies to cyber operations in an armed conflict is an essential first step to avoid or minimise the potential human suffering that cyber operations might cause, it is equally important for states to work towards common understanding of how IHL principles and rules apply to the specific nature of cyber operations (27). In the present section, we emphasise three key challenges in this area (28).

Cyber operations and the notion of 'attack' under IHL

The question of whether or not an operation amounts to an 'attack' as defined in IHL is essential for the application of many of the rules deriving from the principles of distinction, proportionality, and precaution, which afford important protection to civilians and civilian objects (29). Concretely, rules such as the prohibition on attacks against civilians and civilian objects, the prohibition on indiscriminate and disproportionate attacks, and the obligation to take all feasible precautions to avoid or at least reduce incidental harm to civilians and damage to civilian objects when carrying out an attack apply to those operations that qualify as 'attacks' as defined in IHL. The question of how widely or narrowly the notion of 'attack' is interpreted regarding cyber operations is, therefore, essential for the applicability of these rules and the protection they afford to civilians and civilian infrastructure.

Article 49 of the 1977 Additional Protocol I defines attacks as "acts of violence against the adversary, whether in offence or in defence". It is well established that the notion of violence in this definition can refer to either the means of warfare or their effects, meaning that an operation causing violent effects can qualify as an attack even if the means used to bring about those effects are not violent in itself (30).

It is also widely accepted that cyber operations are expected to cause death, injury, or physical damage constitute attacks under IHL (31). Some states, including Denmark, Finland, New Zealand, Norway, Switzerland, and the US, have clarified that this includes harm due to the foreseeable direct and indirect (or reverberating) effects of an attack (32) (for example, the death of patients in intensive-care units caused by a cyber operation on an electricity network that results in a power outage), a view shared by the ICRC (33).

Beyond this, cyber operations that significantly disrupt essential services without necessarily causing physical damage, such as those that would incapacitate banking or communications networks, constitute one of the most important risks that cyber operations raise for civilians. However, diverging views exist on whether a cyber operation that results in a loss of functionality without causing physical damage qualifies as an attack as defined in IHL.

In the ICRC's view, during an armed conflict, an operation designed to disable a computer, or a computer network constitutes an attack under IHL, whether the object is disabled through kinetic or cyber means. Indeed, if the notion of attack is interpreted as only referring to operations that cause death, injury, or physical damage, a cyber operation that is directed at making a civilian network (such as electricity, banking, or communications) dysfunctional, or is expected to cause such effects incidentally might not

be covered by essential IHL rules protecting the civilian population and civilian objects. Such an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the IHL rules on the conduct of hostilities (34).

Because cyber operations can significantly disrupt essential services without necessarily causing physical damage, this question constitutes one of the most critical debates for the protection of civilians against the effects of cyber operations. For the moment, opinions vary amongst the states that have taken public positions. States that subscribe to the broader view, which includes loss of functionality under the notion of 'attack', include Ecuador, France, Germany, Guatemala, Italy, Japan, and New Zealand (35). States that take the narrower view that requires physical damage include Denmark, Israel and Peru (36).

Finally, IHL remains relevant also to those cyber operations that do not qualify as 'attacks'. On the one hand, some rules apply to a broader range of conduct described in IHL as 'military operations'. This is the case, for example, with the obligation that "[i]n the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects" (37). This obligation requires all those involved in military operations to continuously bear in mind the effects of military operations on the civilian population, civilians and civilian objects, to take steps to reduce such effects as much as possible, and to seek to avoid any unnecessary effects (38). Its applicability to cyber operations has been expressly reaffirmed by several states including Finland, France and Germany (39).

On the other hand, some IHL rules afford specific protection to certain categories of persons and objects that goes beyond the protection against attacks (40). For example, IHL specifically makes it illegal "to attack, destroy, remove, or render useless objects indispensable to the survival of the civilian population" (41). The explicit mention of 'rendering useless' must be understood as covering a broader range of operations that may impact these goods, beyond attacks or destruction (42). Accordingly, cyber operations that are designed, or can be expected, to disable indispensable objects (such as drinking water installations) are prohibited, irrespective of whether they qualify as attacks. IHL also requires respecting and protecting medical and humanitarian personnel and facilities, a protection that goes beyond the protection against attack (43), as does the obligation to take constant care in the conduct of military operations (44).

The protection afforded to civilian electronic data under IHL

Essential civilian data—such as medical, biometric and social security data, tax records, bank accounts, companies' client files, or election lists and records—are an essential component of digitalised societies. Such data are key to the functioning of most aspects of civilian life, be it at the individual or societal level. Deleting or tampering with essential civilian data can quickly bring government services and private businesses to a complete standstill and such operations could, therefore, cause more harm to civilians than the destruction of physical objects.

With regard to data belonging to certain categories of objects that enjoy specific protection under IHL, the protective rules are comprehensive. In particular, the obligations to respect and protect medical facilities (45) and humanitarian relief operations (46) must be understood as extending to medical data belonging to those facilities and data of humanitarian organisations that are essential for their

operations (47). Similarly, deleting or otherwise tampering with data in a manner that renders useless objects indispensable to the survival of the civilian population, such as drinking water installations and irrigation systems, is prohibited (48).

Still, it is important to clarify the extent to which civilian data are protected by the existing general rules on the conduct of hostilities. In particular, the debate has arisen on whether data constitute as objects as understood under IHL, in which case cyber operations against data (such as deleting them) would be notably governed by the principles of distinction, proportionality and precaution, and the protection they afford to civilian objects (49).

Experts hold different views on whether data qualify as objects for the purposes of the IHL rules on the conduct of hostilities. One view, held by most experts involved in the Tallinn Manual process (an influential non-binding study on how international law applies to cyber operations), is that the ordinary meaning of the term 'object' cannot be interpreted as including data because objects are material, visible and tangible (50). Some states, including Denmark, Chile, and Israel also subscribe to this view (51).

By contrast, others have argued that either all or some types of data should be considered as objects under IHL. One view, taken by several states—including Finland, Germany, Norway, and Romania—is that the protection of civilian objects extends to civilian data (52). This implies that all data constitute objects for the purposes of IHL. This interpretation is supported by the 'modern meaning' of the notion of objects in society and by the object and purpose of the relevant IHL rules (53). It is also consistent with the traditional understanding of the notion of 'object' under IHL, which is broader than the ordinary meaning of the word and encompasses also locations and animals (54). Another approach, thus far endorsed by one state (France), is to consider content data as protected under the principle of distinction, leaving to the side whether other types of data (such as code) formally qualify as objects or not (55).

While the question of whether and to what extent civilian data constitute civilian objects remains unresolved, the assertion that deleting or tampering with such essential civilian data would not be prohibited by IHL in today's data-reliant world seems difficult to reconcile with the object and purpose of IHL. Logically, the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them (56). In essence, excluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap.

Military use of cyberspace and the effect on its civilian character

To protect critical civilian infrastructure that relies on cyberspace, it is also crucial to protect the infrastructure of cyberspace itself. The challenge lies, however, in the interconnectedness of civilian and military networks.

Except for some specific military networks, cyberspace is predominantly used for civilian purposes. Furthermore, military networks may rely on civilian cyber infrastructures such as undersea fibre-optic cables, satellites, routers or nodes. Conversely, civilian vehicles, shipping and air traffic controls increasingly rely on navigation satellite systems that may also be used by the armed forces. Civilian logistical supply chains and essential civilian services use the same web and communication networks

through which some military communications pass. In other words, except for certain networks that are specifically dedicated to military use, it is to a large extent impossible to differentiate between purely civilian and purely military cyber infrastructures (57).

Under IHL, attacks must be strictly limited to military objectives. In so far as objects are concerned, military objectives are limited to those objects, which by their nature, location, purpose or use, make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage (58). All objects that are not military objectives under this definition are civilian objects under IHL and must not be made the object of an attack or reprisals (59). In case of doubt as to whether an object that is normally dedicated to civilian purposes is being used to make an effective contribution to military action, it must be presumed to remain protected as a civilian object (60).

It is traditionally understood that an object may become a military objective when its use for military purposes is such that it fulfils the definition of a military objective even if it is simultaneously used for civilian purposes (such objects are sometimes referred to as 'dual-use objects') (61). However, a wide interpretation of this rule could lead to the conclusion that many objects forming part of cyberspace infrastructure would constitute military objectives and would therefore not be protected against attack, whether cyber or kinetic. This would be a matter of serious concern because of the ever-increasing civilian reliance on cyberspace (62).

The applicable rules provide some important safeguards in this respect. Firstly, IHL requires that the target's destruction or neutralisation must offer a "definite military advantage" in the circumstances ruling at the time (63). However, because cyberspace is designed with a high level of redundancy, one of its characteristics is the ability to immediately reroute data traffic. This inbuilt resilience must be considered by those who are planning or deciding upon an attack (64) If, because of this resilience, a given cyber operation was expected to only offer "potential or indeterminate advantages" to the attacker (65) its target would remain a civilian object, and thus protected from attack (66).

Secondly, even if certain parts of cyberspace infrastructure qualify as military objectives during armed conflicts, any attack against them remains governed by the prohibition of indiscriminate attacks (67), and the rules of proportionality (68) and precaution in attacks (69). Precisely because civilian and military networks are often highly interconnected, assessing the expected incidental civilian harm of any cyber operation is critical to ensuring that the civilian population is protected against its effects (70). For example, attacks against root servers or submarine data cables would raise concerns under the prohibition of indiscriminate attacks because of the difficulty of limiting the effects of such attacks, as required by IHL (71).

Conclusion

This essay has provided an overview of some of the rules that apply to, and thus limit, the use of cyber operations during armed conflicts. It has also shown that certain legal questions—such as the exact interpretation of the IHL notions of attacks and objects—remain unsettled for the time being. It should thus be welcomed that states have started issuing national positions on the application and interpretation

of international law, including IHL, to cyber operations. After all, only if states make their views known will it be possible to assess whether the law, as applied and interpreted in the cyber context, sufficiently addresses the humanitarian concerns associated with the use of cyber operations.

This is the case irrespective of whether a given state is developing military cyber capabilities or whether it is, or expects to be, involved in armed conflicts. All states must ensure respect for IHL and, therefore, they all share the interest in maintaining this body of law effective and able to respond to modern challenges. In addition, from a more pragmatic perspective, the interconnectivity of cyberspace means that the effects of cyber operations conducted by some states during armed conflicts may well cause harm to civilians and civilian populations in otherwise uninvolved states located on the other side of the globe, which, therefore, have an interest that the protections that IHL affords are upheld with regard to cyber operations.

Therefore, the present circumstances pose a prime opportunity for states who have not yet issued such national positions to consider doing so. At the time of writing, only around 20 such positions have been published worldwide (72), which means that new ones not only contribute to the consolidation of international law in the area, but they may also influence other states both at the regional and the global level (73) In our view, any such new statements should reaffirm the applicability of IHL to the use of cyber operations during an armed conflict—recalling that doing so does not legitimise conflict nor encourage militarisation—and then address the key interpretive challenges posed by the development of cyber capabilities.

Overall, the development of such positions should be informed by an in-depth understanding of the relevant technological developments, the potential human cost they may cause, and the protection afforded by existing law. In this respect, interpretations of IHL with regard to novel issues must not decrease the level of protection developed in traditional contexts. Instead, states and international organisations should be guided by the object and purpose of this body of law, i.e., to restrict the use of means and methods of warfare to protect civilians and civilian objects against the effects of hostilities. In the cyber context, that includes interpreting the law to preserve civilian infrastructure from significant disruption and protect civilian data.

Endnotes

(1) United Nations General Assembly, *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/75/816 (New York: United Nations, 2021), para. 16, https://undocs.org/en/A/75/816.

(2) Kubo Mačák and Ewan Lawson, "Avoiding civilian harm during military cyber operations: six key takeaways," Humanitarian Law and Policy Blog, posted June 15, 2021, https://blogs.icrc.org/law-and-policy/2021/06/15/avoiding-civilian-harm-military-cyber-operations/.

(3) Although written in our personal capacity, this essay is informed by and builds on previous public positioning by the International Committee of the Red Cross (ICRC) on these matters. See, in particular, International Committee of the Red Cross (ICRC), *International humanitarian law and cyber operations during armed conflicts: ICRC position paper* (Geneva: ICRC, 2019), https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf; see also as Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, "Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts", *International Review of the Red* Cross 102, no. 913 (2020), 287-334, https://doi.org/10.1017/S1816383120000387. The analysis in the present essay was first published as Kubo Mačák and Laurent Gisel, "Grammar: rules in a cyber conflict" in *A Language of Power? Cyber Defence in the European Union,* ed. Patryk Pawlak and François Delerue, *Chaillot Paper* (Paris: European Union Institute for Security Studies, 2022). We would like to thank Julio Veiga-Bezerra for his help with the references.

(4) See e.g. U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms* (Washington: Department of Defense, 2021), 55, https://irp.fas.org/doddir/dod/dictionary.pdf.

(5) See e.g. Russian Federation, Ministry of Defence, "Russian Federation Armed Forces' Information Space Activities Concept", https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle.

(6) ICRC, *International humanitarian law and cyber operations during armed conflicts*, 3, fn 1.

(7) See further "The potential human cost of cyber operations," *International Committee of the Red Cross (ICRC)*, May 29, 2019, https://www.icrc.org/en/document/potential-human-cost-cyber-operations.

(8) Examples include the malware *CrashOverride*, the ransomware *WannaCry*, the wiper program *NotPetya*, and the malware Triton. *CrashOverride* affected the provision of electricity in Ukraine; *WannaCry* affected hospitals in several countries; *NotPetya* affected a very large number of businesses; *Triton* was aimed at disrupting industrial control systems, and was reportedly used in attacks against Saudi Arabian petrochemical plants. For some discussion, see Laurent Gisel and Lukasz Olejnik, "The Potential Human Cost of Cyber Operations: Starting the Conversation," Humanitarian Law and Policy Blog, posed November 14, 2018, https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/.

(9) Sergio Caltagirone, "Industrial Cyber Attacks: A Humanitarian Crisis in the Making," Humanitarian Law and Policy Blog, posted December 3, 2019, https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/.

(10) International Committee of the Red Cross (ICRC), *Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts* (Geneva: ICRC, 2021), 12, https://shop.icrc.org/avoiding-civilian-harm-from-military-cyber-operations-during-armed-conflicts-icrc-expert-meeting-21-22-january-2020-geneva-pdf-en.html.

(11) See International Committee of the Red Cross (ICRC), *International humanitarian law and the challenges of contemporary armed conflicts* (Geneva: ICRC, 2011), 37, https://www.icrc.org/en/doc/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf; Gisel, Rodenhäuser and Dörmann, "Twenty years on", 309-310.

(12) ICRC, *International humanitarian law and cyber operations during armed conflicts*, 8.

(13) Peter Maurer, "Developing a New Humanitarian Response in the Area of Cyberspace", in *Our Common Digital Future*, ed. Samir Saran (New Delhi: Observer Research Foundation, 2017), 30-35, 33, https://www.orfonline.org/wp-content/uploads/2017/11/Our-Common-Digital-Future.pdf.

(14) United Nations General Assembly, *Report of the Open-ended Working Group*, para. 34.

(15) United Nations General Assembly, *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security*, UN Doc. A/76/135 (New York: United Nations, 2021), para. 71(f).

(16) United Nations General Assembly, *Report of the Open-ended Working Group*, para. 71(f).

(17) See, e.g., Michael Schmitt, "The Sixth United Nations GGE and International Law in Cyberspace", *Just Security*, June 10, 2021, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/; Adina Ponta, "Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes", *ASIL Insight*, July 30, 2021, https://www.asil.org/insights/volume/25/issue/14; Anna-Maria Osula, "In search of a coherent international approach to governing technologies", *ORF Digital Frontiers*, October 17, 2021, https://www.orfonline.org/expert-speak/international-approach-to-governing-technologies/.

(18) International Committee of the Red Cross (ICRC), *International humanitarian law and the challenges of contemporary armed conflicts* (Geneva: ICRC, 2015), 40, https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf; see also Michael N. Schmitt and Liis Vihul, eds, *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), rule 80.

(19) See e.g. Council of the European Union, *Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy joint communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 11357/13 (Brussels: EU, 2013), para. 6, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/137602.pdf; NATO, *Wales Summit Declaration (issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales)* (Brussels: NATO, 2014), para. 72, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

(20) See e.g. the submissions of China, Cuba, Iran, Nicaragua, or Russia on the Initial "Pre-draft" of the United Nations General Assembly, *Report of the Open-ended Working Group*, www.un.org/disarmament/open-ended-working-group/.

(21) ICRC, *International humanitarian law and cyber operations during armed conflicts*, 4-5.

(22) United Nations General Assembly, *Report of the Group of Governmental Experts*, para. 71(f) in fine noting that 'recalling [IHL] principles by no means legitimizes or encourages conflict'.

(23) For example, IHL prohibits the development of cyber capabilities that would qualify as weapons and would be indiscriminate by nature or would be of a nature to cause superfluous injury or unnecessary suffering. See e.g. Jean-Marie Henckaerts and Louise Doswald-Beck, eds, *Customary International Humanitarian Law, Vol. 1: Rules* (Cambridge: Cambridge University Press, 2005), rules 70-71, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul.

(24) "Charter of the United Nations," adopted October 24, 1945, *United Nations Treaty Series* XVI, art. 2(4), https://www.un.org/en/about-us/un-charter/full-text.

(25) "Charter of the United Nations," arts 2(3) and 33.

(26) United Nations General Assembly, *Report of the Open-ended Working Group*, para. 35; United Nations, General Assembly *Report of the Group of Governmental Experts*, para. 70.

(27) United Nations General Assembly, *Report of the Group of Governmental Experts*, para. 71.

(28) For further analysis of the relationship between international law and military cyber operations, see Kubo Mačák, "Unblurring the lines: military cyber operations and international law", *Journal of Cyber Policy 6*, no. 3 (2021), 411-428, https://doi.org/10.1080/23738871.2021.2014919.

(29) The notion of attack under IHL, defined in Art. 49 of the 1977 First Additional Protocol, is different from and should not be confused with the notion of 'armed attack' under art. 51 of the UN Charter, which belongs to the realm of *jus ad bellum*. To affirm that a specific cyber operation, or a type of cyber operations, amounts to an attack under IHL does not necessarily mean that it would qualify as an armed attack under the UN Charter.

(30) Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians", *International Review of the Red Cross 94*, no. 886 (2012), 557, https://international-review.icrc.org/articles/get-my-cloud-cyber-warfare-international-humanitarian-law-and-protection-civilians; William H. Boothby, *The Law of Targeting* (Oxford: Oxford University Press, 2012), 384; Gisel, Rodenhäuser and Dörmann, supra note 2, 312.

(31) ICRC, *International humanitarian law and the challenges of contemporary armed conflicts,* (2015), 41-42, https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf; Schmitt and Vihul, *Tallinn Manual 2.0*, rule 92.

(32) Danish Ministry of Defence and Defence Command Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations* (Copenhagen: Defence Command Denmark, 2016), 677 (when discussing computer network attacks); Finland, Ministry of Foreign Affairs, *International law and cyberspace: Finland's national positions* (2020), 7; New Zealand Defence Force, *Manual of Armed Forces Law Vol. 4* (2017), para. 8.10.22; Norway, *Manual i krigens folkerett* (2013), para. 9.54; Switzerland, Federal Department of Foreign Affairs (FDFF), *Switzerland's position paper on the application of international law in*

cyberspace: Annex UN GGE 2019/2021 (Bern: FDFF, 2021), 10; United States, *United States Submission to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2014–15),* 6; and from a practical perspective U.S. Department of Defense, *Joint Publication 3-12 (R): Cyberspace operations* (Washington: Department of Defense, 2013), IV-4.

(33) ICRC, *International humanitarian law and cyber operations during armed conflicts*, 7.

(34) ICRC, *International humanitarian law and cyber operations during armed conflicts*, 7-8; for more details, see Gisel, Rodenhäuser and Dörmann, "Twenty years on", 312-316.

(35) Ecuador, *Verbal Note 4-2 186/2019 from the Permanent Mission of Ecuador to the OAS* (June 28, 2019), quoted in Organization of American States (OAS), *Improving Transparency: International Law and State Cyber Operations: Fifth Report*, OAS Doc. CJI/doc. 615/20 rev.1 (Washington: OAS, 2020), para. 32; France, Ministry of the Armies, *International Law Applied to Operations in Cyberspace* (2019), 13; Germany, *On the Application of International Law in Cyberspace Position Paper* (2021), 9; Guatemala, *Note Of. 4VM.200-2019/GJL/lr/bm, from Mr. Gabriel Juárez Lucas, Fourth Vice Minister of the Interior Ministry of the Republic of Guatemala to Luis Toro Utillano, Technical Secretariat, Inter-American Juridical Committee* (June 14, 2019), quoted in OAS, *Improving Transparency*, para. 32; Italy, *Italian Position Paper on 'International Law and Cyberspace'* (2021), 9-10; Japan, Ministry of Foreign Affairs, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations* (2021), 7; New Zealand, *The Application of International Law to State Activity in Cyberspace* (December 1, 2020), para. 25.

(36) Danish Ministry of Defence and Defence Command Denmark, *Military Manual on International Law*, 290-291; Roy Schöndorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies* 97 (2021), 395-406, at 400; Peru, *Response Submitted by Peru to the Questionnaire on the Application of International Law in OAS Member States in the Cyber Context* (2019), quoted in OAS, *Improving Transparency*, para. 32.

(37) "Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts" (Protocol Additional I), June 8, 1977, *United Nations Treaty Series* 3, art. 57(1); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, rule 15.

(38) See e.g. United Kingdom, Ministry of Defence, *The Joint Service Manual of the Law of Armed Conflict* (London: Minister of Defence, 2004), para. 5.32.1; Schmitt and Vihul, *Tallinn Manual 2.0*, para. 4 of the commentary on rule 114; Stefan Oeter, "Methods of Combat", in *The Handbook of International Humanitarian Law*, ed. Dieter Fleck (Oxford: Oxford University Press, 2021), 215; Noam Neuman, "A Precautionary Tale: The Theory and Practice of Precautions in Attack", *Israel Yearbook on Human Rights* 48 (2018), 28-29.

(39) Finland, Ministry of Foreign Affairs, *International law and cyberspace*, 7; France, Ministry of the Armies, *International Law Applied to Operations in Cyberspace*, 15; Germany, *On the Application of International Law in Cyberspace*, 9.

(40) See Gisel, Rodenhäuser and Dörmann, "Twenty years on", 322-329; see also Switzerland, Federal Department of Foreign Affairs (FDFF), *Switzerland's position* paper, 10.

(41) "Additional Protocol I", art. 54(2); Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Additional Protocol II), June 8, 1977, *United Nations Treaty Series* 609, art. 14; Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, rule 54.

(42) Gisel, Rodenhäuser and Dörmann, "Twenty years on", 327; Schmitt and Vihul, *Tallinn Manual 2.0*, para. 6 of the commentary on rule 141.

(43) Gisel, Rodenhäuser and Dörmann, "Twenty years on", 328-329; Schmitt and Vihul, *Tallinn Manual 2.0*, para. 5 of the commentary on rule 131; see also Tilman Rodenhäuser, "Hacking Humanitarians? IHL and the protection of humanitarian organizations against cyber operations," *EJIL: Talk!*, March 16, 2020, https://www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/; Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser, "Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?," *Just Security*, March 27, 2020, https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/.

(44) Gisel, Rodenhäuser and Dörmann, "Twenty years on", 323-324; Schmitt and Vihul, *Tallinn Manual 2.0*, rule 114.

(45) See, for instance, "Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field", August 12, 1949, *United Nations Treaty Series* 31, art. 19; "Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea", August 12, 1949, *United Nations Treaty Series* 85, art. 12; "Geneva Convention (IV) relative to the

Protection of Civilian Persons in Time of War", August 12, 1949, *United Nations Treaty Series* 287, art. 18; "Additional Protocol I", art. 12; "Additional Protocol II", art. 11; Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, rules 25, 28 and 29.

(46) See e.g. "Additional Protocol I", arts 70(4 and 71(2); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, rules 31-32.

(47) See Gisel, Rodenhäuser and Dörmann, "Twenty years on", 327-328; Schmitt and Vihul, *Tallinn Manual 2.0*, para. 3 of the commentary on rule 132.

(48) AP I, Art. 54; AP II, Art. 14; Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, rule 54.

(49) See also Mačák, "Unblurring the lines", 421-422.

(50) See Schmitt and Vihul, *Tallinn Manual 2.0*, para. 6 of the commentary on rule 100. The experts relied on the 1987 ICRC Commentary which notes that objects are material, visible and tangible; this explanation in the Commentary however, aimed at distinguishing objects from concepts such as 'aim' or 'purpose', not at differentiating between tangible and intangible goods, and therefore cannot be seen as determinative for the debate on data (see Gisel, Rodenhäuser and Dörmann, "Twenty years on", 318).

(51) Danish Ministry of Defence and Defence Command Denmark, *Military Manual on International Law*, 292; Chile, *Response submitted by Chile to the OAS Inter-American Juridical Committee Questionnaire* (January 14, 2020), quoted in OAS, (OAS), *Improving Transparency*, para. 36; Schöndorf, "Israel's Perspective on Key Legal and Practical Issues," 401.

(52) Finland, *International law and cyberspace*, 7; Germany, *On the Application of International Law in Cyberspace*, 8; Norway, *Manual i krigens folkerett*, para. 9.58; Romania, "National contribution on the subject of how international law applies to the use of information and communications technologies by States" in United Nations, General Assembly, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266*, UN Doc. A/76/136 (New York: United Nations, 2021), 78.

(53) Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law," *Israel Law Review 48*, no. 1 (2015), 55-80, 80, https://doi.org/10.1017/S0021223714000260; see also Robert McLaughlin, "Data as a Military Objective," *Australian Outlook, Australian Institute of International Affairs*, September 20, 2018, http://www.internationalaffairs.org.au/australianoutlook/data-as-a-military-objective/.

(54) Gisel, Rodenhäuser and Dörmann, "Twenty years on," 319.

(55) France, Ministry of the Armies, *International Law Applied to Operations in Cyberspace*, 14. For the view that, conversely, operational-level data (i.e., code) may qualify as an object, see Heather Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives," *Israel Law Review 48*, no. 1 (2015), 39-54, https://doi.org/10.1017/S0021223714000272.

(56) International Committee of the Red Cross (ICRC), *International humanitarian law and the challenges of contemporary armed conflicts* (Geneva: ICRC, 2019), 28, https://shop.icrc.org/international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts-recommitting-to-protection-in-armed-conflict-on-the-70th-anniversary-of-the-geneva-conventions-pdf-en.

(57) Gisel, Rodenhäuser and Dörmann, "Twenty years on", 320-322.

(58) "Additional Protocol I," art. 52(2); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, rules 7-8.

(59) "Additional Protocol I," art. 52(1); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, rule 9.

(60) "Additional Protocol I," art. 52(3); "Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices, as amended on May 3, 1996" (Protocol II), art. 3(8)(a); see also Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, 35-36 (rule 10).

(61) See e.g. Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, 32 (rule 10); Schmitt and Vihul, *Tallinn Manual 2.0*, para. 1 of the commentary on rule 101.

(62) Gisel, Rodenhäuser and Dörmann, "Twenty years on," 321.

(63) "Additional Protocol I", art. 52(2); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, rule 8.

(64) ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 42.

(65) Yves Sandoz, Christophe Swinarski and Bruno Zimmerman, eds, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, (Geneva: ICRC, 1987), 636, para. 2024 ("it is not legitimate to launch an attack which only offers potential or indeterminate advantages").

(66) Gisel, Rodenhäuser and Dörmann, "Twenty years on", 321.

(67) "Additional Protocol I," art. 51(4); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, rules 11-12.

(68) "Additional Protocol I," arts 51(5)(b) and 57; Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, rule 14.

(69) "Additional Protocol I," art. 57; Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, rules 15-21.

(70) See ICRC, *International humanitarian law and cyber operations during armed conflicts*, 7.

(71) "Additional Protocol I," art. 51(4)(c); Henckaerts and Doswald-Beck, *Customary International Humanitarian Law*, rule 12(c).

(72) For a full overview, see Cyber Law Toolkit, "National positions", https://cyberlaw.ccdcoe.org/wiki/Category:National_position.

(73) See Kubo Mačák, "From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers," *Leiden Journal of International Law 30*, no. 4, 877-899, 896-898, https://doi.org/10.1017/S0922156517000358.

Lawfare in China's Hybrid Warfare Against Taiwan

Jyun-yi Lee

Since Russia's annexation of Crimea in 2014, discussions on hybrid warfare have intensified. Proponents maintain that future conflict will be mostly hybrid in nature. To achieve their political goals, state and non-state actors are inclined to blend the conventional and unconventional, physical and psychological, and the kinetic and non-kinetic means of warfare to target their opponent's combatants and citizens. Most of these means of warfare may not be entirely new, except digital or cyber, but it is their "convergence" that defines the hybridity of future conflicts (1). In contrast, critics contend that war has always been hybrid in nature, so hybrid warfare and other associated terms do not advance our understanding of war and peace and could lead to a false perception that a state unnecessarily sees itself constantly at war (2).

Although its analytical utility is contested, hybrid warfare remains a useful concept by stressing the synchronised application of various means and highlighting the synergistic effects thereby generated (3). This is particularly important insofar as peace and stability in the Taiwan Strait is concerned. With the balance of power between the US and China gradually tipping in favour of the latter and Chinese external behaviour becoming more assertive under Xi Jinping's leadership, Taiwan has been described as "the most dangerous place on earth (4)." China has not gained absolute military superiority in its rivalry with the US thus far, and Taiwan's effort in bolstering its own defence also renders conventional warfare with China difficult, although not impossible. Therefore, it is reasonable that China will deploy various instruments to construct an environment conducive to achieving its goal of unification and conduct hybrid warfare when launching an armed attack against Taiwan.

This essay discusses the role of lawfare in China's hybrid warfare. Law, or rather the instrumental use of law, gives the Chinese leadership the legitimacy to use force against Taiwan. This is further complicated by other instruments in the hybrid warfare toolbox. Modern technology addresses the current limits of China's capability to threaten and ultimately conquer Taiwan and blurs the line between peace and war, posing difficulties for Taiwan and other stakeholders to react and respond effectively. Legal resilience,

in this context, is an effort to limit China's discourse of *jus ad bellum*, or the grounds on which it may resort to the use of force (5).

Lawfare and China's Jus Ad Bellum Claims

The unification of Taiwan and China is a political objective for Beijing. If the use of force to achieve this goal is considered legitimate, the demands of nationalism will be met. Such legitimacy also reduces the likelihood of foreign intervention and lowers the degree of Taiwan's resistance. As the law is the primary resource for legitimacy, it becomes a crucial instrument for China to define cross-Strait relations, constitute specific "facts" about Taiwan, and grant itself rights and justifications for actions on Taiwan (6).

Lawfare defined as "the strategy of using—or misusing—law as a substitute for traditional military means to achieve a warfighting objective (7)," is a key component in China's playbook. While China does not use the term hybrid warfare, lawfare or legal warfare (*falu zhan*) is one of its "three warfares" (*san zhan*) alongside public opinion warfare and psychological warfare. The "three warfares" was first codified by the People's Liberation Army (PLA) in 2003 as part of its political work. Lawfare involves "arguing that one's own side is obeying the law, criticising the other side for violating the law, and making arguments for one's own side in cases where there are also violations of the law (8)." The instruments leveraged include national laws and the full range of legal instruments such as legislation, judicial law, legal pronouncements, law enforcement, and legal education (9). With China's external behaviour becoming more assertive, if not aggressive, since Xi's ascension, international law has also become an instrument.

China's exploitations of the law to justify a possible military assault against Taiwan is particularly evident in two instances. First, in its March 2005 Anti-Secession Law, China unilaterally defines three conditions under which "non-peaceful means" may be utilised (10). Article 8 of the Anti-Secession Law stipulates that "secessionist forces ... cause the fact of Taiwan's secession from China," that "major incidents entailing Taiwan's secession" occur, or that "possibilities for peaceful reunification" are exhausted will justify "non-peaceful means and other necessary measures." It is worth noting that the three conditions are left ambiguous. This ambiguity affords Beijing the freedom to decide whether a situation or incident crosses the red line. It not only gives China policy flexibility but also aims to deter Taiwan from undertaking actions considered provocative by Beijing.

The US Pentagon has identified six scenarios that may trigger China's Anti-Secession Law (11):

1. Formal declaration of Taiwan independence;
2. Undefined moves toward Taiwan independence;
3. Internal unrest in Taiwan;
4. Taiwan's acquisition of nuclear weapons;
5. Indefinite delays in the resumption of cross-Strait dialogue on unification;
6. Foreign military intervention in Taiwan's internal affairs.

From the perspective of hybrid threats (the combination of various means of threats short of the use of force), the third scenario is particularly worrisome. This is, arguably, the only scenario under which China has the will and capability to bring about a change in Taiwan. This can be achieved by exploiting divisions or cleavage within Taiwan. Should this happen, China may use force against Taiwan to restore law and order upon the request of some Taiwanese people.

A second example concerns China's efforts to advance in the international arena using its discourse of jus ad bellum. In April 2022, Xi proposed a Global Security Initiative (GSI) in his opening speech at the Boao Forum (12). The GSI consists of six "commitments":

1. The vision of common, comprehensive, cooperative, and sustainable security, and work together to maintain world peace and security.
2. Respecting the sovereignty and territorial integrity of all countries, upholding non-interference in internal affairs, and respecting the independent choices of development paths and social systems made by people in different countries.
3. Abiding by the purposes and principles of the UN Charter, rejecting the Cold War mentality, oppose unilateralism, and saying no to group politics and bloc confrontation.
4. Taking the legitimate security concerns of all countries seriously, upholding the principle of indivisible security, building a balanced, effective and sustainable security architecture, and opposing the pursuit of one's own security at the cost of others' security.
5. Peacefully resolving differences and disputes between countries through dialogue and consultation, supporting all efforts conducive to the peaceful settlement of crises, rejecting double standards, and opposing the wanton use of unilateral sanctions and long-arm jurisdiction.
6. Maintaining security in both traditional and non-traditional domains, and working together on regional disputes and global challenges such as terrorism, climate change, cybersecurity and biosecurity.

In essence, the GSI argues that peace and security is a common good for all states (commitments one and six). To achieve this, mutual respect is key (commitments two and four), which is enshrined in the UN Charter (commitment three) and supported by international norms (commitment five). While there is ostensibly nothing wrong with this argument, the GSI neglects the ways in which irreconcilable claims and interests should be addressed. Consider China's sovereign claim over Taiwan and Russia's so-called "legitimate security concerns" about Ukraine. Chinese and Russian views are certainly not acceptable for Taiwan and Ukraine, respectively. These differences can never be resolved through "mutual respect" or "dialogue and consultation" (commitments two and four). Additionally, existing US-led security arrangements in the Indo-Pacific and Europe are reduced by the GSI to nothing but "Cold War mentality," "group politics", and "bloc confrontation". The only option left for countries seems to be the United Nations (UN), where both China and Russia can veto any unfavourable resolution in the UN Security Council. In other words, if China opts to use force against its neighbouring countries in the name of "sovereignty and territorial integrity," then, according to the discourse of the GSI, there would be no effective way to deter or dissuade Beijing. It can, therefore, be inferred that the GSI seeks to promote "sovereignty and territorial integrity" and "legitimate security concerns" as causes for jus ad bellum.

Technology in China's Hybrid Warfare Against Taiwan

The instrumental use of law mainly serves China in justifying its employment of military force, but this says nothing about whether and how military force is used. Given that the Chinese Communist Party (CCP) under Xi has asserted that "the long-standing political differences between the two sides [of the Taiwan Strait]" should not be "passed down from one generation to the next (13)," it is likely that China will not just draw certain redlines warning Taiwan not to cross or waiting for it to cross but may actively seek to create conditions for waging a war against Taiwan. In addition to works that analyse what China's invasion of Taiwan may look like (14), China's own propaganda also provides clues to its aspirations in terms of war scenarios as well as the role of technology in modern warfare.

In 2021, a magazine published by the Chinese Society of Naval Architects and Marine Engineers released an animated video simulating a military attack on Taiwan to mark the CCP's centenary. The video suggested that the attack will consist of three stages. In the first stage, ballistic missile attacks will destroy strategic spots such as airports, early warning radar, anti-air missile bases, and command centres. Naval ports would not be destroyed, but temporarily suspended for the PLA to use later. The attacks at this stage would last until the PLA's surface troops had accomplished an assault landing. The second stage would be several rounds of intensive cruise missile attacks, launched from land, ships and submarines, and targeting military bases, ammunition depots, communications infrastructure, and key road junctions. The final stage would consist of artillery strikes from surface ships and land-based rocket forces to remove any remaining obstacles for the PLA's marine corps and amphibious landing troops (15).

The video did not mention possible counterattacks or responses from other stakeholders such as the US and Japan (16). It further depicted Taiwan as being unable to undertake meaningful counterattacks. Most commentators, therefore, dismissed the video as Chinese propaganda. While this is certainly the case, the absence of reactions from the US, Japan, and Taiwan may also be thought of as a result of the PLA's strategy. In other words, technology may well be used to enable the PLA to launch successful attacks against Taiwan. By pushing Taiwan and others into a difficult position to react and counterstrike, China can pose challenges to Taiwan's decision-making.

According to a study published by the NATO Cooperative Cyber Defence Centre of Excellence, cyber technology may be used in four types of scenarios to render (cyber) warfare more effective and cause legal confusion (17). First, technology may serve as an enabler for traditional kinetic attacks. For instance, the Israeli air strike on a construction site at Tall al-Abyad, Syria, on 6 September 2007 (18). An airborne network attack system may have been deployed to allow the attackers to "invade communications networks, see what enemy sensors see and even take over as systems administrator so sensors can be manipulated…so that approaching aircraft can't be seen (19)." In the aforementioned video, Taiwan witnessed its strategic assets being destroyed by Chinese air strikes without realising their coming might be considered the work of this kind of cyber espionage and/or other forms of electronic warfare. The legal challenges in this regard include the difficulty in attribution and the indefinite nature of the threats. Copying what enemy sensors see may be an act of cyber espionage below the threshold of use of force. But once the intruder takes over as systems administrator, this may indicate an armed attack is imminent or be an integral part of an actual armed attack.

Second, technology may be a contributing factor in the context of hybrid warfare. Technology would either be a multiplier, or its effects would be multiplied by any other contributing factor(s) (20). The actual damage caused by PLA air strikes and its psychological impacts on Taiwan society will be multiplied if cyberattacks on Taiwan's critical infrastructure and disinformation campaigns occurred simultaneously.

Third, technology might be leveraged to degrade or deny decision-making and associated command and control capabilities, and/or achieve information superiority in the field of strategic communication. Before the armed conflict broke out in Georgia in August 2008, it was reported that a "short occasion of turbulence" occurred in July, which was believed to "have reduced Georgian decision-making capability, as well as its ability to communicate with allies, thereby possibly impairing the operational flexibility of Georgian forces (21)." This cyber operation was not a prerequisite for the armed conflict, and was not considered a factor that multiplied the effects of the conflict. Therefore, the operation functioned neither as an enabler nor as a multiplier. Given that it was not taken as a sustaining activity either, it must be classified as playing a supportive role. In the context of Taiwan, the sabotage of communication systems such as satellites and undersea cables by unknown causes and before a contingency erupts may be an example in this regard. Such an event or incident can result in the disruption of Taiwan's command and control system. In such a scenario, it will be difficult for the Taiwanese government to establish a causal relationship between the incident and the armed attack, let alone determine when or whether it is at war before the kinetic attack takes place.

The fourth scenario concerns the use of technologies on their own. The attack on energy grids by cyber or electronic means, large-scale cyberattacks, disruption of critical social functions, disinformation, and associated cognitive warfare are examples. The video of the simulated attack did not include these types of threats, probably because it was designated as a showcase of a PLA military attack. But if one or more of these hostile operations take place in the real world, they will aim at creating "internal unrest in Taiwan," which provides China with a cause to intervene. Such kinds of operations will also make it difficult for the Taiwanese government to determine whether a military operation will follow. As such attacks are executed below the threshold of an armed attack and largely target civilian objects, they pose the biggest policy challenges to the government among the four scenarios of cyber technology use in warfare.

In sum, the threat posed by the interplay of China's lawfare and technological warfare against Taiwan has been growing. China seeks to confine Taiwan's political development by enacting domestic laws, including the Anti-Secession Law. The Anti-Secession Law establishes that to preserve China's "sovereignty and territorial integrity" it is necessary to oppose and check the so-called Taiwan independence activities. Jus ad bellum claims are made that give the Chinese authority the right to determine whether an act by or event in Taiwan constitutes an instance of Taiwanese independence and legitimise China's possible use of force against it. The jus ad bellum arguments based on the notion of "sovereignty and territorial integrity" are subsequently extended to the international arena. This is reflected in, among others, the GSI. It can be argued that the ground on which to justify the use of force against Taiwan has been laid. What is left is for China's claims to be accepted by most members of the international community.

Consequently, it is imperative to think of what future conflicts or warfare across the Taiwan Strait may look like. The simulated attack video did not show any possible reactions from the US and its allies in the event of a PLA military attack, and Taiwan was depicted as barely able to organise an effective counterstrike. Whether as an enabler, multiplier or supporter, technology can be applied in cyber espionage, cyber warfare, disinformation, electronic warfare, and so on, to facilitate the PLA's kinetic offense capabilities in the future. Such threats by themselves can interrupt important social functions and lead to "an internal unrest" that could lead to a PLA military operation across the Strait. Importantly, China can further blur the line between peace and war through the use of technology, thus creating difficulties in Taiwan's decision-making process.

Legal Resilience: Addressing the Root Cause of China's Hybrid Warfare

To achieve the political goal of taking over Taiwan, China must first construct a claim. For China, "sovereignty and territorial integrity" constitutes jus ad bellum through the making of domestic law., and it then seeks to advance this claim in the international arena. This view is not in line with the current international legal order. Article 2(4) of the UN Charter makes a general prohibition on the threat of or use of force by states. The only two exceptions include self-defence from an armed attack and actions authorised by the Security Council to restore international peace and security. In this regard, the idea that preserving "sovereignty and territorial integrity" justifies the use of force not only serves China's interest but is also an attempt to reshape the legal order. While some may argue that since many countries accept or acknowledge China's claim over Taiwan the UN Charter is not applicable to it, allowing China to advance this discourse will likely have spillover effects, with China using the same argument in its territorial disputes with other countries.

Consequently, it is crucial to strengthen the resilience of the current international legal order. Legal resilience refers to the ability of a legal system to resist change and its capacity to adapt in response to disturbances (22). With respect to the former, democratic countries must contest China's claim by taking part in the interpretation of international law. Russian Foreign Minister Sergey Lavrov has frequently criticised "the trend of…Western partners to make fewer references to international law or even remove it from the international lexicon altogether (23)." His words suggest that if the legal and moral ground that the democratic world helped build and once dominated is left unchecked, then countries like Russia and China will seize it. Democratic countries must, therefore, refer to, confer with, and abide by international law. They must also frequently and publicly express explicit disagreements with China's interpretation.

Democratic countries must pay greater attention, individually and collectively, to the legal consequences various forms of hybrid warfare bring about. This itself would signal that China's tactics are noticed and called out. While this may not be sufficient to deter China from acting, it may reduce the likelihood of such instances. Taiwan and other countries should also discuss legal responses in different scenarios while considering the possible internal and external public opinions that may arise.

Endnotes

(1) Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Forces Quarterly* 52, no. 1 (2009), 34–39; Gregory F. Treverton et al., *Addressing Hybrid Threats* (Stockholm: Swedish Defence University, 2018).

(2) Donald Stoker Craig Whiteside, "Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking," *Naval War College Review* 73, no.1 (2020), https://digital-commons.usnwc.edu/nwc-review/vol73/iss1/4/.

(3) Robert Johnson, "Hybrid War and Its Countermeasures: A Critique of the Literature," *Small Wars & Insurgencies* 29, no. 1 (2018), p. 158.

(4) "The most dangerous place on Earth," *The Economist*, May 1, 2021, https://www.economist.com/leaders/2021/05/01/the-most-dangerous-place-on-earth.

(5) Carsten Stahn, "'*Jus ad bellum', 'jus in bello'. . . 'jus post bellum'*? –Rethinking the Conception of the Law of Armed Force," *European Journal of International Law*, Vol. 17, no, 5 (Nov. 2006), pp. 921-943.

(6) Lyle J. Morris, et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: RAND Corporation, 2019), pp. 9-10.

(7) Charles J. Dunlap, Jr., "Lawfare Today… and Tomorrow," *International Law Studies Series* 87 (2011), p. 315.

(8) Han Yanrong, "Legal Warfare: Military Legal Work's High Ground: An Interview with Chinese Politics and Law University Military Legal Research Center Special Researcher Xun Dandong," Legal Daily (PRC), February 12, 2006. Cited from Dean Cheng, "Winning Without Fighting: Chinese Legal Warfare," Heritage Foundation Backgrounder No. 2692, May 21, 2012, https://www.heritage.org/asia/report/winning-without-fighting-chinese-legal-warfare.

(9) Dean Cheng, "Winning Without Fighting: Chinese Legal Warfare."

(10) National People's Congress, Government of the People's Republic of China, https://www.refworld.org/docid/474403752.html.

(11) Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2021*, Washington D.C.: GPO, 2021, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF, Tom O'Connor, "U.S. No Longer Lists Foreign Troops on Taiwan as Trigger for China Conflict," *Newsweek*, November 3, 2021, https://www.newsweek.com/us-no-longer-lists-foreign-troops-taiwan-trigger-china-conflict-1645729.

(12) Ministry of Foreign Affairs, Government of the People's Republic of China, https://www.fmprc.gov.cn/mfa_eng/topics_665678/kjgzbdfyyq/202205/t20220505_10681820.html

(13) Taiwan Affairs Office, State Council, Government of the People's Republic of China, http://www.gwytb.gov.cn/wyly/201904/t20190412_12155687.htm.

(14) Cf. David Lague and Maryanne Murray, "T-DAY: The Battle for Taiwan," *Reuters*, November 5, 2021, https://www.reuters.com/investigates/special-report/taiwan-china-wargames/, Kori Schake and Allison Schwartz, eds., *Defending Taiwan* (Washington, DC: American Enterprise Institute, 2022), https://www.defendingtaiwan.com/wp-content/uploads/2022/06/BK-Defending-Taiwan-online-final.pdf.

(15) Kristin Huang, "Mainland Chinese magazine outlines how surprise attack on Taiwan could occur," *South China Morning Post*, July 2, 2021, https://www.scmp.com/news/china/military/article/3139460/mainland-chinese-magazine-outlines-how-surprise-attack-taiwan.

(16) Kristin Huang, "Mainland Chinese magazine outlines how surprise attack on Taiwan could occur."

(17) Ulf Häußler, "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty," in Eneken Tikk and Anna-Maria Talihärm, eds., *International Cyber Security Legal & Policy Proceedings 2010* (Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010), pp. 116-122.

(18) David A. Fulghum and Douglas Barrie, "Israel used electronic attack in air strike against Syrian mystery target," *ABC News*, October 8, 2007, https://abcnews.go.com/Technology/story?id=3702807&page=1.

(19) Ulf Häußler, "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty," p. 116.

(20) Ulf Häußler, "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty," p. 118.

(21) Ulf Häußler, "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty," p. 118.

(22) Aurel Sari, "Legal Resilience in an Era of Grey Zone Conflicts and Hybrid Threats," Exeter Centre for International Law Working Paper Series 2019/1, p. 18.

(23) Jorgensen, "The Weaponisation of International Law in Ukraine."

Emerging Technologies and their Impact on National Strategies

Samyak Rai Leekha, Pulkit Mohan,
and Rajeswari Pillai Rajagopalan

Technology has played a critical role in human development and progress, with humans far exceeding their biological potential. However, as the atom bombs of the previous century demonstrated, technology also has the potential to bring enormous destruction and death, especially in warfare. As evidenced by the Russia-Ukraine war, the rise of a new generation of technologies demonstrates the potential to unleash mayhem (1). Therefore, it is critical to globally regulate the flow (where applicable) and use of these technologies to avert any disaster. Amid the rapidly changing geopolitical scenario, technology regulation is a battleground for competition and influence (2). Under this environment, emerging technologies continue to develop in a global policy environment that is struggling to keep pace.

This essay discusses the growth and improvements in technologies, their potential military impacts, and the challenges in regulation. In addition, it suggests that geopolitical competition is the cause for the lack of consensus in developing global regulation for these technologies. Lastly, it provides recommendations to effectively regulate emerging technologies in a war-fighting context. Specific technologies covered in this essay include space, cyber, nuclear, and artificial intelligence (AI), and automation.

Cyber: Brief, Impacts, and Challenges in Regulation

Along with the wide proliferation of the internet, associated security concerns have also grown. Cyber warfare is defined as "actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks" (3). The rise in internet connectivity has meant that the malicious use of

the technology has also increased. In 2021, nearly half of all organisations globally were targeted by cyberattacks (4). The proliferation of internet of things (IoT) technologies also means that such attacks are no longer limited to informational targets and can produce kinetic effects in multiple domains. Cyber-physical attacks on critical infrastructure, including power grids, railroads, hospitals, and airports, have in the past deprived thousands of people of essential services. With increasing interconnections fuelled by IoT, future cyber-physical attacks may result in "cascading crises" involving much higher costs than ever before (5). Additionally, attacks targeting critical infrastructure and supply chains have grown twofold in the past two years (6).

States have similarly leveraged this technology in pursuit of strategic objectives. The US had allegedly initiated the Stuxnet attack on Iranian nuclear facilities in the last decade (7). The People's Republic of China (PRC) and North Korea have waged similar attacks on foreign targets (8). Russia has also engaged in cyberattacks against other countries, most spectacularly against Ukraine in recent months (9). Consequently, the wartime utility of this technology is also now becoming more evident.

Uncovered by incumbent disarmament regimes, the cyber domain is gaining prominence in states' arsenals. The UN Open-Ended Working Group (OEWG) on the security of and in the use of information and communications technologies and the Group of Governmental Experts (GGE) have been attempting to build consensus on the regulations governing the cyber domain. However, the exercise is marred by geopolitical competition (10). While the first OEWG was partially successful in fostering a more inclusive debate on the matter, the second iteration is plagued by rising geopolitical competition between the West, Russia, and the PRC. Stalemates caused by the Russia-Ukraine conflict, "data security, agreement on how to approach emerging threats, relevance of inclusion of gender, capacity building, and CBMs [confidence building measures]" (11) have rendered the exercise impotent.

AI: Brief, Impacts, and Challenges in Regulation

AI is defined as "a stream of study that involves creation of advanced algorithms that can mimic the human brain" (12). It also can combine "physical, information, cognitive, and social areas, blurring the boundaries between the private sector and the military; wartime and peacetime; and spaces for warfare and everyday lives" (13). AI has permeated "almost every sector" with immense military potential in "Intelligence, Surveillance, and Reconnaissance (ISR), cyber security, military logistics, autonomous vehicles and Lethal Autonomous Weapons Systems (LAWS)" (14). In addition, the technology enables cost advantages for modern militaries via integrating low-cost systems to produce an impact equivalent to large state-of-the-art weapons systems (15).

AI and LAWS in the military context are subjected to heated debates around three primary issues of international humanitarian law (IHL). First, it is argued that LAWS may violate the principle of distinction under IHL. This principle requires parties in an armed conflict to differentiate civilian and military assets and personnel. Only military assets under the principle can be legitimate targets. Second, it is argued that LAWS may violate the principle of proportionality, which mandates the determination of the civilian cost of achieving a particular military target by parties in an armed conflict. Attacks with disproportionate civilian damages are unlawful under the principle. Third, critics argue that LAWS may

violate the legal review principle that requires parties to the convention to determine if weapon systems and method of war comply with international law (16).

At the same time, supporters of LAWS argue that the technology has the potential to reduce unnecessary loss of life on the battlefield. This can be achieved by limiting the quantum of human soldiers needed on the battlefield via utilising LAWS in a self-sacrificing manner. Lack of emotions and human judgement may also lessen collateral civilian damage. Further, it may be too early to discuss the legality of LAWS as they could be utilised in scenarios where civilian loss is limited, such as in a naval context (17).

Under this context, since 2017, the UN GGE on LAWS has attempted to regulate their use, with the adoption of guiding principles in 2019 (18). But critics argue that these principles are "rather vague" (19). States also diverge on the form of LAWS regulations—one group argues in favour of legally binding regulations (20),(21) while the other has opposed such mechanisms (22). Efforts focused on middle-of-the-road proposals have similarly been subject to geopolitical machinations. Such measures have received criticism from the two camps for doing too little or too much in terms of legally binding regulation (23).

Nuclear Interface and Impact of Nuclear Weapons

With changing trends in the geopolitical, technological, economic, and military domains of warfare, the role of nuclear weapons in future conflicts is a key consideration. Although nuclear weapons were already used in 1945 (the bombings of Hiroshima and Nagasaki (24)), efforts to constrain their use and limit the use of conventional forces in conflict to avoid crossing the nuclear threshold continue. Nuclear weapons have both conventional and unconventional impacts on warfare.

The salience of nuclear weapons, at present and in the future, can be understood by analysing the shifts in nuclear postures, the changing role of deterrence for nuclear-weapon states, the increasing desire to acquire nuclear weapons by non-nuclear states, and the advent of new and emerging technologies. First, nuclear weapons factor into military doctrines, postures, and forces of both nuclear and non-nuclear states. Nuclear weapons play a major role in threat perceptions, and conventional and unconventional military modernisation.

Nuclear weapons were a more potent threat during the Cold War era when the number of nuclear warheads was far higher than present. Nevertheless, they remain a crucial factor of influence in future conflicts. The existence of nuclear weapons made it unlikely for large-scale conventional wars to break out during the Cold War, and this still applies in the case of conflict between nuclear states. However, a vital aspect of nuclear weapons in the future of warfare is the desirability of possessing such weapons by non-nuclear states and non-state actors. In the backdrop of the ongoing Ukraine invasion, Russia's status as a nuclear-weapon state attacking a non-nuclear country reaffirms concerns about non-nuclear states' desire to acquire nuclear weapons to employ them for coercion or as a bargaining chip to protect sovereignty and national security.

Vulnerable states are likely to reanalyse their military postures and reform their deterrence tactics (25). As the international security scenario becomes hostile or unpredictable, non-nuclear states may find

merit in acquiring nuclear capabilities as a competitive edge or a deterrent to attack or war. Nuclear weapons possessed by small states and non-state actors further impact both threat perceptions and the volatile international scenario. For example, North Korea's use of its nuclear weapons arsenal during a potential war has long been a matter of pause for the international community (26).

National Policies and International Regulations

For decades, one section of the international community has been pushing for global nuclear disarmament, with several nuclear-weapon states reaffirming their commitment to reducing their nuclear weapons forces until complete and total nuclear disarmament. Notably, none of the five nuclear-weapon states (the US, Russia, the UK, France, and China) shares this view, and nuclear weapons continue to factor in their military modernisation, force structure, and defence spending. The US, for example, is projected to spend approximately US$634 million to sustain and modernise its nuclear arsenal (27), while Russia and the PRC have also invested in maintaining and upgrading their nuclear stockpiles (28). Therefore, the role of nuclear weapons in how wars are fought and how actors with nuclear weapons capabilities are perceived remains a key tenet in how the future of warfare will take shape.

Additionally, international and bilateral treaties designed to promote international peace have weakened considerably. The usefulness of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) has also recently come into question. The lack of consensus among its members at the 2022 NPT Review Conference on the future of non-proliferation and the treaty's effectiveness has also raised concerns (29). The 2022 conference ended without consensus on a tangible action plan or concrete timelines to achieve the primary goals of the NPT. Additionally, there is growing scepticism on if NPT states will ever implement the commitments set by the treaty (30). The diminishing trust in the effectiveness of the NPT and the international nuclear community is further exacerbated by the demise of certain measures, such as the Intermediate-Range Nuclear Treaty (31) and the uncertainty raised by the US pull-out from the Joint Comprehensive Plan of Action (the Iran nuclear deal). The New Strategic Arms Reduction Treaty between Russia and the US is one of the few surviving treaties in the nuclear domain, but as ties between the two countries worsen, its future remains uncertain (32).

Interplay of Emerging Technologies

Another key consideration in future warfare is the interplay of emerging technologies with conventional military and nuclear domains. With the advent of technologies such as offensive cyber capabilities and AI, and the pervasiveness of the digital element in nuclear weapons and nuclear command, control and communications systems, the risks associated with nuclear weapons in warfare has heightened (33). Emerging technologies can be employed for unauthorised nuclear weapons use by adversaries, raising the risks exponentially. Advancements in emerging technologies, and the increasing reliance on cyberspace in the conventional military domains and the interplay with the nuclear domain are risky propositions. Current international nuclear agreements and bilateral treaties lack measures to effectively navigate the interplay between the nuclear domain and emerging technologies. For example, the draft final document of the 2020 NPT Review Conference recognises the importance of cybersecurity

measures for member states in the context of maintaining effective nuclear measures (34). However, it excludes concrete steps to address the challenges posed in warfare by the growing reliance on emerging technologies in warfare, conventional or otherwise.

A key issue associated with emerging technologies is the increased possibility of surprise attacks due to the difficulty of timely detection and the inability to counter such attacks promptly. This gives rise to other ways to address such threats, for instance, by an attack-first approach to eliminate the adversary's leadership, or the complete destruction of second-strike nuclear retaliatory capabilities. Under normal circumstances, states are unlikely to consider such options, but the potential of adversaries turning to such plans could push countries to formulate riskier nuclear operational strategies, like launch-on-warning. Another potential option is where states with smaller nuclear arsenals feel compelled to increase the size of their stockpiles to have a minimal second-strike capability. This could drive a new round of the arms race, which will be costly in more ways than one.

Even though emerging technologies pose challenges, their integrated effects will be far greater than the sum of their parts. Such an interplay is seen in many domains. Cyberattacks on nuclear facilities with "economic, operational and reputational costs" is one potential way this could play out (35). The number of such cyberattacks has risen manifold in recent years (36).

The scenario is not vastly different in the outer space domain. The growing salience of space and its increasing role in national security have pushed many states to develop counterspace capabilities to deny the advantages that may accrue from using space. The effects of advancements in the cyber domain have spilt over to the space domain. Cyber capabilities are cheaper than other anti-satellite (ASAT) options and provide the initiator with deniability because of difficulty in attribution. Cyber capabilities possess the potential to enact "large-scale disruptions or even permanent damage" to space assets without the perpetrator being identified (37). Other counterspace capabilities, including ASAT weapons, and electronic warfare means and directed energy weapons are being developed and tested to disrupt, deny, degrade, or destroy adversaries' space systems. These weapons have both kinetic and non-kinetic means of disruption and destruction. ASAT weapons produce an inherently destabilising effect on outer space security, but they can impact nuclear stability since nuclear warning and command control systems rely on space-based assets far more today than a few decades ago.

Any cyberattack that disables critical satellites for early warning or communications will have destabilising consequences. The destruction of these satellites through counterspace capabilities can create havoc but such destruction and disruption through an ASAT weapon will call for an immediate and categorical response due to its impact on early warning, command, control, or communication. An immediate response to an ASAT weapon use will also be needed as the demonstration effect of such an incident is more severe, and no state will want to run the risk of normalising such behaviour. Even middle-power states have a good number of satellites for ISR (intelligence, surveillance and reconnaissance) and communication functions, and, as such, any disruption or interference with satellite functioning can aggravate the risks and worsen the strategic stability dynamics.

Conclusion

While states agree on the need for regulating the militarised use of emerging technologies, disagreements on the type, scope and level of regulation persist. Comprehensive regulation finds support in some quarters to mitigate risks. Others stress the need to regulate specific military applications of emerging technologies (38). The temporal scope of any proposed regulations is also contested. While some states favour limiting wartime regulations, critics advocate covering "all stages of military application regardless of peacetime or war, from research and development to actual deployment" (39).

Emerging technology regulation is inevitably associated with the application of the primary principles of international law (40). However, geopolitical lines drawn are based on specific characteristics of the technologies in concern, in addition to the level of a state's technological capabilities. This divide is witnessed in questions of self-defence. Arguing that countermeasures would inevitably lead to the conception of deeper cyber and space battlefields, the PRC and Russia oppose the application of self-defence principles in space and cyber domains. However, the West is undertaking steps to apply these principles in the cyber and space domains in response to the increased potential for peacetime surprise attacks ushered by emerging technologies. For instance, the US seeks easing standards for mobilising self-defence measures during peacetime in the cyber and space domains (41).

Likewise, the absence of distinct recommendations for strengthening nuclear disarmament policies and dwindling efficacy and trust in international norms, regulations and agreements will play a large role in how nuclear weapons are perceived in the future, either for war-fighting or deterrence. International norms, even voluntary and non-binding ones, are useful as they explicitly define the mutual benefit to states. However, when confronted with core national interests, norms "always struggle" (42).

What can be done to reduce the dangers? Can global governance measures effectively address these risks? Are legally-binding measures the ideal solution? In the absence of agreement among states on threats and possible solutions, other options must be considered as the first step to reduce such threats, including political agreements such as transparency and confidence-building measures to boost confidence among states. Strengthening dialogues through multiple channels, information-sharing mechanisms, and establishing and using hotlines between important offices (such as military operations and defence) can also be considered.

Given the dual-use nature of emerging technologies, regulation is intrinsically linked to the policy parlance surrounding technology control and supply chain security. Additionally, technical norms aimed at ensuring safer offensive operations must be considered. While emerging technologies complicate prospects for traditional inspection requirements akin to arms control regimes, this approach possesses the potential to deliver more "pragmatic and specific results than [relying solely on] political norms" (43).

This dual-use nature also implies that NGOs and the private sector must play a central role in future norm formation. International NGOs have traditionally been critical for the promotion of international peace and disarmament initiatives. It is imperative that leaders in the military, industry and academia dealing with questions of emerging technologies "align….perspectives, clarify issues, and formulate strategies to deal with emerging challenges" (44).

States must also collaborate with the private sector to mitigate such challenges. Cooperation must be enacted via information sharing, expert exchanges, joint research, and enhancing private industry's presence in international cooperation. Additionally, states and the private sector must endeavour to construct a "shared perception of security" via strategic dialogues and drills (45).

While various steps, including technical and legal measures, can be used to reduce the vulnerabilities and risks from emerging and critical technologies, political commitments are key to implementing effective compliance, irrespective of the type of pact. The lack of consensus among major powers has become the most significant impediment in ensuring the fuller implementation of old agreements or developing new rules of the road.

Endnotes

(1) Gregory C. Allen, "Across Drones, AI, and Space, Commercial Tech Is Flexing Military Muscle in Ukraine," *Center for Strategic and International Studies Commentary*, May 13, 2022, https://www.csis.org/analysis/across-drones-ai-and-space-commercial-tech-flexing-military-muscle-ukraine

(2) Tae Eun Song, "Security Effects of Emerging Military Technologies: Implications and Key Issues," *IFANS Focus*, January 6, 2022, https://www.ifans.go.kr/knda/ifans/eng/pblct/PblctView.do?csrfPreventionSalt=null&pblctDtaSn=13894&menuCl=P11&clCode=P11&koreanEngSe=ENG&pclCode=&chcodeId=&searchCondition=searchAll&searchKeyword=&pageIndex=3

(3) RAND Organization, "Cyber Warfare," RAND Organization, https://www.rand.org/topics/cyber-warfare.html.

(4) NTT, *Global Threat Intelligence Report*, NTT, 2022, https://us.nttdata.com/en/insights/global-threat-intelligence-report

(5) John Lee, "The Connection of Everything: China and the Internet of Things," *MERICS*, (2021), https://merics.org/sites/default/files/2021-06/MericsChinaMonitor70InternetOfThings2.pdf

(6) "Global Threat Intelligence Report"

(7) "IRNA: Stuxnet a product of US and Israel," *Jerusalem Post*, April 16, 2011, https://www.jpost.com/Breaking-News/IRNA-Stuxnet-a-product-of-US-and-Israel

(8) Office of the Director of National Intelligence, Government of the United States of America, *Annual Threat Assessment of US Intelligence Community*, Washington, D.C, 2022, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

(9) Jakub Przetacznik with Simona Tarpova, "Russia's war on Ukraine: Timeline of cyber-attacks," European Parliamentary Research Service, June 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf; Tae Eun Song, "Cyber Warfare in the Russo-Ukrainian War: Assessment and Implications," *IFANS Focus*, August 4, 2022, https://www.ifans.go.kr/knda/ifans/eng/pblct/PblctView.do?csrfPreventionSalt=null&pblctDtaSn=14028&menuCl=P11&clCode=P11&koreanEngSe=ENG&pclCode=&chcodeId=&searchCondition=searchAll&searchKeyword=&pageIndex=1

(10) Louise Marie Hurel, "The Rocky Road to Cyber Norms at the United Nations," *Council on Foreign Relations*, September 6, 2022, https://www.cfr.org/blog/rocky-road-cyber-norms-united-nations-0

(11) Hurel, "The Rocky Road to Cyber Norms at the United Nations"

(12) Sanur Sharma, "AI and National Security: Major Power Perspectives and Challenges," *IDSA Issue Brief,* (2022), https://idsa.in/issuebrief/ai-and-national-security-ssharma-120922.

(13) Song, "Security Effects of Emerging Military Technologies"

(14) Sharma, "AI and National Security"

(15) Song, "Security Effects of Emerging Military Technologies"

(16) R S Panwar, "Artificial Intelligence in Military Operations: Technology and Ethics Indian Perspective," *USI Journal* CXLIX, no. 615 (2019), https://usiofindia.org/publication/usi-journal/artificial-intelligence-in-military-operations-technology-and-ethics-indian-perspective/?_sf_s=Cognitive.

(17) Panwar, "Artificial Intelligence in Military Operations"

(18) United Nations Office for Disarmament Affairs, "Background on LAWS in the CCW," United Nations Office for Disarmament Affairs, https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/

(19) Lutiana Valadares, Fernandes Barbosa and Gustavo Macedo, "What Have the Recent UN Attempts to Regulate Lethal Autonomous Weapons Brought?," *Völkerrechtsblog*, September 19, 2022, https://voelkerrechtsblog.org/what-have-the-recent-un-attempts-to-regulate-lethal-autonomous-weapons-brought/

(20) United Nations, Office for Disarmament Affairs, Draft submitted by Argentina, Ecuador, Costa Rica, Nigeria, Panama, the Philippines, Sierra Leone and Uruguay (New York: Office for Disarmament Affairs, 2022), https://documents.unoda.org/wp-content/uploads/2022/07/WP-Argentina_Costa-Rica_Ecuador_Nigeria_Panama_Philippines_Sierra-Leone_Uruguay.pdf

(21) United Nations, Office for Disarmament Affairs, Elements for a Legally Binding Instrument to Address the Challenges posed by Autonomy in Weapons Systems (New York: Office for Disarmament Affairs, 2022), https://documents.unoda.org/wp-content/uploads/2022/08/WP-Chile-and-Mexico-.pdf.

(22) United Nations, "2022 Group of Governmental Experts (GGE) on emerging technologies in the area of lethal autonomous weapons systems (LAWS), Second session," United Nations, https://indico.un.org/event/1001117/page/75-transcripts-automatic

(23) Barbosa and Macedo, "What Have the Recent UN Attempts to Regulate Lethal Autonomous Weapons Brought?"

(24) Daryl G. Kimball, "Reality Check: The Atomic Bombings of Hiroshima & Nagasaki," *Arms Control Association,* https://www.armscontrol.org/pressroom/2020-07/reality-check-atomic-bombings-hiroshima-nagasaki

(25) "The Future of Warfare," *ESPAS Ideas Papers Series*, European Parliamentary Research Service (EPRS), 4, https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/Future%20of%20Warfare%20-%20ESPAS%20Ideas%20Paper%20-%20Leopold%20Schmertzing.pdf

(26) Future of Warfare, EPRS.

(27) "Cost Overview", U.S. Nuclear Modernization Programs, *Arms Control Association,* January 2022, https://www.armscontrol.org/factsheets/USNuclearModernization#costoverview

(28) Cost Overview, *Arms Control Association.*

(29) Pulkit Mohan, "The Future of Nuclear Disarmament: A look at the Tenth NPT Review Conference, *ORF Expert Speak,* 31 August 2022, https://www.orfonline.org/expert-speak/the-future-of-nuclear-disarmament/

(30) Frank Jackson, "Is it time to abandon the nuclear non-proliferation treaty?" *The Guardian*, August 31, 2022, https://www.theguardian.com/world/2022/aug/31/is-it-time-to-abandon-the-nuclear-non-proliferation-treaty

(31) "U.S. Withdrawal from the INF Treaty on August 2, 2019," Press Statement by Michael R. Pompeo, U.S. Department of State, 2 August 2019, https://2017-2021.state.gov/u-s-withdrawal-from-the-inf-treaty-on-august-2-2019/index.html

(32) "The New START Treaty between the US and Russia: The last surviving pillar of nuclear arms control," European Parliament Think Tank, 22 March 2021, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)690523

(33) "Emerging technologies and nuclear weapon risks," International Campaign to Abolish Nuclear Weapons, https://d3n8a8pro7vhmx.cloudfront.net/ican/pages/1166/attachments/original/1580226579/ICAN_emerging_technology_and_nuclear_weapons_policy_briefing.pdf?1580226579

(34) "2020 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons," NPT/CONF.2020/CRP.1, *United Nations,* https://reachingcriticalwill.org/images/documents/Disarmament-fora/npt/revcon2022/documents/CRP1.pdf

(35) Pulkit Mohan, "Cyber Security in India's Nuclear Systems," *ORF Issue Brief No. 412, October 2020,* Observer Research Foundation, https://www.orfonline.org/research/ensuring-cyber-security-in-indias-nuclear-systems/.

(36) Mohan, "Cyber Security in India's Nuclear Systems"

(37) Rajeswari Pillai Rajagopalan, "Electronic and Cyber Warfare in Outer Space," *Space Dossier 3*, United Nations Institute for Disarmament Research, Geneva, May 2019, https://unidir.org/sites/default/files/publication/pdfs//electronic-and-cyber-warfare-in-outer-space-en-784.pdf

(38) Joonkoo Yoo, "Regulating the Military Application of Emerging Technologies: Recent Trends, Key Issues and Implications," *IFANS Focus*, March 28, 2022, https://www.ifans.go.kr/knda/ifans/eng/pblct/PblctView.do?csrfPreventionSalt=null&pblctDtaSn=13978&menuCl=P11&clCode=P11&koreanEngSe=ENG&pclCode=&chcodeId=&searchCondition=searchAll&searchKeyword=emerging&pageIndex=1

(39) Yoo, "Regulating the Military Application of Emerging Technologies"

(40) Yoo, "Regulating the Military Application of Emerging Technologies"

(41) Yoo, "Regulating the Military Application of Emerging Technologies"

(42) Laura G. Brent, "Geopolitics keeps overruling cyber norms, so what's the alternative?," *Breaking Defense*, January 12, 2022, https://breakingdefense.com/2022/01/geopolitics-keeps-overruling-cyber-norms-so-whats-the-alternative/

(43) Brent, "Geopolitics keeps overruling cyber norms, so what's the alternative?"

(44) Song, "Security Effects of Emerging Military Technologies"

(45) Song, "Cyber Warfare in the Russo-Ukrainian War

About the Editor and Authors

Rajeswari (Raji) Pillai Rajagopalan is the Director of the Centre for Security, Strategy and Technology at ORF.

Almudena Azcárate Ortega is an Associate Researcher in the Space Security and Weapons of Mass Destruction programme at the United Nations Institute for Disarmament Research.

Major General Amarjit Singh was commissioned into the Indian Armoured Corps and retired as Major General after 37 years of active service. He is a visiting professor at Panjab University, and Director of Gyan Chakra Think Tank.

Air Vice Marshal Arjun Subramaniam is the President's Chair of Excellence in National Security at National Defence College. He is a retired fighter pilot from the Indian Air Force.

Ashok GV is Partner at Factum Law.

Bart Hogeveen is Head of Cyber Capacity Building at the Australian Strategic Policy Institute's International Cyber Policy Centre.

Brett van Niekerk is a Senior Lecturer at the Department of Information Technology, Durban University of Technology.

Jyun- Yi Lee is an Associate Research Fellow at Institute for National Defense and Security Research, Taiwan.

Kazuto Suzuki is professor of science and technology policy at the Graduate School of Public Policy at the University of Tokyo and senior fellow of the Asia Pacific Initiative, an independent policy think tank.

Kubo Mačák is a legal adviser jointly assigned to the Commentaries Update Unit and the Arms and Conduct of Hostilities Unit at the Legal Division of the International Committee of the Red Cross in Geneva.

Laurent Gisel is the Head of the Arms and Conduct of Hostilities Unit at the Legal Division of the International Committee of the Red Cross in Geneva.

Malcolm Davis is a Senior Analyst at the Australian Strategic Policy Institute.

Manpreet Sethi is a Distinguished Fellow at the Centre for Air Power Studies, New Delhi.

Michal Křelina is a theoretical physicist and quantum technology consultant, analyst and strategist focusing on defence and security applications. He is also the Founder of Quantum Phi s.r.o. and Chief editor at qubits.cz.

Nivedita Raju is a Researcher in the Stockholm International Peace Research Institute's Weapons of Mass Destruction programme.

Noëlle van der Waag-Cowling is the Cyber Programme Lead at the Security Institute for Governance and Leadership in Africa, Stellenbosch University.

Pulkit Mohan is an Associate Fellow with the Centre for Security, Strategy and Technology at ORF.

Lt. Gen. Raj Shukla is a recently retired Indian Army commander.

Lt. Gen. Ravindra Singh Panwar, AVSM, SM, VSM (retd.) is the 57th Colonel Commandant of the Corps of Signals. His last appointment in the Indian Army was as Commandant of Military College of Telecommunication Engineering, Mhow.

Sameer Patil is a Senior Fellow at ORF Mumbai.

Samyak Rai Leekha was a Junior Fellow with the Centre for Security, Strategy and Technology at ORF.

Shambhavi Naik is the Head of Research at Takshashila and is the chairperson of the Advanced Biology programme.

Trishana Ramluckan is an Honorary Research Fellow at the School of Law, University of KwaZulu-Natal, and Group Research Manager at Educor Holdings.

Wilfred Wan is the Director of the Stockholm International Peace Research Institute's Weapons of Mass Destruction programme.