gp ORF

global POLICY

GP-ORF Series

Future Warfare and Critical Technologies: Evolving Tactics and Strategies

Edited by

Rajeswari Pillai Rajagopalan and Sameer Patil

Durham University

WILEY

FUTURE WARFARE AND CRITICAL TECHNOLOGIES: EVOLVING TACTICS AND STRATEGIES

EDITED BY

RAJESWARI PILLAI RAJAGOPALAN AND
SAMEER PATIL

© 2024 Observer Research Foundation and Global Policy Journal. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical or photocopying, recording, or otherwise, without the prior permission of the publisher.

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.

Cover image: Getty Images / Anton Petrus

Cover Design: Rahil Miya Shaikh

Layout: Simijaison Designs

ISBN: 978-81-19656-43-1 (print); 978-81-19656-02-8 (digital)

Citation: Rajeswari Pillai Rajagopalan and Sameer Patil, eds, *Future Warfare and Critical Technologies: Evolving Tactics and Strategies* (New Delhi: ORF and Global Policy Journal, 2024).

CONTENTS

Introduction 7

Strategic and Tactical Perspectives on Technologies

The Plague Beckons: On the Proliferation of Drone Swarms 12
Zachary Kallenborn

Virtual and Augmented Reality and Warfare: Fighting War as a Computer Game? 28
Akshat Upadhyay

The Future of Competition and Warfare in Cyberspace 43
Nishant Rajeev

Exploring the Utility of Blockchain in Military Operations 57
Meghna Bal and Mohit Chawdhry

Biotechnology and the Return of Biological Warfare 70
Shruti Sharma

Assessing the Military Applications of Generative AI 84
Amoha Basrur

Space and Counterspace Technologies in Future Warfare 98
Victoria Samson

General Strategic Perspectives

Should India Publicly Attribute International Cyber Incidents? 109

Arindrajit Basu

How the US Should Prepare for Space Warfare: Illustrated by Countering Rendezvous Spacecraft Threat 123

Brian G. Chow

Decoding China's Nuclear Modernisation 137

Rajeswari Pillai Rajagopalan

The Role of Nuclear Deterrence 151

Tanvi Kulkarni

No Domain an Island: Ground Forces Need AI in Other Domains to Succeed 164

Michael Depp

’It was an Accident’: Implications of AI on the Ability to Distinguish Between ‘True’ Accidents and Violations of International Humanitarian Law 175

Laura Bruun

Introduction

MODERN WARFARE has continuously evolved, with technological advancements shaping its conduct. Critical technologies like cyberspace and artificial intelligence (AI) are making new warfighting tools available, even as traditional ones like nuclear weapons are witnessing a resurgence. These changes have brought greater lethality and destruction in warfighting and blurred the lines of conflict, with direct warfare being replaced by new forms such as hybrid warfare or grey zone tactics (where the threat has diffused, and proxy actors have taken the lead).

Multiple analytical frameworks have examined this shift in warfare, studying its implications for tactics and strategies. For example, the 'generations of warfare' literature describes five generations of warfare. First-generation warfare involved person-to-person fighting, primarily dependent upon physical strength, skills, and numbers. Second-generation warfare, through firepower, resulted in combatants with asymmetrical force or strength levels being able to impose their will on traditionally more powerful adversaries. Third-generation warfare prioritised manoeuvres after infiltrating enemy lines. Fourth-generation warfare blurred boundaries between state and non-state actors and border regions and the hinterland, with terrorism or proxy warfare holding primacy. The decision-making process of the target's leadership is targeted in this form of warfare. Fifth-generation warfare aims to control the adversary's population by distorting their worldview and threat perceptions, even without knowledge of the target.

These shifting battlefields have transformed with critical technologies like cyber, virtual and augmented reality (VR/AR), AI, and 3D printing. Several of these technologies have made the battlefield a complex and interconnected ecosystem with the convergence of the physical and virtual domains. They have allowed combatants to engage in fighting without resorting to kinetic means, which has been the hallmark of the battles of the previous centuries. At the same time, they have also spawned discussions about their ethical implications, legal frameworks, and potential unintended consequences. The use of lethal autonomous weapon systems, for instance, has been a controversial topic, with a growing chorus of voices from various sectors advocating for a global prohibition for their purported violation of international humanitarian law. Similarly, using cyber tools to target critical national infrastructure has raised concerns about potential widespread disruption and civilian casualties, which may have cascading effects on other essential infrastructure and services. Yet, several countries are pursuing these technologies to weaponise and deploy them as quickly as possible.

National security establishments and military planners worldwide are now faced with new challenges with this transformation in warfighting. It has made policy choices more complex and responses more challenging. The essays in this volume seek to unpack key critical technologies and explore their implications for the future of warfare. They tackle themes like cyberwarfare, challenges of attribution, swarming drones, autonomous weapons, AI, and their impact on land warfare, blockchain, and warfighting while also looking at the impact of these technological advancements on nuclear weapons and space. These essays, written by domain experts and renowned scholars, answer four critical questions: Who/what are we fighting? Where are we fighting? How are we fighting? And when are we fighting?

Zachary Kallenborn, discussing the drone swarms, argues that while their global proliferation is expected, it will not happen immediately. Different states will adopt different approaches to their proliferation—some focusing on numbers, some focusing on the drones' technological sophistication, and others implementing export controls to check their spread. Exploring another critical technology, Akshat Upadhyay examines the role of VR/AR in warfare. He highlights that VR and AR have increased relevance for warfighting, as VR can stimulate conditions that are impossible to create in the lab or on training grounds for safety reasons, while AR adds a layer of additional information (audio, visual, haptic), heightening the sensory performances required for the battlefield.

Looking at cyber warfare, Nishant Rajeev discusses how states exploit cyberspace to further their strategic objectives. He argues that it is easier for states to leverage cyber capabilities in the competitive dynamic than in the armed conflict or wartime dynamic due to the unique nature of cyber capabilities. Next, Meghna Bal and Mohit Chawdhry, discussing the utility of blockchain technology for warfighting, look at the prominent early-use cases and argue that while several militaries are experimenting with the technology, its utility in military operations is presently unproven. Meanwhile, Shruti Sharma focuses on biotechnology and highlights its crucial role in developing and producing biological weapons. Given the dangerous potential of biological agents, she argues that it is necessary to strengthen the norm that biotechnology will be used only in non-harmful ways.

Among other critical technologies, Amoha Basrur looks at generative AI, exploring its utility for militaries and the potential risks involved. Just like biotechnology, she also advocates for the safe and ethical deployment of generative AI. Victoria Samson, examining the role of space and counter-space technologies, highlights the increased importance of space for many countries. This has led to efforts to disrupt other countries' abilities to utilise space, resulting in the proliferation of counterspace capabilities beyond the major powers.

After looking at the strategic and tactical perspectives on critical technologies, the next set of essays offers general strategic perspectives.

Arindrajit Basu tackles the question of attribution for cyber incidents and notes that India has not publicly attributed a specific international cyber incident to a specific private perpetrator or nation-state. However, as the frequency and intensity of such cyber incidents increase, India cannot afford not to use the critical option of public attribution, when deemed effective, to navigate the uncertainty of cyber unpeace and further its strategic interests. Next, Brian G. Chow looks at the American space warfare capabilities and argues that, although the US has beefed up its capabilities, its overall space resilience is only as strong as its weakest link, particularly when it comes to China, which poses significant threats.

Regarding China, Rajeswari Pillai Rajagopalan discusses the nuclear modernisation of the People's Liberation Army. She argues that China appears to be undertaking a vast nuclear expansion in quantitative and qualitative terms. While much of this modernisation is aimed at the US, it also has ripple effects among its neighbours in the Indo-Pacific. Tanvi

Kulkarni, dwelling further on this theme, examines the role of nuclear deterrence. She argues that two factors—the strength of nuclear norms and the applications of modern and emerging technologies—are most likely to affect how and to what extent nuclear weapons will play a role in future conflicts. Added to this is the uncertainty of global geopolitics and the uncertainty arising from the rapidly evolving nature of existential threats to human life and the environment.

The final two essays explore the related aspects of AI. Michael Depp argues that while significant advancements in AI technology in military systems have occurred, automating ground warfare has proven particularly difficult. Much of the progress has been achieved in air and naval systems. Nonetheless, these advancements will be the key to effectively using AI for success in ground operations. Finally, Laura Bruun argues that as more and more militaries become dependent on AI, it may add new layers to the fog of warfare. Therefore, developing a deeper understanding of the risks is critical to ensure legal compliance and human accountability in future and potentially more AI-reliant warfare. In a sense, this is a precautionary tale for applying all critical technologies in warfighting.

Overall, this compendium of 13 essays brings out multiple nuances of the implications of critical technologies for warfighting.

We want to thank our editor, Preeti Lourdes John, for her immaculate editing and efforts to make the volume publication-ready.

- Rajeswari Pillai Rajagopalan and Sameer Patil

Rajeswari (Raji) Pillai Rajagopalan *is the Director of ORF's Centre for Security, Strategy and Technology.*

Sameer Patil *is Senior Fellow at ORF's Centre for Security, Strategy and Technology, and Deputy Director, ORF Mumbai.*

STRATEGIC AND TACTICAL PERSPECTIVES ON TECHNOLOGIES

The Plague Beckons: On the Proliferation of Drone Swarms

Zachary Kallenborn

IN A JULY 2020 REPORT, *New America* identified 38 states with armed drone programmes, 11 of which had used armed drones in combat (1). Twenty-eight more states have programmes in development (2). Global exports enable the rapid proliferation of drones, as states share drone technology with others. The US, Israel, and China have been the largest exporters (3). Iran has also helped non-state allies—Hezbollah, Hamas, and the Houthi rebels—acquire drones (4). The expanding, broad commercial drone industry and simple do-it-yourself ingenuity have also helped the Islamic State and various lone-wolf actors acquire and use them (5).

Single drones are increasingly being integrated into collaborative drone swarms. Precisely defined, drone swarms are “multiple unmanned systems capable of coordinating their actions to accomplish shared objectives” (6). These are proliferating quickly as well. Armenia, China, France, India, Israel, the Netherlands, Russia, Spain, South Africa, South Korea, and the US all have drone swarm programmes under development (7). In May 2021, Israel became the first state to use a drone swarm in combat, collecting and relaying information on Hamas militant locations for follow-up attacks (8). In most cases, the drone swarm consists of homogeneous, aerial drones, such as the 103 Perdix drone that the US Strategic Capabilities office launched out of three F/A-18 Super Hornets in January 2017 (9). But others, such as Elbit System’s Torch-X, integrate diverse ground and aerial vehicles (10).

Although global proliferation can be expected, drone swarm proliferation should not be expected to be even or immediate. Some states may race to develop massive, armed drone swarms, while others may never develop sophisticated drone swarm capabilities. Over time, the holdouts may change their views as they come to recognise the military value drone swarms bring. Motivated states can also put their finger on the scale, implementing national export controls to limit transfers of drone swarms to states without them. Groups of states might work together to expand the scope of those restrictions, and encourage larger international norms around drone swarm development, use, and transfer.

Thinking About Drone Swarm Proliferation

Drone swarms are a technological innovation. Any military innovation requires the financial resources to buy or build the technology and organisational capacity to incorporate changes into recruiting, training, and operations (11). Incorporating drone swarms into larger operations requires identifying and assessing the most effective use cases to know where the technology is of the most value, and incorporating those uses into doctrine. Success depends on leadership delegations of authority, effective control over training, and independent doctrinal assessment mechanisms (12). For drone swarms, the unique organisational challenges are likely to revolve around sustaining drone mass over time in an area of operation, requiring integrated production, logistics, and sustainment systems. States may differ in how they do that and how well. For example, in the US, doctrine frequently drives technology, while in China, technology may drive doctrine (13).

Drone swarms are a sub-type of drones, so the proliferation dynamics of drones apply. For example, hobbyist, mid-size military and commercial, large military-specific, and stealth combat drones will all differ in how quickly and broadly they proliferate (14). Although hobbyist drones are broadly and easily available for only a few thousand dollars, the US appears to be the only operator of stealth drones (though China, India, Israel, Russia, and a European consortium are also developing them) (15). Organisational and laboratory resources place constraints in state and non-state actor's ability to create drones (16). Adding swarming must necessarily increase the constraints: a state developing a swarm of stealth combat drones has all the constraints of building the stealth combat drone, and the additional challenge of integrating them into a swarm. But that increase will depend on the system in question. MIT engineering students designed the Perdix drone swarm, suggesting that a simple drone swarm requires relatively limited capability (17). However, a swarm of MQ-9 Reaper drones would require not only the capability and resources to build an MQ-9, but the capability to build, deploy, and test the software and hardware needed to integrate them. Some factors that have encouraged drone proliferation, such as reduced risk to human operators, will apply to drone swarms too (18). Drone swarms probably reduce the immediate operator risk even more, because their use necessarily implies larger adoption of drones.

The Demand for Drone Swarms

Demand drives drone swarm proliferation. States must perceive that they gain some meaningful economic, political, tactical, strategic, or other benefit from the use of drone swarms. Otherwise, why pursue them? Drone swarm advantages include cheap mass, limited operator requirements, distributed complexity, and applicability to various military missions. Additionally, those gains must be greater than any economic, political, tactical, or strategic risks and requirements. In the case of drone swarms, those include general fears of remote warfare, questions over drone swarm reliability, adversary countermeasures, and building and integrating necessary infrastructure and support systems. If the risks outweigh the gains, why bother expending time and energy (19)?

Why Drone Swarms?

Cheap mass: Drone swarms allow militaries to generate and manage large numbers of drones. Drone swarms can consist of thousands of drones to overwhelm adversary defences. In a 2012 master's thesis at the Naval Postgraduate School, Loc Pham and co-authors found that eight drones were enough to overwhelm naval destroyer vessels (20). Typically, four drones would hit the ship (21). Cheap mass is useful not only for overwhelming defences but also for depleting munitions over time and fixing platforms in undesirable locations. In the Ukraine-Russia war, Russia employed cheap Shahed-131 and 136 drones extensively in attacks against Ukrainian critical infrastructure. Although the drones were shot down at high rates, the attacks still forced Ukraine to deploy air defences to protect infrastructure instead of forward-deployed units waging the war (22). If defenders employ expensive surface-to-air missiles to shoot down cheap drones, missile stocks will not be unavailable for use against more valuable targets like manned aircraft.

Limited operator requirements: As drone swarms scale in size, they must necessarily be autonomous. As General John Murray of the US Army Futures Command puts it, "When you have little drones operating in different patterns and formations, all talking to each other and staying in sync with one another...imagine that with the ability to create lethal effects on the battlefield. There is no human who will be able to keep up with that" (23). That may mean no personnel needed to operate and manage the swarm. Instead, humans may be relegated to providing oversight, such as providing high-level command and control, supporting logistics and launch, and providing any needed maintenance or support activities.

Distributed complexity: Drone swarms can integrate multiple capabilities and spread over a broad area. Combined arms effectiveness can be baked into the DNA of a drone swarm. A single drone swarm may contain multiple payloads operating together: sophisticated sensors to identify and track targets, electronic warfare equipment for jamming, and bombs and missiles for carrying out strikes (24). A couple of drones might suppress the target with electronic warfare, while other drones coordinate kinetic attacks from multiple axes simultaneously. Drone-to-drone communication allows drones to distribute widely to coordinate intelligence gathering and searches, providing situational awareness for follow-on attacks.

Broad military applications: Drone swarms can be used in a broad range of missions, from undersea warfare to countering anti-access/area-denial and amphibious warfare. Drones could be distributed throughout the ocean, seeking to identify and track adversary submarines, bringing greater transparency to the ocean (25). That could create stability concerns by reducing the viability of ocean-based second-strike deterrence measures. The US also sees great value in drone swarms for defeating Chinese anti-access area-denial measures, using mass drones to exhaust missile defence magazines, suppress or destroy defensive sites, and protect more valuable manned assets (26). Although the value of drone swarms to any mission will depend on the state and their conflict environment, the broad range of applications means drone swarms can help many states tackle their security challenges.

Why Not Drone Swarms?

Fears of remote warfare: Some states hesitate to use any armed drones. Some fear drones will result in states more readily engaging in violence and war because the costs of loss are lower (27). Others note that the combination of decreased risk to soldiers and physical distance from the battlefield makes discrimination between combatants and non-combatants more difficult, a critical law-of-war issue (28). For example, Germany only allowed military forces to deploy unarmed drones until April 2022, when the nearby war between Russia and Ukraine spurred a rethink along with a broader defence bump (29). If states are unwilling to use armed drones, they certainly would be unwilling to use numerous drones networked together, especially if drone swarms exacerbate the ethical concerns. German concerns were associated with drone use during the War on Terror, where drone strikes were relatively narrow against pre-identified targets. Thousands of drones deployed against thousands of targets would exacerbate concerns about remote warfare thousands of times.

Reliability questions: As drone swarms scale in size, the swarm may become ever more unpredictable and unreliable in practice. In a truly massive drone swarm, a human operator could not plausibly maintain direct operational control over the swarm. This creates at least three reliability concerns. First, autonomous target selection and engagement using current artificial intelligence is unlikely to be reliable. A single pixel change is enough to convince a machine-learning system that a stealth bomber is a dog (30). Although such a radical error was only possible in a specific circumstance, battlefields are complex and dynamic, and those errors may arise unexpectedly. Second, because drones within a swarm communicate by definition, a mistake in one drone may cascade to the drone swarm as a whole. For example, if one drone attacks a school bus after mistaking it for an enemy tank, other drones may attack, too, because they are following the lead of the first. Third, the interaction between the drones may produce collective error. That is, a drone swarm operating on a distributed, collective intelligence may collect accurate information from its sensors, but draw an incorrect inference about the location or existence of an adversary. Altogether, the reliability challenges coupled with the potential for mass harm mean that drone swarms are potential future weapons of mass destruction, with significant challenges in holding to laws of armed conflict around discriminating between civilian and non-civilian targets and applying proportional force to achieve a military objective (31).

Dealing with adversary action: Integrating drones into a drone swarm provides new potential paths for adversaries to manipulate or disrupt the drones. Drone swarms depend on communication between the drones, which may be jammable or manipulatable (32). Because the drone swarms must be increasingly autonomous, an adversary might also attempt to trick the swarm into hitting a friendly target or, say, crashing into a mountainside (33). An adversary might also attempt to exacerbate the reliability concerns by using decoys or camouflage to induce more frequent and serious errors. Although testing, evaluation, and technological hardening may reduce adversarial concerns, it is likely to be extremely difficult to certify operations for large, complex drone swarms operating in a dynamic environment (34). If an adversary can readily defeat or manipulate the swarm, adding swarming capability may not be worth it.

Infrastructure and support systems: Battlefield drone swarms require logistics, maintenance, and production capabilities to sustain them. A state might be able to develop a swarm of 10,000 drones, all integrated and working together, but to be effective, that swarm still must be delivered to the battlefield. States are developing motherships—larger platforms to transport and deploy drones—but that necessarily means added cost and added vulnerability (35). If an adversary can find and destroy the mothership, all the drones it carries may be defeated or destroyed as well. If the 10,000 drones make it to the battlefield, many will likely be defeated or destroyed in combat. There are so many drones that even if half are lost, the swarm may still accomplish its objective. However, to sustain that momentum, the drones must be replaced. For example, in Ukraine's war with Russia, Ukraine lost an estimated 10,000 drones per month (36). States need the production and supply capacity to replace the drones lost in combat.

The Supply of Drone Swarms

If a military desires drone swarms, they must acquire one. That means acquiring four things: the drone platform, payloads, control stations, and the swarm management system. The drone platform can range broadly from a simple quadcopter to a large MQ-9 Reaper or naval vessel.

Although drone swarm platforms may be virtually identical to a non-swarming drone, the platform may incorporate transmitters and receivers for intra-swarm communication. The drones might carry some combination of infrared, electromagnetic, or other sensors; grenades, bombs, guns, or other munitions; jammers, microwaves, or other directed weapons; even chemical or biological weapons. The control station allows operators to provide command and control for the drone swarm and may be handheld or have man-portable controls, a station at a base, or integrated into another platform, like a manned aircraft or truck. The swarm management system makes the swarm a swarm. That system includes the algorithms, software, and any specialised hardware needed to connect the drones together and allow them to operate as a collective.

States have two basic options: build or buy. In the short term, states will almost certainly have to build their own, because drone swarms are an immature, emerging technology. But as the technology matures and becomes more broadly available, buying a drone swarm becomes increasingly plausible.

Building a drone swarm requires the financial, technological, and production resources to build the drone platforms, develop the swarming behavioural algorithms, write the software and firmware code to integrate the swarming behaviours into the drone platforms, equip the drones with whatever payloads they might use, and test and evaluate the result. Of course, not all needs to be done from scratch. The actor may already have drone platforms capable of autonomous functions that can be readily modified to accommodate swarming, as well as access to basic swarming algorithms through open-source research. However, as drone swarms are a novel, emerging technology, developing the system may require basic scientific research through university laboratories. It is possible that a state that does not have sufficient capability (or better capability exists elsewhere) can acquire it from another state by funding research, as suggested by June 2023 reports that Iran worked with British scientists to investigate using lasers for intra-swarm communication (37).

Battlefield recovery, theft, or illicit transfer of swarming drones, components thereof, or technical data could help. The value of drone swarms in generating attritable mass also creates a proliferation risk. A drone swarm might have the numbers to endure and overwhelm adversary defences, but the adversary can recover fallen drones to understand how they operate and develop their own. For example, in December 2011, Iran captured an American RQ-170 Sentinel drone by manipulating the RQ-170's GPS, after which Iran proceeded to build its own version (38). Growth in drone forensics as a discipline may enable proliferation through battlefield recovery in expanding the know-how to acquire critical information about how recovered drones function (39). Alternatively, states can use cyberattacks or conventional espionage to steal technical information usable to design and build drone swarms. For example, for decades, China has stolen information on American military technology, including the F-22 and MQ-9 Reaper, and appears to have used that information to develop native weapon systems (40). However, once the information is acquired, a state still needs the technical capacity to use that information and build the new system.

Buying a drone swarm requires financing, and, more importantly, a willing seller. Only one state—Israel—possesses a drone swarm used in actual combat. If Israel is unwilling to sell that system, there is no other option for a battle-tested drone swarm. Of course, as drone swarm technology matures and more states develop, deploy, use, and produce drone swarms at scale, more options might open. However, states may still be unwilling to sell. In August 2020, a bipartisan group of US senators attempted to block the sale of the MQ-9 Reaper to Saudi Arabia and the United Arab Emirates due to concerns about the US getting too involved in the Saudi and Emirati war with Yemen and the potential to encourage broader proliferation (41). If drone swarms prove to be quite militarily significant, states may worry that sales will affect regional balances of power. If the drone swarm involves aerial drones capable of carrying over 500 kilograms, the Missile Technology Control Regime would also apply (42). But even if the state cannot build a complete drone swarm, they may be able to buy commercial parts that can be used to help make one. For example, 40 out of 53 identified components in Iranian Shahed-136 drones are manufactured in Western countries, including multiple American companies, despite years of sanctions and tough export controls on Iran (43).

Commercial entities provide alternate sources to buy a drone swarm, but the military value may be limited. Companies are increasingly developing and making simple drone swarms available, such as Red Cat

Holding's 4-Ship (44). The 4-Ship allows operators to control six drones simultaneously: four carrying out operations with the other two to swap in as needed (45). Four drones might be a useful drone swarm for small unit reconnaissance and surveillance, but they are unarmed and far from the hundreds of drones that might make up a military swarm. The control systems and swarming algorithms in a commercial drone swarm will likely also need to be modified, if not wholly replaced, to accommodate military needs. A commercial drone swarm does not need the capability to release a bomb, engage adversaries, or respond to signal or GPS jamming or spoofing (46). Nonetheless, commercial drone swarms are still significant for the proliferation of military drone swarms, because the technical know-how they invest in, develop, maintain, and expand could be used for military purposes.

Combatting Proliferation

States concerned about the proliferation of drone swarms can attempt to limit supply and reduce demand. Export controls on the transfer of drone swarm technology and the know-how necessary to create them may help slow the spread of drone swarms, while new international norms, backed up by international legal regimes, can help reduce demand. The effects of drone swarm proliferation can also be mitigated through concentrated and collaborative research on swarm countermeasures. If novel countermeasures neutralise the military value of drone swarms, then the effects on global stability may be limited.

Export controls can help reduce the transfer of military drone swarms, critical components, and the know-how to create either. Legitimate defence companies depend on trust relationships with their governments, and few would risk the loss of reputation, future contracts, and fees over a single deal. For drone swarms, the challenge is the small start-ups that may be unaware of their export compliance requirements, or lack the capacity to provide adequate due diligence (47). Small companies may also lack robust cybersecurity measures to guard against cyber theft. Universities and other research institutes are also a challenge because researchers may not appreciate the dual-use aspect of technology, may be repatriated to their home countries, or participate in academic exchanges with researchers in countries of concern (48). Governments should emphasise public-private collaborations to build awareness of compliance requirements and build necessary capacity (49). Global governments will likely struggle to detect illicit transfers without private-sector collaboration. As of 2020, 38 states already have armed drones, while 28 more have programmes in development (50). Turning those drones into drone swarms depends primarily on acquiring software that could be transferred on a thumb drive or the intangible know-how to develop the algorithms and code. Both will be quite difficult to detect.

International norms, augmented by binding international laws, can help reduce demand for drone swarms, and encourage global implementation of export controls. The reliability problems of drone swarms, especially armed, autonomous ones, may lead states to forego them entirely. No soldier wants a weapon that does not work. An errant attack that destroys a neutral or friendly target is a waste of munition, may hinder friendly movements, and may alert adversaries to friendly positions. Plus, states may be unwilling to use a weapon with significant law-of-war concerns. Although states may still develop and acquire unarmed drone swarms for intelligence gathering, they may refrain from massive armed drone swarms. New international norms, conventions, and laws restricting or banning autonomous weapons would also necessarily apply to autonomous drone swarms (51). Of course, states that perceive a strong military need for drone swarms are unlikely to forego armed drone swarms entirely. However, norms can still limit the speed of proliferation by reducing the availability of technical know-how and the number of states willing and able to transfer the technology.

Improved drone swarm defences would counter the effects of global proliferation. If states can reliably defeat drone swarms, effects on regional security balances are reduced. Although the outline of the drone swarm answer is clear, the details are not. The challenge with countering drone swarms is finding solutions that can disable, defeat, or destroy many drones in a cost-effective manner. High-powered microwaves like the Leonidas or THOR systems have some promise. High-powered microwaves have a very low cost per shot, demanding only electricity to fire, and can create effects over a broad area. However, the systems themselves are costly (Leonidas platforms cost about $16.5 million per platform), set-up takes a few hours, effective ranges are short, and simple countermeasures like microwave absorbing materials are in development (52). States concerned about drone swarm proliferation could participate in and encourage multilateral countermeasure development activities, invest in novel technologies and concepts, and export solutions to friendly and allied nations.

Conclusion

Numerous states are rushing to build drone swarms; however, global proliferation will take a while. This is especially the case when it comes to large, complex drone swarms that are still a nascent technology. States may also choose to forego building them. Although drone swarms offer cheap mass, limited operator requirements, and distributed complexity across a broad range of military applications, drone swarms also have potential reliability problems, require significant support infrastructure, and entail risk and opportunity costs. Plus, some states just do not like armed drones. States that want armed drone swarms will need to build their own, but buying a drone swarm will become increasingly feasible as the technology matures. States concerned about the spread of drone swarms can aim to reduce the demand for drone swarms through new international norms and treaties. States can also limit the supply of drone swarms through robust, multilateral export controls, involving strong engagement with small companies and research institutions.

Drone swarms are not science fiction; they are used on battlefields today. What remains to be seen is how globally ubiquitous the weapons become.

Zachary Kallenborn *is an Adjunct Fellow (non-resident) with the Center for Strategic and International Studies (CSIS), Policy Fellow at the Schar School of Policy and Government, Fellow at the National Institute for Deterrence Studies, Research Affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), an officially proclaimed US Army "Mad Scientist," and national security consultant.*

Endnotes

(1) Peter Bergen, Melissa Salyk-Virk, and David Sterman, "World of Drones," *New America,* July 30, 2020, https://www.newamerica.org/international-security/reports/world-drones/introduction-how-we-became-a-world-of-drones/.

(2) Bergen, Salyk-Virk, and Sterman, "World of Drones"

(3) Bergen, Salyk-Virk, and Sterman, "World of Drones"

(4) Dion Nissenbaum, Sune Engel Rasmussen, and Benoit Faucon, "With Iranian Help, Hamas Builds, 'Made In Gaza' Rockets and Drones To Target Israel," *Wall Street Journal,* May 20, 2021, https://www.wsj.com/articles/with-iranian-help-hamas-builds-made-in-gaza-rockets-and-drones-to-target-israel-11621535346; "Roster Of Iran's Drones," United States Institute of Peace, March 2, 2023, https://iranprimer.usip.org/blog/2023/mar/02/roster-iran%E2%80%99s-drones; Håvard Haugstvedt and Jan Otto Jacobsen, "Taking Fourth-Generation Warfare To the Skies? An Empirical Exploration of Non-State Actors' Use of Weaponized Unmanned Aerial Vehicles," *Perspectives on Terrorism* 14, no. 5 (October 2020), https://www.jstor.org/stable/26940037?seq=5.

(5) Dan Rassler, "Islamic State and Drones: Supply, Scale, and Future Threats," Combatting Terrorism Center at West Point, July 2018, https://ctc.westpoint.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf.

(6) Zachary Kallenborn and Philipp C. Bleek, "Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons," *Nonproliferation Review* 25, no. 5–6 (2019): 523–43.

(7) David Hambling, "What are Drone Swarms and Why Does Every Military Suddenly Want One?" *Forbes,* March 1, 2021, https://www.forbes.com/sites/davidhambling/2021/03/01/what-are-drone-swarms-and-why-does-everyone-suddenly-want-one/?sh=3248e4392f5c; Wiebe de Jager, "Dutch Drone Makers Develop Autonomous Drone Swarm for Defense Dept." *DroneXL,* July 22, 2021, https://dronexl.co/2021/07/22/dutch-drone-makers-autonomous-drone-swarm/; Bruce Crumley, "Korean Air Advances Use of Drone Swarms in Plane Inspections," DroneDJ*,* June 12, 2023, https://dronedj.com/2023/06/12/korean-air-advances-use-of-drone-swarms-in-plane-inspections/; David Hambling, "Israel Used World's First AI-Guided Combat Drone Swarm in Gaza Attacks," *New Scientist,* June 30, 2021, https://www.newscientist.com/article/2282656-israel-used-worlds-first-ai-guided-combat-drone-swarm-in-gaza-attacks/.

(8) Hambling, "Israel Used World's First AI-Guided Combat Drone Swarm in Gaza Attacks"

(9) Aaron Mehta, "Pentagon Launches 103 Unit Drone Swarm," *DefenseNews,* January 10, 2017, https://www.defensenews.com/air/2017/01/10/pentagon-launches-103-unit-drone-swarm/.

(10) "Elbit Systems Demonstrated Heterogeneous Swarm Capability to the Dutch RAS Concept Development & Experimentation Program," Elbit Systems, November 15, 2021, https://elbitsystems.com/pr-new/elbit-systems-demonstrated-heterogeneous-swarm-capability-to-the-dutch-ras-concept-development-experimentation-program/.

(11) Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Oxfordshire: Princeton University Press, 2010), https://press.princeton.edu/books/paperback/9780691143965/the-diffusion-of-military-power.

(12) Michael A. Hunzeker, *Dying to Learn: Wartime Lessons from the Western Front* (Cornell University Press, 2021), https://www.cornellpress.cornell.edu/book/9781501758454/dying-to-learn/#bookTabs=1.

(13) Dennis J. Blasko, "Technology Determines Tactics: The Relationship between Technology and Doctrine in Chinese Military Thinking," *Journal of Strategic Studies* 34, no. 3 (June 17, 2011), https://www.tandfonline.com/doi/abs/10.1080/01402390.2011.574979.

(14) Kelley Sayler, "A World of Proliferated Drones: A Technology Primary," Center for a New American Security, June 2015, https://drones.cnas.org/wp-content/uploads/2016/03/CNAS-World-of-Drones_052115.pdf.

(15) Sayler, "A World of Proliferated Drones: A Technology Primary"

(16) Andrea Gilli and Mauro Gilli, "The Diffusion of Drone Warfare? Industrial, Organizational, and Infrastructural Constraints," *Security Studies* 25, no. 1 (February 25, 2016), https://www.tandfonline.com/doi/abs/10.1080/09636412.2016.1134189.

(17) MIT Beaver Works, "Project Perdix," https://beaverworks.ll.mit.edu/CMS/bw/projectperdixcapstone.

(18) Michael Horowitz, Sarah Kreps, and Matthew Fuhrman, "Separating Fact from Fiction in the Debate Over Drone Proliferation," *International Security* 41, no. 2 (October 1, 2016), https://direct.mit.edu/isec/article/41/2/7/12140/Separating-Fact-from-Fiction-in-the-Debate-over.

(19) Of course, the relative value of each advantage, risk, and constraint will vary depending on the state in question.

(20) Loc V. Pham et al. "UAV Swarm Attack: Protection System Alternatives for Destroyers," 2012.

(21) Pham et al. "UAV Swarm Attack: Protection System Alternatives for Destroyers"

(22) Max Hunder, "Ukraine Says it Shot Down 36 Drones in Overnight Russian Attacks," *Reuters,* May 25, 2023, https://www.reuters.com/world/europe/ukraine-says-it-shot-down-36-drones-overnight-russian-attacks-2023-05-25/.

(23) Kris Osborn, "Drone Swarms Could Be Too Fast to Handle. Is AI the Answer?" *The National Interest,* April 14, 2021, https://nationalinterest.org/blog/reboot/drone-swarms-could-be-too-fast-handle-ai-answer-182659.

(24) Zachary Kallenborn, "Swarm Talk: Understanding Drone Typology," Modern War Institute at West Point, December 10, 2021, https://mwi.usma.edu/swarm-talk-understanding-drone-typology/.

(25) Rebecca Hersman et al., "Under the Nuclear Shadow: Situational Awareness Technology and Crisis Decisionmaking," Center for Security and International Studies, March 2020, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200318_UnderNucearShadow_FullReport_WEB.pdf; Zachary Kallenborn, "If the Oceans Become Transparent," U.S. Naval Institute, October 2019, https://www.usni.org/magazines/proceedings/2019/october/if-oceans-become-transparent.

(26) Joseph Trevithick, “Massive Drone Swarm Over Strait Decisive in Taiwan Conflict Wargames,” *The Drive,* May 19, 2022, https://www.thedrive.com/the-war-zone/massive-drone-swarm-over-strait-decisive-in-taiwan-conflict-wargames; David Hambling, “The US Navy Wants Swarms of Thousands of Small Drones,” *MIT Technology Review,* October 24, 2022, https://www.technologyreview.com/2022/10/24/1062039/us-navy-swarms-of-thousands-of-small-drones/.

(27) Erik Lin-Greenberg, “Wargame of Drones: Remotely Piloted Aircraft and Crisis Escalation,” *Journal of Conflict Resolution* 66, no. 10 (June 6, 2022), https://journals.sagepub.com/doi/pdf/10.1177/00220027221106960?casa_token=SznysPgZMM8AAAAA:oYnjFvQjiFYp0jZqFYYkGRlvAdmilOyVT__w4DYL6BKSGQv9dsVWLoW4Z1OB5e7B5sUgupBiXUzmZlw.

(28) Daniel Brunstetter and Megan Braun, “The Implications of Drones on the Just War Tradition,” *Ethics & International Affairs* 25, no. 3 (2011), https://www.cambridge.org/core/services/aop-cambridge-core/content/view/97ABF476B8494CC44A71E011DD8B7600/S0892679411000281a.pdf/the-implications-of-drones-on-the-just-war-tradition.pdf.

(29) “Germany to Get Weaponized Drones for the First Time,” *AFP,* April 6, 2022, https://www.thedefensepost.com/2022/04/06/germany-weaponized-drones/.

(30) “AI Image Recognition Fooled by Single Pixel Change,” *BBC,* November 3, 2017, https://www.bbc.com/news/technology-41845878.

(31) Zachary Kallenborn, “Future Warfare Series No. 60: Are Drone Swarms Weapons of Mass Destruction?” United States Air Force Center for Strategic Deterrence Studies, June 29, 2020, https://media.defense.gov/2020/Jun/29/2002331131/-1/-1/0/60DRONESWARMS-MONOGRAPH.PDF; Zachary Kallenborn, “Meet the Future Weapon Of Mass Destruction, the Drone Swarm,” *Bulletin of the Atomic Scientists,* April 5, 2021, https://thebulletin.org/2021/04/meet-the-future-weapon-of-mass-destruction-the-drone-swarm/.

(32) Zachary Kallenborn, “InfoSwarms: Drone Swarms and Information Warfare,” *Parameters* 52, no. 2 (2022), https://press.armywarcollege.edu/parameters/vol52/iss2/13/.

(33) Paul Scharre, “Counter-Swarm: A Guide to Defeating Robotic Swarms,” War on the Rocks, March 31, 2015, https://warontherocks.com/2015/03/counter-swarm-a-guide-to-defeating-robotic-swarms/.

(34) Arthur Holland Michel, “The Black Box, Unlocked: Predictability and Understandability in Military AI,” United Nations Institute for Disarmament Research, 2020, https://unidir.org/sites/default/files/2020-09/BlackBoxUnlocked.pdf

(35) David Hambling, “Robot Motherships to Launch Drone Swarms from Sea, Underwater, Air, and Near-Space,” *Forbes,* February 5, 2021, https://www.forbes.com/sites/davidhambling/2021/02/05/robot-motherships-to-launch-drone-swarms-from-sea-underwater-air-and-near-space/?sh=57cda4d4215c; Zachary Kallenborn, “368. The Swarm Mother,” Mad Scientist Laboratory, November 22, 2021, https://madsciblog.tradoc.army.mil/368-the-swarm-mother/; Joe Saballa, “China Unveils ‘Mothership’ to Launch Drone Swarms,” *Defense Post,* May 31, 2022, https://www.thedefensepost.com/2022/05/31/china-mothership-drone-swarms/.

(36) Jack Watling and Nick Reynolds, “Meatgrinder: Russian Tactics in the Second Year of its Invasion of Ukraine,” *RUSI,* May 19, 2023, https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf.

(37) David Rose and Felix Pope, "Britain's 'Swarming Drone' Research Shared with Iran," *The Jewish Chronicle,* June 15, 2023, https://www.thejc.com/news/news/britains-swarming-drone-research-shared-with-iran-5P709ETPi4A6ciem12exx.

(38) Scott Peterson, "Exclusive: Iran Hijacked US Drone, Says Iranian Engineer," *Christian Science Monitor,* December 15, 2011, https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer; Tyler Rogoway, "Iran's RQ-170 Clone Crashes Suspiciously on 10th Anniversary Of the Real One Falling into its Hands," *The Drive,* December 6, 2021, https://www.thedrive.com/the-war-zone/43390/irans-rq-170-clone-suspiciously-crashes-on-10th-anniversary-of-real-one-falling-into-its-hands.

(39) "Framework For Responding to a Drone Incident: For First Responders and Digital Forensics Practitioners," INTERPOL, January 2020, https://www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf.

(40) Ellen Loanes, "China Steals US Designs for New Weapons, and it's Getting Away with 'The Greatest Intellectual Property Theft in Human History'," *Business Insider,* September 24, 2019, https://www.businessinsider.com/esper-warning-china-intellectual-property-theft-greatest-in-history-2019-9.

(41) "US Senators Push to Block Drone Sales to Saudi Arabia, UAE," *Middle East Eye,* August 7, 2020, https://www.middleeasteye.net/news/us-uae-saudi-arabia-senators-drone-sales; Edward Wong, "Trump Administration is Bypassing Arms Control Pact to Sell Large Armed Drones," *New York Times,* July 24, 2020, https://www.nytimes.com/2020/07/24/us/politics/trump-arms-sales-drones.html.

(42) Missile Technology Control Regime, https://mtcr.info/.

(43) Natasha Bertrand, "CNN Exclusive: A Single Iranian Attack Drone Found to Contain Parts from More Than a Dozen US Companies," *CNN,* January 4, 2023, https://www.cnn.com/2023/01/04/politics/iranian-drone-parts-13-us-companies-ukraine-russia/index.html.

(44) Loz Blain, "You Can Now Buy a Co-Ordinated Multi-Drone Swarm in a Box," *New Atlas,* June 2, 2022, https://newatlas.com/drones/red-cat-drone-swarm-product/.

(45) Blain, "You Can Now Buy a Co-Ordinated Multi-Drone Swarm in a Box"

(46) Kallenborn, "InfoSwarms: Drone Swarms and Information Warfare"

(47) Rudi du Bois, Julia Bell, and Dries Bertrand, "To Share Or Not To Share?: The Challenge Of Controlled Technologies in Research and Development (R&D)," *Strategic Trade Review* 9, no. 10 (Winter / Spring 2023), https://strategictraderesearch.org/wp-content/uploads/2023/02/Rudi-du-Bois-Export-Controls-and-Research-and-Development.pdf.

(48) Andrea Viski, "Advanced Conventional Weapons and Emerging Technologies: Recognizing and Preempting Proliferation Threats," *Strategic Trade Review,* February 2022, https://strategictraderesearch.org/wp-content/uploads/2022/02/Advanced-Conventional-Weapons-and-Emerging-Technologies.pdf.

(49) Viski, "Advanced Conventional Weapons and Emerging Technologies: Recognizing and Preempting Proliferation Threats"

(50) Bergen, Salyk-Virk, and Sterman, "World of Drones"

(51) Zachary Kallenborn, “A Partial Ban on Autonomous Weapons Would Make Everyone Safer,” *Foreign Policy*, October 14, 2020, https://foreignpolicy.com/2020/10/14/ai-drones-swarms-killer-robots-partial-ban-on-autonomous-weapons-would-make-everyone-safer/; Dharvi Vaid, “Human Rights Watch Seeks Treaty Banning ‘Killer Robots,” *DW*, August 11, 2020, https://www.dw.com/en/human-rights-watch-seeks-treaty-banning-killer-robots/a-54521323.

(52) Ashley Roque, “US Army Selects Epirus’ Leonidas for High-power Microwave Initiative,” *Breaking Defense*, January 23, 2023, https://breakingdefense.com/2023/01/us-army-selects-epirus-leonidas-for-high-power-microwave-initiative/#:~:text=WASHINGTON%20%E2%80%94%20Epirus%2C%20a%20technology%20company,drones%2C%20the%20firm%20announced%20today; Oliver Parken, “THOR Microwave Anti-Drone System Downs Swarms in Test,” *The Drive*, May 19, 2023, https://www.thedrive.com/the-war-zone/thor-microwave-anti-drone-system-downs-swarms-in-test; Zachary Kallenborn and Marcel Plichta, “Breaking the Drone Shield: Countering Drone Defenses,” *Joint Force Quarterly*.

Virtual and Augmented Reality and Warfare: Fighting War as a Computer Game?

Akshat Upadhyay

IN THE PENULTIMATE SCENE OF THE MOVIE *The Matrix,* Neo, after transforming into the all-powerful The One, says, "I can see everything clearly now." The camera then shifts to Neo's point of view, displaying a cascade of ones and zeros against a green screen. The implication is that Neo can now access the duality behind the Matrix, a simulation created by machines to keep humans in a state of stupor while their bodies are used as bio-electric fuel for the machine civilisation. The simulation immerses human beings into the world as it was in 1999, and life inside the Matrix is designed to be as normal as possible to create a sense of presence for the users while precluding them from ever thinking of the greater reality beyond the simulation.

The aim of virtual reality (VR)-based applications and hardware is to create such a user immersion inside a synthetic environment, though for purely benign and educative purposes. However, the current peculiarities of the hardware, software, and user requirements have created several devices and programmes that combine elements of both physical and virtual reality. This mixed reality (MR) can be thought of as forming part of a reality–virtuality continuum with the physical and virtual environments (VE) acting as extreme bounds. Two intermediate states of augmented reality (AR), which comprises the use of certain equipment and data to accentuate the user's perception of the physical world, and augmented virtuality (AV), which is the augmentation of VE with real or unmodelled imaging data, fall between the two bounds (1). VR and AR have increased relevance for warfighting, as VR models worlds and conditions that are impossible to create in the lab or on training grounds for safety reasons, and adds to a quantitative and systemised approach towards training. AR, on the other hand, adds a layer of additional information (audio, visual, haptic) between the soldier and his/her physical world and heightens certain sensory performances required for the battlefield. Whether these are cost-effective and adequately ruggedised needs to be studied in detail.

War as a Game

Though depicted as a fusion of war and a chess game between two kings in the Bollywood movie *Shatranj ke Khiladi,* war is never fought like a game, since, unlike games, there are no rebirths or second chances. Soldiers or 'players' cannot respawn at a given location to continue the fight. Unlike a video game player, a soldier does not have omniscience on the battlefield, nor is the call for airstrikes or additional resources delivered in quick time. There are additional challenges of post-traumatic stress disorder (PTSD), informing the next of kin (NoK) of the soldiers killed in action, and treatment of prisoners of war. All these experiences are missing from games. So, does that mean that games have no connection with war?

Ironically, games play an important and rather critical role in warfighting, but not in the way they are imagined. Gamification is the use of game-style incentives, such as rewarding users for achievements, earning badges, and 'levelling-up', which are used to motivate individuals to carry their game-based learning to real life (2). Johan Huizinga said in 1938 that humankind's most important activity belonged to the realm of fantasy and that play was the structuring element of all cultures, the function by which man created subjectivity (3). The use of quantifiable indicators to earn points, improve performance, and perform 'what-if' thought experiments, i.e., using games for analysing and manipulating human behaviour takes major inspiration from the quantitative movement in institutes such as the Institute for Advanced Studies in Princeton and the RAND Corporation in California (4). Game theory was created in the US keeping in mind the rational human being, one who looked after only his own interests and maximised his rewards (5). Based on these 'games', the entire strategic canon of the Cold War was devised, containing terms such as brinksmanship, deterrence, and compellence (6). Simulations were run on the effect of nuclear weapons on cities and forces, and based on these calculations, targeting strategies were modified and doctrines designed and redesigned (7). Games have therefore played a major part in the US strategic posture, at least since the Second World War.

Another area where simulations played a huge part and still do is theoretical physics and cosmology, where even the notion of proving hypotheses regarding the origin of the universe or observing the nuclear reactions within stars is not possible directly (8). The word 'gamification' itself entered the contemporary lexicon in 1978 when Richard Bartle coined it in the context of a game called Multi User Dungeon (MUD). Several games were designed in the early 1980s to enhance learning using three core features of games: goals, competition, and narrative (9).

VR and the Military

The mainstreaming of VR began with the entertainment industry in the US with the intention of immersing the user within a movie using all of their five senses. Morton Heilig, a professional cinematographer, developed the "Sensorama" in 1962 as a rudimentary VR device (10). Ivan Sutherland wrote about the 'ultimate display' in 1965 that would include interactive graphics, force-feedback devices, audio, smell, and taste (11). Jaron Lanier, a computer scientist and founder of VPL Research, coined the term VR in 1987 (12).

In terms of the military, the introduction of VR was in the form of flight simulators for training pilots (13). From thereon, the utility of VR has involved the increasing use of VE, i.e., digitally created worlds either mediated through real-world inputs or totally insulated from it. VR as a military utility has grown from computer simulations, computer games, flight simulators, networked simulators for small teams, formation simulators, joint simulators, and even multi-domain simulators for combat tasks. Another area where VR is being used, at least in the US, is in military medicine to treat PTSD in soldiers returning from overseas deployments. Complex and invasive surgical procedures are also being simulated in VR, and the same is imparted to military doctors through transfer of training. This is because the use of VR accords certain advantages to military personnel, a significant amount of which is borne out of studies. The basic set-up of VR in any industry is an input device (including haptic gloves, microphones, joystick, and motion sensors), a processor, and certain output devices (14). Before diving into the findings of the studies, however, it is important to define certain terms specific to the AR and VR fields.

(a) **Immersion**: Refers to the tracking and display that a VR/AR system delivers to the user. This can be measured objectively. As per Mel Slater, the more a system delivers displays and tracking that preserves fidelity to their equivalent real-world sensory modalities, the more immersive it is (15).

(b) **Presence**: Presence is the subjective experience of the user inside a VR world. As of now, it cannot be measured. In other words, presence is a human reaction to the immersion. Given the same levels of immersion, different humans can experience different levels of presence. One of the major reasons to achieve presence through a VR system is to elicit human physiological responses that would be commensurate with that of the real world. There are two ways to achieve presence. One is to mirror reality within the VR to such fidelity that there is no distinction between the virtual and physical worlds (16). The second is to extract the relevant sensory stimuli through knowledge of the perceptual system, i.e., to find out what is important in a human's representation of reality and deliver presence without a high level of immersion.

(c) **Tracking**: The tracking sensors and devices are the main components of the VR system. They interact with the system's processing unit and relay the user's orientation to the system. These include electromagnetic, acoustic, mechanical, and optical tracking systems (17).

(d) **Registration**: This is a term used for AR systems and can be defined as a process that merges virtual objects generated by a computer with real-world images caught by a camera to create an accurate alignment of the two. Without accurate registration, the issue of the virtual object 'dangling' in the overlaid graphic without context cannot be ruled out, defeating the purpose of using AR.

The subsequent sections detail the findings and conclusions of certain studies on the military aspects of VR that were carried out mostly in the US, but also in Taiwan, Spain, Argentina, and Malaysia on different aspects and impacts of VR on military personnel.

A game-based learning environment was created to improve the training and results of rifle firing for 160 high school students in Taiwan, all with prior gaming experience. The results of the study showed that a combination of real-world training and rifle simulator and 3D VR training led to a significant improvement in the shooting scores of the students (18). These 'games' in which storytelling is applied outside the context of entertainment are known as 'serious games' (19). The aim here is to educate and facilitate transfer of training from the virtual to the physical world. This has both its supporters and detractors. Academics writing in the early 1990s—at a time when image, audio, and haptic processing had not reached the immersive level of today—were dismissive of the value of VR-based training and any transfer of skills back to the physical world (20). However, the challenge today is different. How can one transfer military knowledge and experience gained by servicemen in combat during their varied tours of duty to 18-year-olds? Is the immersive environment the answer?

A study by Boyce et al. shows that increasing the fidelity of the terrain representation or the 'immersivity' of the simulation does not increase the overall understanding of the terrain in a simulated mission planning environment (21). One must remember that, for a majority of the youth undergoing these simulations for the first time, most of the basic skills acquired during combat by their predecessors—fire and move, hand-to-hand combat, taking cover during artillery barrages—will be new to them and will necessitate a lot of trial and error with no guarantees that the correct skills will be learnt. There might be need for a knowledge representation system within VR that quantifies, measures, and then faithfully reproduces the stimuli required to respond to combat situations while providing detailed feedback on the actions of the trainees. One critique of the current process of military training using VR is that it serves as a practice platform rather than a training device (22). In other words, there is a presumption of the presence of certain skills that need to be honed rather than starting from scratch. As a result, these VR and simulation-based scenarios are minimally guided and not designed as per the cognitive capabilities of the trainees.

An Aviation Combined Arms Trainer designed for the US Army enables training of heterogeneous mobile units based on armoured formations and combat aviation assets, with a modular design that allows for a change of mission. Multiple simulators are networked together using standardised distributed interactive simulation protocols that allow for joint training amongst geographically dispersed units (23). The Taiwanese military has experimented with body area networks where training data is collected on individual soldiers when they are inserted into a VR military simulator. This provides researchers greater access to the soldier's physical actions and postures as they occur in real-time training (24). They can form a bridge between physical and virtual environments as future simulations can be devised with the expected stances of soldiers in mind. Accelerometers, when combined with VR-based training scenarios, can also assist in monitoring stress in soldiers in real time (25). Assessing the fidelity of VEs in judgement decisions of shoot/do not shoot scenarios (which form the core of soldiering), a study (with a sample size of 39 Royal Air Force dismounted soldiers) found that live-fire and VR had similar results while 2D video presented little decision-making challenge to the soldiers. The findings indicated that 2D video had a lower ranking than either VR or live-fire in terms of creating decision dilemmas, thus making the training lessons stick.

Learning under stress conditions can be recalled easier. In psychology, this is termed as "state-dependent learning." (26) Construct Validity (27) or the effectiveness of a training simulation to sufficiently represent the functionality of the skill-to-be-acquired needs to be kept in mind when designing simulations. A comparative study by the Indian Air Force's (IAF) Institute for Aerospace Medicine on the use of simulators and standard procedures by the Indian and the US Air Forces for countering spatial disorientation (SD) found that the IAF used a customised SD simulator for trainee as well as operational pilots, resulting in a much more improved response to SD-related air disasters (28). This is another example of transferring certain skills from the virtual to the physical world. Furthermore, VR is being used in analysing and witnessing the trajectory and impact of hi-tech ammunition such as rockets and missiles (29). Apart from combat and deployment-related training, VRs are also used in two other very critical areas related to the military: medicine and cultural communication.

The Office of Naval Research, based on user feedback, developed the Virtual Iraq application with a 'virtual Afghanistan' scenario as an addendum in an initial open clinical trial with 20 soldiers, positive clinical outcomes, such as improvement in neuro-cognitive functioning, memory and learning, spatial cognition, and executive functioning (30). One of the more practical uses of VR, also emphasised by the US Department of Defense in their Comprehensive Soldier Fitness programme is stress resilience testing, which is based on the view that it is not the event that causes the emotion but how a person appraises the event, which is intertwined with the emotion (31). The focus is on teaching coping skills to soldiers. VR exposure therapy uses a mix of cognitive–behavioural treatment (CBT) with prolonged exposure (PE) that is delivered through multi-sensory and context-relevant cues that evoke the trauma, the intensity of which can be calibrated by the clinician. The use of PE as a psychotherapeutic tool is based on the emotional processing theory that states that PTSD involves "pathological fear structures" when information represented in the structures is encountered. Treatment using this theory calls for the emotional processing of the fear structures to modify their pathological elements so that the stimuli do not provoke fear (32).

VR is also looked upon as an innovative and effective stress training programme as it is a good tool for assessing an individual's resilience to stress and in identifying the importance of stress on physiological reactivity and performance. Stress management training in military medicine is a holistic concept that looks at both stress inoculation training and resilience training. While the former increases stress tolerance through exposure, the latter looks at stress management (33). VR phobia therapy looks at using VR to activate the patient's fear structures. For this, the VE must produce sufficiently realistic sensory stimuli to trigger fear and requires a high degree of fidelity to the real world structures (34). In terms of immersion, while studying the AMADEUS VR system used by civil engineers to study the aspects of tunnelling, it has been found that increasing the level of immersion in the VR led to greater spatial understanding (35). Since tunnelling through rocks for making roads and pipelines are incredibly complex tasks, high levels of immersion in terms of stereoscopy can lead to improved task performance.

In terms of cultural communication, VR has many uses, some of which are already being indirectly applied in commercial video games. The integration of generative artificial intelligence (AI), especially large language models in video games for character development for role playing games, has expedited the trend towards individualisation of narratives and characters within the game (36). The presence of intelligent virtual agents (IVAs) in VR applications who can dynamically converse in the local dialect and model local customs and behaviours in the areas where troops have to be deployed for humanitarian and disaster relief operations or peacekeeping missions will prove to be a handy tool for armies deployed in unfamiliar terrain. Terrain familiarisation is another area that can be modelled using VR and troops practised on the same. India, one of the largest contributors of soldiers to multiple United Nations (UN) missions across the globe, can benefit from these technologies, and the Centre for UN Peacekeeping can take a lead in test bedding VR technologies for training Indian troops. The US Army already has had great success in the use of VR-based applications for training their troops for overseas deployments. A report by the North Atlantic Treaty Organization's Research and Technology Organisation lists the use of VR in military operations other than war where IVAs can simulate indigenous personnel, communicate non-verbal cues associated with foreign cultures, and function as coaches and mentors for trainees (37).

Augmented Reality

Augmented reality (AR) merges the virtual and the physical worlds. Although it has become synonymous with a helmet-mounted display (HMD) or see-through glasses, AR has also been consumerised in the form of mobile applications like Pokemon Go (38). It is a blend of technologies that accentuate the user's perception of the physical reality. One of the more prominent examples of AR is the series of space telescopes launched by the National Aeronautics and Space Administration (NASA), the latest iteration being the James Webb Space Telescope (JWST). Though JWST 'sees' in the infrared range, the images are translated into a form that is visible to the human user (39). AR can also extend into the auditory and haptic domains, using devices, technologies, and processes to increase human perceptivity of a particular strand of the physical reality (40). For the military, AR can be used to augment situational awareness through the merging of multiple intelligence, surveillance, and reconnaissance streams, generating a common operational picture and then disseminating them to the soldiers on the ground through an HMD. However, this will also require an intelligent and context-aware AR application to cater to the chaotic and dynamic battlefield. In closely contested areas, with multiple agents and installations, there is a danger of information overload on the soldier, which may retard rather than enhance his sense of the combat zone.

An urban terrain is considered to be the ideal setting for an AR-based device due to two reasons: rapid urbanisation of areas previously considered and suited for mechanised warfare, and the issue of clutter necessitating the use of AR in the first place. An urban warfare AR has three objectives: transparent battlefield, intuitional perception, and natural interaction (41). For this, better hardware, powerful software, and a much more integrated process of combining geographical information systems with a virtual geographic environment are essential. In peacetime, AR has multiple uses, such as enhancing the level of detail in table-top and sand-model wargames (42), maintenance training for military equipment (43), and even merging AR with the web (Web AR) (44)—a superb tool that can be used for augmenting open-source intelligence data for effective debunking of disinformation operations.

Use of Augmented and Virtual Reality in the Indian Armed Forces

The Indian Armed Forces have also slowly started utilising VR to simulate and immerse soldiers into virtual training grounds, while using VR-based war games to practise operational strategies at the same time. Whereas simulators have been a part of the Forces' inventory since the 1970s, induction of VR-based systems has taken place only in the last few years. In fact, in the recently concluded Army Commanders' Conference of 17 April 2023, the Raksha Mantri reviewed an equipment display that also comprised VR-based systems (45). The Indian Army already has a wargaming centre that is in the process of employing VR and AR technologies in conjunction with AI and data analytics to create metaverse-enabled gameplay (46). Incidentally, "metaverse for mental health" has been adjudged as one of the top ten emerging technologies of 2023 by the World Economic Forum (47). A custom-built CBT tool will be used for teaching strategies to student officers and extrinsic factors will also be included and/or modified (48).

Some Indian defence start-ups have also developed VR applications. HoloSuit, a motion capture haptic suit, has nine haptic feedback devices fitted across the body. When connected to the HoloSuit Engine on any mobile or desktop operating system, the application creates an instant 3D avatar that faithfully reproduces the user's movements, in effect providing a wealth of stance, posture, and reactivity data for in-depth training (49). The suit is reportedly being used by the Indian Armed Forces. Another start-up, Mumbai-based Parallax Labs, has developed a VR-based personal flight simulator. The first prototype has been installed at a naval aviation unit in Goa while talks are on to install the second one in Nashik (50). Certain army units are also using VR systems for terrain familiarisation along the Line of Control (51). Missile simulators (52) are being used by personnel of the Corps of Army Air Defence to provide realistic targeting practice without expending precious surface-to-air missiles.

On the other hand, AR is being recognised as one of the major breakthroughs for mechanised operations, a fact that has been acknowledged in the updated request for information (RFI) for see-through armour in the future-ready combat vehicle (FRCV) (53) which is slated to start domestic production in 2030 (54). A see-through armour combines data and footage from multiple sources, such as drones and nearby vehicles and overlays the same onto a tank gunner's sight enabling him to increase his field of view within the safety of the tank. The FRCV is also supposed to be integrated with assets on land and air, ensuring a longer detection range and enhancing situational awareness, another reason why a tethered drone system has also been included in the FRCV RFI (55). The increasing importance of AR and VR systems in the Indian Armed Forces was also reflected during multiple editions of India's Def Expo, which have witnessed these systems being displayed for visiting dignitaries (56).

Conclusion

VR and AR systems have proliferated globally and have important uses in the military and civil domains. However, there are certain challenges that need to be met with before these new technologies can be considered safe and utilisable for the Indian Armed Forces. An important aspect of the psychological effects of long-term usage of VR applications has not been studied in detail for the armed forces. However, the extrapolation of certain studies on the impact of video games on Indian students and teenagers shows that online gaming can have an adverse impact on the emotional and behavioural development of young adults (57).

Moreover, it has been reported that youth between the ages of 12 and 25 who indulge in online gaming are more prone to committing violence in the physical world (58). Recruits applying for the military are generally in the age bracket of 17–19, and therefore, more vulnerable to being hooked to VR-based games. Some have termed the use of promotional video games and VR simulations by certain armies as 'militainment' (59). Ironically, the level of immersion sought within VR has to conform, in certain stimuli-based aspects, to the physical reality, thereby increasing the user's "sense of presence". This has to be balanced by constant monitoring and mentoring of the recruits. Another aspect that merits consideration is the cost–benefit analysis of saving on ammunition, training time, and pollution vis-à-vis the relatively high installation costs of simulators that will also require seamless connectivity, high-definition rendering software, specialised screens, and motion sensors. Obviously, this has to be calculated and analysed on a long-term rather than an immediate basis. With the receding cost of wearable technology and likelihood of indigenisation of chip production capacity, there is an opportunity for the VR and AR fields to be enmeshed much more firmly with the armed forces, provided requisite safeguards are maintained.

Lt Col Akshat Upadhyay *is a Research Fellow in the Strategic Technologies Centre at the Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA).*

Endnotes

(1) Paul Milgram et al., "Augmented Reality: A Class of Displays on the Reality-Virtuality Continuum," *Telemanipulator and Telepresence Technologies* 282, no. 92 (2005), https://doi.org/10.1117/12.197321.

(2) "Gamification: What it is, How it Works, Risks," Investopedia, https://www.investopedia.com/terms/g/gamification.asp.

(3) J. Huizinga, *Homo Ludens: A Study of the Play-Element in Culture* (Boston: Beacon Press, 1950), 89-105.

(4) A. B. Bhattacharya, *The Man from the Future: The Visionary Life of John von Neumann* (Manchester: Allen Lane, 2021), 143.

(5) F. M. Fisher, "Games Economists Play: A Noncooperative View," *The RAND Journal of Economics* 20, no. 1 (1989), https://www.jstor.org/stable/2555655.

(6) G. Schaub Jr, "Deterrence, Compellence, and Prospect Theory," *Political Psychology* 25, no. 3 (2004), https://www.jstor.org/stable/3792549.

(7) G. Oakes, "The Cold War Conception of Nuclear Reality: Mobilizing the American Imagination for Nuclear War in the 1950's," *International Journal of Politics, Culture, and Society* 6, no. 3 (1993), http://www.jstor.org/stable/20007095.

(8) Sean Carroll, "Andrew Pontzen on Simulations and the Universe," Sean Carroll's Mindscape: Science, Society, Philosophy, Culture, Arts, and Ideas, June 19, 2023, https://www.preposterousuniverse.com/podcast/.

(9) Ty McCormick, "Gamification: A Short History," *Foreign Policy*, June 24, 2013, https://foreignpolicy.com/2013/06/24/gamification-a-short-history/.

(10) N. Gutierrez, "The Ballad of Morton Heilig: On VR's Mythic Past," *Journal of Cinema and Media Studies* 62, no. 3 (2023), https://muse.jhu.edu/article/893520/summary.

(11) Michael A. Gigante, "Virtual Reality: Definitions, History and Applications," *Virtual Reality Systems* 3, no.14 (1993), https://doi.org/10.1016/B978-0-12-227748-1.50009-3.

(12) Jaron Lanier, *Dawn of the New Everything: Encounters with Reality and Virtual Reality* (New York: Henry Holt and Company, 2017), 39.

(13) Gigante, "Virtual Reality: Definitions, History and Applications"

(14) A. Lele, "Virtual Reality and its Military Utility," *Journal of Ambient Intelligence and Humanized Computing* 4, no. 1 (2013), https://doi.org/10.1007/s12652-011-0052-4.

(15) Department of Computer Science of the University College of London, "A Note on Presence Terminology by M.L. Slater," University College of London, http://www0.cs.ucl.ac.uk/research/vr/Projects/Presencia/ConsortiumPublications/ucl_cs_papers/presence-terminology.htm.

(16) Department of Computer Science of the University College of London, "A Note on Presence Terminology by M.L. Slater"

(17) Virtual Reality Society, "Virtual Reality Tracking Systems - Virtual Reality Society," https://www.vrs.org.uk/virtual-reality-gear/tracking.html.

(18) K. K. Bhagat et al., "A Cost-Effective Interactive 3D Virtual Reality System Applied to Military Live Firing Training," *Virtual Reality* 20, no. 2 (2016), https://doi.org/10.1007/s10055-016-0284-x.

(19) A. Lugmayr et al., "Serious Storytelling – a First Definition and Review," *Multimedia Tools and Applications* 76, no. 14 (2017), https://doi.org/10.1007/s11042-016-3865-5.

(20) J. J. Kozak et al., "Transfer of Training from Virtual Reality," *Ergonomics* 36, no. 7 (1993), https://doi.org/10.1080/00140139308967941.

(21) M. W. Boyce et al., "Enhancing Military Training Using Extended Reality: A Study of Military Tactics Comprehension," *Frontiers in Virtual Reality* 3 (2022), https://doi.org/10.3389/frvir.2022.754627.

(22) J. J. Vogel-Walcutt et al., "Instructional Strategies Framework for Military Training Systems," *Computers in Human Behavior* 29, no. 4 (2013), https://doi.org/10.1016/j.chb.2013.01.038.

(23) Grigore C. Burdea, "Teaching Virtual Reality: Why and How?" *Presence: Teleoperators and Virtual Environments* 13, no. 4 (2004), https://doi.org/10.1162/1054746041944812.

(24) Yun-Chieh Fan et al., "A Virtual Reality Soldier Simulator with Body Area Networks for Team Training," *Sensors* 19, no. 3 (2019), https://doi.org/10.3390/s19030451.

(25) Lotte Linssen et al., "Using Accelerometry and Heart Rate Data for Real-Time Monitoring of Soldiers' Stress in a Dynamic Military Virtual Reality Scenario," *Multimedia Tools and Applications* 81, no. 17 (2022), https://doi.org/10.1007/s11042-022-12705-6.

(26)D. A. Overton, "State-Dependent Learning Produced by Depressant and Atropine-Like Drugs," *Psychopharmacologia* 10, no. 1 (1966), https://pubmed.ncbi.nlm.nih.gov/5982984.

(27) A. M. Kelley et al., "Evaluation of the Military Functional Assessment Program: Preliminary Assessment of the Construct Validity Using an Archived Database of Clinical Data," *Journal of Head Trauma Rehabilitation* 30, no. 4 (2015), https://pubmed.ncbi.nlm.nih.gov/24922040.

(28) M. D. Sharma, "Indian Air Force and US Air Force Spatial Disorientation Countermeasure Training: A Comparison," *Indian Journal of Aerospace Medicine* 59, no. 1 (2015), https://indjaerospacemed.com/indian-air-force-and-us-air-force-spatial-disorientation-countermeasure-training-a-comparison.

(29)Z. Meng et al., "Research on High-tech Ammunition Training System Based on Virtual Reality Technology," *MATEC Web of Conferences* 128 (2017), https://doi.org/10.1051/matecconf/201712801012.

(30) A. Rizzo et al., "Virtual Reality Goes to War: A Brief Review of the Future of Military Behavioral Healthcare," *Journal of Clinical Psychology in Medical Settings* 18, no. 2 (2011), https://doi.org/10.1007/s10880-011-9247-2.

(31) Andrew Ortony, Gerald L. Clore, and Allan Collins, *The Cognitive Structure of Emotions* (Cambridge: Cambridge University Press, 2022), 34.

(32) S. Rauch et al., "Emotional Processing Theory (EPT) and Exposure Therapy for PTSD," *Journal of Contemporary Psychotherapy* 36 (2006), https://link.springer.com/article/10.1007/s10879-006-9008-y.

(33) F. Pallavicini et al., “Virtual Reality Applications for Stress Management Training in the Military,” *Aerospace Medicine and Human Performance* 87, no. 12 (2016), https://doi.org/10.3357/AMHP.4596.2016.

(34) B. O. Rothbaum et al., “Effectiveness of Computer-Generated (Virtual Reality) Graded Exposure in the Treatment of Acrophobia,” *The American Journal of Psychiatry* 152, no. 4 (1995), https://pubmed.ncbi.nlm.nih.gov/7694917.

(35) D. A. Bowman et al., “Virtual Reality: How Much Immersion Is Enough?” *Computer* 40, no. 7 (2007), https://doi.org/10.1109/MC.2007.257.

(36) Tim Bradshaw, “Gaming Industry Puts Generative AI to the Test,” *Financial Times*, June 27, 2023, https://www.ft.com/content/58ddd586-0c06-4d67-9215-54b14b4fc1b1.

(37) Research and Technology Organisation, “Virtual Reality: State of Military Research and Applications in Member Countries,” North Atlantic Treaty Organisation, https://apps.dtic.mil/sti/pdfs/ADA411978.pdf.

(38) Nick Wingfield and Mike Isaac, “Pokémon Go Brings Augmented Reality to a Mass Audience,” *The New York Times*, July 11, 2016, https://www.nytimes.com/2016/07/12/technology/pokemon-go-brings-augmented-reality-to-a-mass-audience.html.

(39) James Webb Space Telescope, “Frequently Asked Questions Lite,” Goddard Space Flight Centre, https://webb.nasa.gov/content/about/faqs/faqLite.html#:~:text=Although%20Webb%20images%20are%20infrared,just%20as%20beautiful%20as%20Hubble%E2%80%99s.

(40) David Eagleman, “Can We Create New Senses for Humans?” Inner Cosmos with David Eagleman, https://eagleman.com/podcast/can-we-create-new-senses-for-humans.

(41) X. You et al., “Survey on Urban Warfare Augmented Reality,” *ISPRS International Journal of Geo-Information* 7, no. 2 (2018), https://doi.org/10.3390/ijgi7020046.

(42) Trond Nilsen, “Tankwar: AR Games at Gencon Indy 2005” (paper presented at the 2005 International Conference on Augmented Tele-Existence, Christchurch, New Zealand, December 5-8, 2005).

(43) W. Wang et al., “Augmented Reality in Maintenance Training for Military Equipment,” *Journal of Physics: Conference Series* 1626, no. 1 (2020), https://doi.org/10.1088/1742-6596/1626/1/012184.

(44) X. Qiao et al., “Web AR: A Promising Future for Mobile Augmented Reality—State of the Art, Challenges, and Insights,” *Proceedings of the IEEE* 107, no. 4 (2019), https://doi.org/10.1109/JPROC.2019.2895105.

(45) Ministry of Defence, Government of India, https://pib.gov.in/Pressreleaseshare.aspx?PRID=1917883.

(46) Vaibhav Jha, “Explained: Project WARDEC – India’s Upcoming AI-Powered Wargame Centre,” *The Indian Express*, May 21, 2022, https://indianexpress.com/article/explained/explained-project-wardec-india-ai-powered-wargame-centre-7928387/.

(47) Centre for the Fourth Industrial Revolution, & Frontiers Media, “Top 10 Emerging Technologies of 2023,” World Economic Forum, https://www3.weforum.org/docs/WEF_Top_10_Emerging_Technologies_of_2023.pdf?_gl=1*xhg1kg*_up*MQ..&gclid=Cj0KCQjw7uSkBhDGARIsAMCZNJuUACSApsUoc1trCFBGB2W0L2_mtHLhcTVqV8ZpohbK45PYHPYPPMkaAjiQEALw_wcB.

(48) “Indian Military Would Be Implementing AI-Based Wargame in Project WARDEC,” *Businessworld*, November 11, 2022, https://www.businessworld.in/article/Indian-Military-Would-Be-Implementing-AI-based-Wargame-In-Project-WARDEC/11-11-2022-453709.

(49) Bharat Sharma, “Armies Around the World are Training in Virtual Reality with India’s “HoloSuit”,” *India Times*, July 5, 2022, https://www.indiatimes.com/technology/news/armies-around-the-world-are-training-in-virtual-reality-with-indias-holosuit-573912.html.

(50) Abhijit Ahaskar, “Military Turns to AR/VR for Combat and Training Pilots,” *LiveMint*, March 9, 2022, https://www.livemint.com/technology/military-turns-to-ar-vr-for-combat-and-training-pilots-11646847576618.html.

(51) Yuvraj Tyagi, “Indian Army Adopts Virtual Reality to Secure the LOC Amid Modernisation Bid,” *Republic World,* January 25, 2023, https://www.republicworld.com/india-news/general-news/indian-army-adopts-virtual-reality-to-secure-the-loc-amid-modernisation-bid-articleshow.html.

(52) Indian Defence News, “Indian Army’s Orders for RPAV, VR-Based Missile Simulator, MQ-9B Contract Ending,” YouTube video, July 25, 2023, https://www.youtube.com/watch?v=l5kAbEwdJ-s#:~:text=Today’s%20Latest%20Indian%20Defence%20News/Indian%20defence%20Updates,Army’s%20Orders%20for%20RPAV%20%2CVR%2DBased%20Missile%20Simulator%2CMQ%2D9B.

(53) “Why Indian Army is Seeking “Future Tanks” Amid Tensions with China,” *WION News*, June 4, 2021, https://www.wionews.com/india-news/why-indian-army-is-seeking-future-tanks-amid-tensions-with-china-389540.

(54) Dinakar Peri, “Army Pushes New Tank and Armoured Carrier Projects,” *The Hindu*, August 27, 2022, https://www.thehindu.com/news/national/army-pushes-new-tank-and-armoured-carrier-projects/article65818881.ece.

(55) Ajay Banerjee, “The Tank, Mechanised Makeover: Armoured Corps and Mechanised Infantry are Undergoing their Biggest Transformation,” *The Tribune*, October 9, 2022, https://www.tribuneindia.com/news/features/the-tank-mechanised-makeover-armoured-corps-and-mechanised-infantry-are-undergoing-their-biggest-transformation-439548.

(56) Ministry of Defence, Government of India, https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1602542.

(57) A. Singh et al., “Online Gaming and its Association with Emotional and Behavioral Problems Among Adolescents – A Study from Northeast India,” *Archives of Mental Health* 21, no. 2 (2020), https://doi.org/10.4103/AMH.AMH_20_20.

(58) Sheezan Nezami, “Online Gaming Takes a Toll on Mental Health of Teenagers,” *The Times of India*, May 30, 2022, https://timesofindia.indiatimes.com/city/patna/online-gaming-takes-a-toll-on-mental-health-of-teenagers/articleshow/91877043.cms.

(59) Peter Singer, “War Games,” Brookings, February 22, 2010, https://www.brookings.edu/articles/war-games.

The Future of Competition and Warfare in Cyberspace

Nishant Rajeev

THE RUSSIA-UKRAINE WAR that began in February 2022 is now in its second year with no clear end in sight. At the outset of the war, analysts expected cyberattacks to play a key role in the war. Analysts expected an opening offensive cyber campaign, aiming to paralyse digital networks as tanks rolled across the Ukrainian border (1). Such analysis is usually buttressed in a deeper belief that in the cyber realm, offensive operations are easier to execute than defensive ones (2). However, as in the case of physical war, the digital war has not lived up to expectations. Russia's cyber operations, although extensive, have had a negligible impact on battlefield outcomes during the war.

While Russia failed to or simply was unable to leverage cyber capabilities to improve its military effectiveness in the Russia-Ukraine war, cyberspace still remains an arena of conflict. According to one report, nearly 72 percent of businesses worldwide have faced ransomware attacks in 2023, up from 55 percent in 2018 (3). These attacks are not limited to businesses and commercial enterprises. Criminal entities operating in cyberspace have managed to attack and hold at ransom critical infrastructure as well (4). States have also used cyberspace to pursue strategic goals, both for intelligence collection and physical destruction. An example of the former was the SolarWinds hack in 2020 by Russia on the US (5). Perhaps the most famous instance of the latter was Operation Olympic Games, the US and Israeli sabotage of the Iranian nuclear programme in 2009-10 (6). There is also speculation that the US had prepared more expansive cyber operations against Iranian and North Korean nuclear programmes (7).

This paper analyses the trends of how states compete in cyberspace. It does so in two dynamic situations. First is a competitive dynamic, where adversarial states are competing with each other but are not in an open armed conflict. Here, states typically have disputes, and at times, tend to be in open confrontation. They usually vie for a more strategically advantageous position within the global international system without resorting to armed conflict. The second situation is where states are in open armed conflict or war. The paper analyses how cyberspace can be leveraged in these two situations to further the strategic objectives of competing states. It argues that it is easier for states to leverage cyber capabilities in the competitive dynamic than in the armed conflict or wartime dynamic. This is mainly due to the unique nature of cyber capabilities.

The scope of this paper will be limited to computer network exploitation and attacks. These are usually employed for the purposes of intelligence collection, network disruption and degradation, and somewhat rarely, physical destruction. This paper will not cover issues related to misinformation operations and political propaganda. To be clear, misinformation and propaganda are important elements of a state's ability to leverage cyber capabilities to further strategic goals. It is also a significant part of Russia's cyber operations in the Ukraine war. However, due to constraints of space, the author has chosen to focus solely on the former set of issues.

This essay proceeds as follows. First, it gives an overview of current geopolitical and strategic context in which cyber capabilities will be deployed. It then provides an overview of the unique characteristics of cyber weapons. Third, the essay analyses how these unique characteristics can be advantageous or disadvantageous in competition and armed conflict dynamics. Finally, the paper ends by summarising the conclusions of this approach and presents some lessons for the future.

Geopolitical Context of Current Cyber Conflicts

The Russian invasion of Ukraine was the first large-scale conventional war to occur in Europe since the Second World War. Now, the expectation is that large-scale conventional wars are back in favour (8). Analysts have begun to make predictions on the next war even as the ongoing Russia-

Ukraine war is yet to conclude. The most hype is around the potential for conflict in the Taiwan Straits, driven by China's desire to reunite Taiwan with Mainland China. Some senior military officials claim that a war with China over Taiwan could come as early as 2025 (9). Others have alluded to a longer timeframe, with the invasion date being closer to 2030 (10). However, other theatres of conflict also appear to be flaring up, India and China engaged in bloody clashes along their disputed border in the Himalayas in June 2020 being one. The military standoff between the Himalayan neighbours is still ongoing. Following this and Russia's invasion of Ukraine, India's Chief of Defence Staff Gen. Anil Chauhan suggested that India needs to prepare for long conventional wars as well as short and swift wars (11).

Prior to Russia's invasion of Ukraine, the expectation was that wars would be less bloody and costly (12) as well as short and swift. In fact, many believed that states would aim to achieve their revisionist objectives through more indirect means using proxies and militias or that states would compete in the grey zone and avoid direct armed confrontation with each other, sometimes referred to as non-kinetic warfare. Lawrence Freedman defines this form of competition as a "high-level of conflict that is essentially non-violent" (13). More precisely, he notes that non-kinetic warfare is a "struggle for advantage that might take place before the outbreak of full-scale war" (14). However, Freedman's definition might be narrow in its scope. The "struggle for advantage" need not be limited only to the activity or timeframe preceding the outbreak of war. Harknett and Smeets note that states pursue broader goals such as to strive to achieve strategic advantageous positions in the global international system. For them, strategic advantage is "an outcome in which a relative change occurs in the bilateral, regional, or global distribution of power in the favour of the actor" (15).

Russia's invasion of Ukraine has grossly undermined the international norm of respecting territorial integrity of sovereign countries. However, the desire for countries, even revisionist and authoritarian ones, to engage in large-scale wars may not be as pronounced. Despite rising tensions and intensifying geopolitical rivalries, countries have demonstrated restraint. India and China are engaged in bilateral negotiations to defuse the tensions along their borders, although it has not resulted in total disengagement of forces (16). US Defence Secretary Loyd Austin and others cast doubt on claims that the invasion of Taiwan is imminent (17). Colin Kahl has suggested that China still seeks to "resolve the Taiwan issue without having to resort to force" (18).

It is these two geopolitical dynamics in which this paper assesses the utility of cyber capabilities. The former, which is referred here as the 'wartime dynamic', is when states are engaged in armed conflict against each other. The latter, referred to here as the 'competition dynamic', is when states are looking to achieve advantages over others or improve their position within the international system. The paper will assess the utility of cyber operations within these two dynamics.

Unique Attributes of Cyberspace and Cyber Weapons

Perhaps the most unique attribute of the cyber domain is its ubiquity. Cyberspace has proliferated in almost all aspects of human life in developed countries and is increasingly doing so in the developing world. Lucas Kello defines cyberspace as "comprising three partially overlapping terrains: (a) the internet, encompassing all interconnected computers, including (b) the world wide web, consisting only of nodes accessible via a URL interface; and (c) a cyber "archipelago" comprising all other computer systems that exist in theoretical seclusion (i.e., not connected to the internet or the web)" (19). Thus, cyberspace is a network of interconnected devices that allow information to flow through one another. This quality of cyberspace is key to strategic action. It gives adversaries the ability to theoretically access any point in cyberspace regardless of their physical location. The ubiquity of cyberspace also makes it possible for attackers to bypass the traditional physical barriers and access secure locations. This includes perimeter security measures to prevent espionage and sabotage and armed defenders meant to prevent any physical destruction within a state's territory. Accessing secure facilities remotely and lack of physical contact between attacker and defender makes the risk of orchestrating attacks low. Hackers cannot be targeted individually, and states can plead deniability.

Deniability is one of the key advantages of the cyber realm. Some scholars have characterised this as an attribution problem (20). However, in many cyberattacks, states have been able to identify the perpetrators with a fair degree of accuracy. The US public attribution of Russia's election interference and its attack on the Internet Research Agency is one example (21). The issue, therefore, is the ability to link the state's intentions to the activity of non-state actors. States can deny any link to non-state actors who perpetrate cyberattacks. In many cases, states even deny their involvement in cases where state-based actors have been suspected of cyberattacks. This gives state actors a shield to protect them from direct retaliation. In several cases, states are able to act through non-state actors or proxies to accomplish strategic goals, an issue that will be discussed further below.

One of the main advantages of cyber operations is its flexibility. Cyber weapons are usually tailormade for specific tasks they undertake and networks they need to penetrate. Cyber means can be used to conduct a range of operations—infiltration and extraction, disruption, degradation, and destruction. Once infiltration is achieved, the attacker can choose to simply extract data or disrupt and degrade networks. Ransomware gangs follow this model where they threaten to disrupt infiltrated networks if a ransom amount is not paid. Furthermore, the inherent reversibility of a cyberattack, where no physical damage is caused, makes it an attractive option. It allows states to keep their activities below the threshold of armed conflict, lowering the threat of kinetic retaliation. The cyber option allows states and other actors to calibrate their actions depending on whether the goal is espionage, signalling, or coercion.

An important caveat to note here is that not all actors in cyberspace can undertake all these activities. Through his study on the Stuxnet virus, Jon Lindsay shows that destructive attacks, especially on secure facilities, require considerable time and resources to accomplish (22). Indeed, the more sophisticated an attack, the more likely it is that only a select group of actors can execute it. Special payloads developed by attackers are needed to tailor the effects of a cyberattack. Another analyst notes that "a cyberweapon could not create an effect without being tailor-made for a specific target's digital and physical environment. In short, this requires ICS [Industrial Control Systems] schematics, network maps, application developers, cryptographers and a virtual environment replicating the target to the sensor or weapons tests before deployment" (23).

Cyber operations, especially ones that are extremely complex, do have disadvantages. First is that they are not a particularly responsive tool.

They cannot be easily transformed to execute different tasks out of their originally intended tasks. Furthermore, actors need a significant amount of time to prepare for cyber operations. The preparations for such attacks are long-drawn-out because if detected and the vulnerabilities of the network repaired, then recreating the attack becomes even more challenging. Thus, there is a premium on stealth and secrecy. Both these aspects were key factors that shaped planning for the above-mentioned cyber operations.

This brings us to another shortcoming of cyber operations. Several cyberattacks are reliant on zero-day exploits. A zero-day exploit "is a cyberattack vector or technique that takes advantage of an unknown or unaddressed security flaw in computer software, hardware or firmware" (24). However, if detected by the defender, the flaw will lose its utility for further attack. Essentially, if the vulnerability becomes known to the defender, then the attacker needs to find another way into the network. This may also be a time-consuming process. In this sense, cyber weapons have a "single use" characteristic to them (25).

The advantages of cyber weapons make it useful in some scenarios but difficult to employ in others. Given their technical attributes, the next section will analyse the political circumstances in which cyber weapons can be effectively employed. The political circumstances have been broken down into two types—the competitive dynamic and wartime dynamic.

Cyber Operations in Competition and War

In the current geopolitical environment, geopolitical rivalry has intensified as states compete to seek strategically advantageous positions within the international system. Furthermore, Russia's invasion of Ukraine has eroded the norm of the non-use of military force to change territorial status quos. Thus, states wish to avoid war, even as they prepare for it. Cyber capabilities are seen as integral means to achieve both these ends. Cyber operations can support a state's strategy to improve its position, i.e., in the competitive dynamic. Cyber operations are also perceived to be force multipliers in warfare, allowing states to degrade and destroy an adversary's military power before and during a war, i.e., in the wartime dynamic. However, trends in the real-world highlight that while cyber operations are useful in competitive dynamics, their utility declines in wartime dynamics.

Cyber Operations in the Competitive Dynamic

There are two key characteristics in the competitive dynamic that need to be considered for cyber operations. Firstly, geopolitical competitions are long-drawn-out affairs. In war, time can be a source pressure. Militaries and their commanders need to react quickly to enemy attacks and windows of opportunity for one's own attacks can be small. The luxury of long preparations is usually absent. However, geopolitical rivalries can take place over decades. Think of the Cold War or the ongoing US-China rivalry. This gives countries time to plan their actions, sometimes taking incremental steps to bolster their positions in the international system. Secondly, the competition tends to encompass several arenas, including military, economic, political narratives, and legitimacy. Each can be leveraged independently or together to further a state's objectives. States aim to enhance their capabilities in some or all these domains.

These dynamics are ideally suited for cyber operations, given cyber operations' technical characteristics. As geopolitical competition tends to encompass several areas, it also increases the number of cyberattack targets. This allows states in competition to leverage a key aspect of cyberspace: its pervasiveness. The digital domain is used by the military, commercial enterprises, and the media to enhance the quality and effectiveness of their operations. However, cyberattacks can be used to penetrate all these sectors to steal information or disrupt their operations as well. Cyberattacks, for instance, have not been limited to secure facilities like military networks, defence companies, and energy sectors. They have been used to attack banks, commercial manufacturers, and health service providers, and to propagate false narratives. The data stolen or operations disrupted can have consequences on a state's ability compete economically and militarily. Furthermore, information operations that propagate false narratives can bolster support for an adversary's actions. This can be targeted both at a domestic audience of an adversary state or at international audiences. The digital domain's growing ubiquity also allows a geographically distant state's networks to be penetrated and its data to be stolen. The long-drawn-out nature of geopolitical competition also allows states to plan cyber operations for specific targets. It allows time for information on the target to be collected, attacks to be planned, and cyber weapons to be developed that are tailored to the target. It allows for patient preparations, thereby also enabling cyberattacks to be stealthy. Thus, cyber attackers can infiltrate computer networks with a higher chance of success. Both Operation Olympic Games of 2009–10 and the SolarWinds hack in 2020 took over a year to execute at least (26). The initial preparations for both attacks may have taken even longer. Ultimately, a combination of the reversibility of cyber disruption and degradation and its deniability keep conflicts below the threshold of war.

Diverging from the traditional debate on the efficacy of cyberwarfare, Harknett and Smeets discuss the utility of cyber campaigns in furthering a state's strategic objectives. For them, "A cyber campaign refers to a series of coordinated cyber operations, which take place over time, to achieve a cumulative outcome leading to strategic advantage" (27). They have used the US-China cyber competition and the Chinese theft of US military secrets as a case study.

This understanding and approach can be extended to other examples as well, such as North Korean cyber operations. North Korean hackers and ransomware gangs are frequently used by the DPRK government for cyber theft. For North Korea, this is an effective means to circumvent the sanctions regime. According to one report, North Korea earns over half its foreign currency from cyberattacks. In 2022, the amount estimated to be stolen was nearly US$700 million (28). The Lazarus hacker group based in North Korea is suspected of stealing US$1.75 billion since its inception (29). The group's most notorious heist was likely that of Singapore's cryptocurrency exchange, estimated at US$275 million (30). Its thefts are used to partly fund North Korea's nuclear programme. North Korean hackers have also targeted the Indian Space Research Organisation and nuclear facilities (31), and also stole "technology-related data" from a nuclear plant's administrative computer networks (32). Although the cyber intrusions occurred in 2019, efforts to hack into these institutions began in 2018. Data and information stolen from both these institutions can be used to further North Korea's own nuclear and space programmes. Iran, another country under sanctions, is also known to use cyberattacks for commercial espionage, albeit to a much lesser degree (33).

Cyber Operations in the Wartime Dynamic

Several of the advantages of the competition dynamic do not translate into wartime dynamic. Firstly, time is usually of the essence, as alluded to above. Actions need to be highly coordinated and ideally undertaken swiftly. Timelines for offensive, counter-offensive, and defensive campaigns are dependent on windows of opportunity. These can be highly compressed or based on small timeframes. Secondly, the target sets in a war campaign are usually the adversary's military forces and their supporting infrastructure. In some cases, a country's critical infrastructure can also be targeted, but the primary effort is directed towards the adversary's military. Thirdly, destruction rather than degradation is the preferred option while conducting a war. The effects on an adversary's military need to have permanence. Otherwise, the adversary's forces and platforms can just be redeployed to hinder military efforts later.

The technical characteristics of cyber operations make its wartime application challenging. As noted above, the pressure of time always exists in war. This can adversely affect cyber operations, which need to be responsive to the evolving physical battlefield conditions. Cyber weapons need to be deployed quickly to respond to physical operations, such as responding to enemy counterattacks or bringing down defences. However, cyberattacks take time to execute. Coordinating between cyberattacks and physical attacks is the most challenging task and has not been done successfully till date. In an effort to quickly penetrate networks, infiltrations can be discovered, and vulnerabilities patched. Pre-war planning of cyber operations could potentially alleviate the time pressures of wartime operations. Hypothetically, they could be used to penetrate networks prior to an opening offensive and the two campaigns could be launched simultaneously. However, they would face two more technical challenges—a narrow and select target set, and the element of reversibility in cyberattacks. Cyberattacks during wartime will mostly be targeted at military systems and other critical services. These systems tend to be much more secure networks than the ones found in the civilian and commercial enterprises. Given higher levels of security, cyberattacks would be more time-consuming. This again does not make them very responsive tools and ill-placed to support fast-moving kinetic operations. Finally, the reversibility of cyberattacks is a disadvantage. The damage caused by cyberattacks that are meant to disrupt or even degrade can be reversed, putting systems back in field or at service after the attack has been dealt with. Again, if the initial vulnerabilities are detected and patched, regaining access to the system becomes all the more challenging.

The shortcomings of cyber operations during wartime have been borne out by the lacklustre effectiveness of Russia's cyber forces. Early analyses of Russia's cyber operations reveal that few of them actually made lasting effects (34). One report speculated that poor coordination between agencies responsible for cyber and kinetic operations and lack of skilled cyber forces are reasons for the limited effectiveness (35). More broadly, Kostyuk and Gartzke argue that cyber and kinetic operations are inherently difficult to coordinate, and therefore, cyber operations supporting or replacing kinetic operations are unlikely (36).

We will perhaps not know fully whether these technical characteristics hampered Russia's cyber operations. Information is right now limited as the war is still ongoing. As noted in the preceding paragraph, most analyses point to internal organisational failures rather than technical ones. However, when overlaid with what is known in general about cyber operations by analysing previous operations, it would be a fair assessment to say that cyber operations during wartime require very high technical proficiency. Another unknown key aspect is the extent of Western cyber operations in Russia. Western cyber capabilities are assumed to be better than Russian ones. The aggregate of the US' and Western Europe's capabilities will most likely overshadow that of Russia. A full understanding of the effectiveness of cyber operations during wartime will only be achieved by studying this data set.

Future of Competition and Warfare in Cyberspace

The analysis above suggests that, in looking ahead, there will be severe competition in cyberspace during times of intense geopolitical rivalry. This may not be limited to during military standoffs or diplomatic confrontations. However, its wartime utility will be limited, especially for those states that cannot raise the resources to build an effective cyber force.

In a competitive dynamic, cyber operations will be used to advance a state's geopolitical position. States can deploy either their own cyber forces or proxy forces for theft, espionage, or spreading propaganda. An actor like Russia, which is globally isolated due to economic sanctions and diplomatic condemnation, may increasingly rely on cyber means. This will include spreading misinformation to bolster its global image, accessing and stealing advanced technologies for its commercial sector, and engaging in espionage against its military adversaries. While the US has the capacity to withstand such attacks, other states will be vulnerable. The growing ubiquity of cyberspace in Africa, Asia, and Latin America present several "softer" targets for cyberattacks, propaganda and state-backed cybercrime. While this will not bring countries in military parity with the US, it can help advance key strategic and defence programmes and aid economic activity.

In a wartime dynamic, cyber operations are unlikely to change battlefield outcomes. To be sure, the Russian military's internal dysfunction further stymied the already difficult task of coordinating kinetic and cyber operations. However, even if internal organisational issues can be resolved, forces need to be trained and equipped. In the cyber domain, given the technical challenges, this will not be an easy task. However, one can expect cyber operations, especially in intelligence-gathering tasks, to play a central role. Furthermore, just prior to the outbreak of a war when time pressures are lower, states can expect cyberattacks to intensify, for the purpose of both intelligence collection and setting up disruptive attacks. Ultimately, the defending state's ability to effectively respond to cyberattacks will determine whether or not cyberattacks are successful.

Nishant Rajeev *is a senior analyst with the South Asia Program at the S. Rajaratnam School of International Studies, NTU in Singapore.*

Endnotes

(1) William Courtney, "If Russia Invaded Ukraine," RAND Blog, December 8, 2021, https://www.rand.org/blog/2021/12/expect-shock-and-awe-if-russia-invades-ukraine.html; Jason Healey, "Preparing for Inevitable Cyber Surprise," War on the Rocks, January 12, 2022, https://warontherocks.com/2022/01/preparing-for-inevitable-cyber-surprise/.

(2) William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89 (September-October 2010): 97–108.

(3) CyberEdge, "Annual Share of Organizations Affected by Ransomware Attacks Worldwide from 2018 to 2023," Statista, May 18, 2023, https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/.

(4) Stephanie Kelly and Jessica Resnick-ault, "One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators," *Reuters*, June 9, 2021, https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.

(5) "Solarwinds Hack Was 'Largest and Most Sophisticated Attack' Ever: Microsoft President," *Reuters,* February 15, 2021, https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R.

(6) Adam Leong Kok Wey, "These Olympic Games Launched a New Era of Cyber Sabotage," *The National Interest,* July 25, 2021, https://nationalinterest.org/blog/buzz/these-olympic-games-launched-new-era-cyber-sabotage-190082.

(7) In case of Iran, this plan was called Nitro Zeus. See David E. Sanger and Mark Mazzetti, "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *New York Times,* February 16, 2016, https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html; David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times,* June 1, 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html; In the case of North Korea, see William J. Board and David E. Sanger, "US Strategy to Hobble North Korea was Hidden in Plain Sight," *New York Times,* March 4, 2017, https://www.nytimes.com/2017/03/04/world/asia/left-of-launch-missile-defense.html.

(8) Dan Sabagh, "Traditional, Heavy Warfare Has Returned to Europe with Ukraine Conflict," *The Guardian,* March 6, 2023, https://www.theguardian.com/world/2023/mar/06/traditional-heavy-warfare-has-returned-to-europe-with-ukraine-conflict.

(9) Helen Davidson, "US General's 'Gut' Feeling of War with China Sparks Alarm Over Predictions," *The Guardian,* February 2, 2023, https://www.theguardian.com/world/2023/feb/02/us-general-gut-feeling-war-china-sparks-alarm-predictions.

(10) Mallory Shelbourne, "Davidson: China Could Try to Take Control of Taiwan in 'Next Six Years'," *USNI News,* March 9, 2021, https://news.usni.org/2021/03/09/davidson-china-could-try-to-take-control-of-taiwan-in-next-six-years.

(11) Amrita Nayak Dutta, "India Needs to Have Tech, Weapons to Fight a Swift as Well as a Long War: CDS," *The Indian Express,* March 4, 2023, https://indianexpress.com/article/

india/india-needs-to-have-tech-weapons-to-fight-a-swift-as-well-as-a-long-war-cds-8478328/.

(12) Sabagh, “Traditional, Heavy Warfare Has Returned to Europe with Ukraine Conflict”

(13) Lawrence Freedman, “The Language of War,” Substack, March 9, 2023, https://samf.substack.com/p/the-language-of-war.

(14) Freedman, “The Language of War”

(15) Richard J. Harknett and Max Smeets, “Cyber Campaigns and Strategic Outcomes,” *Journal of Strategic Studies* 45 (2022): 543.

(16) “Galwan Valley: A Year After the Violent Clash,” *The Indian Express,* June 14, 2021, https://indianexpress.com/article/india/galwan-valley-clash-timeline-india-china-disengagement-7358554/.

(17) “‘Seriously Doubt’ Imminent Invasion of Taiwan by China - Pentagon Chief,” *Reuters,* January 12, 2023, https://www.reuters.com/world/asia-pacific/seriously-doubt-imminent-invasion-taiwan-by-china-pentagon-chief-2023-01-11/.

(18) Joe Gould, “China Seizure of Taiwan Not ‘Imminent,’ Says Key Dod Official,” *Defence News,* February 7, 2023, https://www.defensenews.com/pentagon/2023/02/06/china-seizure-of-taiwan-not-imminent-says-key-dod-official/.

(19) Lucas Kello, “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft,” *International Security* 38 (Fall 2013): 17.

(20) Kello, “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft,” 33; Joseph S. Nye Jr., “Deterrence and Dissuasion in Cyberspace,” *International Security* 41 (Winter 2016/17): 49–52.

(21) Evan Perez and Theodore Schleifer, “US Accuses Russia of Trying to Interfere with 2016 Election,” *CNN,* October 18, 2016, https://edition.cnn.com/2016/10/07/politics/us-blames-russia-for-targeting-election-systems/index.html; Jen Kirby, “The US Launched a Cyberattack on a Russian Troll Factory During the 2018 Midterms,” *Vox,* February 26, 2019, https://www.vox.com/2019/2/26/18241654/us-cyberattack-internet-research-agency-russia-2018-elections.

(22) Jon R. Lindsay, “Stuxnet and the Limits of Cyber Warfare,” *Security Studies* 22, no. 3 (2013): 365–404.

(23) Panayotis A. Yannakogeorgos, “The Unique Characteristics of Cyber Weapons,” Atlantic Council, May 20, 2013, https://www.atlanticcouncil.org/blogs/natosource/the-unique-characteristics-of-cyber-weapons/; See also Panayotis A. Yannakogeorgos, “Keep Cyberwar Narrow,” *The National Interest,* May 17, 2013, https://nationalinterest.org/commentary/keep-cyberwar-narrow-8459.

(24) “What is a Zero-Day Exploit?” IBM, August 18, 2023, https://www.ibm.com/topics/zero-day.

(25) James A. Lewis, “Conflict and Negotiation in Cyberspace,” CSIS, 2013, https://csis-website-prod.s3.amazonaws.com/s3fs-public/130208_Lewis_ConflictCyberspace_Web.pdf; Max Smeets, on the other hand, highlights the connection between time and utility of cyberweapons by a characteristic he calls a cyberweapon’s ‘transitory property’. See

Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies* 41, no. 1-2 (2018): 6–32.

(26) Jon Lindsay has provided a detailed overview of the technical details of the Stuxnet attack. See Lindsay, "Stuxnet and the Limits of Cyber Warfare," 378–85. On the SolarWinds Hack, see Robert Chesney, "SolarWinds and the Holiday Bear Campaign: A Case Study For the Classroom," Lawfare, August 25, 2021, https://www.lawfaremedia.org/article/solarwinds-and-holiday-bear-campaign-case-study-classroom.

(27) Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," 541.

(28) Ryo Nakamura and Junnosuke Kobara, "North Korea Gets Half its Foreign Currency from Cyber Theft: U.S. Official," *Nikkei Asia Review,* June 5, 2023, https://asia.nikkei.com/Spotlight/N-Korea-at-crossroads/North-Korea-gets-half-its-foreign-currency-from-cyber-theft-U.S.-official#:~:text=The%20South%20Korean%20government%20estimated,from%20tech%20workers%20employed%20abroad.

(29) "Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to be Exploring New Money Laundering Options," *China Analysis,* February 9, 2021, https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack/.

(30) "Lazarus Group Pulled Off 2020's Biggest Exchange Hack"

(31) Stephanie Findlay, Edward White, and Song Jung-a, "Suspected North Korea Hackers Targeted Indian Space Agency," November 7, 2019, https://www.ft.com/content/ac6a8782-ffad-11e9-b7bc-f3fa4e77dd47.

(32) Sushovan Sircar, "Exclusive: N Korea Stole Data from Kudankulam Attack, Says Expert," *The Quint,* November 7, 2019, https://www.thequint.com/news/india/kudankulam-nuclear-power-plant-cyber-attack-malware-north-korea-stole-information-data#read-more.

(33) Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," Carnegie, January 4, 2018, https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf.

(34) Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," Carnegie Working Paper, December 16, 2022, https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

(35) Gavin Wilde, "Cyber Operations in Ukraine: Russia's Unmet Expectations," Carnegie Working Paper, December 12, 2022, https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607.

(36) Nadiya Kostyuk and Erik Gartzke, "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine," *Texas National Security Review* 5 (Summer 2022): 113–26, https://tnsr.org/2022/06/why-cyber-dogs-have-yet-to-bark-loudly-in-russias-invasion-of-ukraine/.

Exploring the Utility of Blockchain in Military Operations

Meghna Bal and Mohit Chawdhry

BLOCKCHAIN, OR DISTRIBUTED LEDGER TECHNOLOGY (DLT), garners some attention for its potential military applications. Developed as a decentralised peer-to-peer mechanism for global financial transactions in 2008, blockchain can potentially be applied across different warfighting domains, including communications, logistics, and cyber warfare (1). However, the relative nascency of the technology and some of its inherent characteristics also pose challenges for military adoption.

This essay explores the potential military applications of blockchain technology based on existing academic literature and prominent early-use cases. Broadly, findings suggest that while several advanced militaries are experimenting with blockchain technology, its utility in military operations is presently unproven.

Technological Overview

Blockchain technology first saw public prominence in 2008, when Satoshi Nakamoto published a whitepaper on Bitcoin, positing it as an alternative to the centralised financial system (2). In simple terms, a blockchain is a decentralised and distributed database or ledger. On a blockchain, each new transaction in the database is recorded and secured through cryptography, and verified by network participants (3).

As the description above indicates, several aspects of blockchain technology have utility for military operations.

1. **Immutability:** Blockchain technology deploys sophisticated encryption techniques and time stamps to make records immutable and tamper-proof.

2. **Provenance:** An immutable chain of transactions stored on a ledger enables charting the provenance of items both on- and off-chain.

3. **Verification:** Blockchain relies on consensus-based verification of transactions ensuring all stakeholders agree on the state of records before they are logged in the ledger.

The type of blockchain is also relevant when considering use cases for the military. Broadly, there are two types: permissioned and permissionless. In permissioned blockchains, validators are known and need to be granted special admittance to join the network. Permissionless open blockchain networks where anyone with the right software can serve as a node to validate and maintain a record of transactions have limited utility for most military operations, given the need for operational integrity, security, and confidentiality. However, there are instances where permissionless blockchain networks play an indirect role in facilitating warfighting, such as the evasion of sanctions.

Future Use Cases of Blockchain in Warfighting: A Survey of Global Developments

Table 1: Overview of military blockchain adoption in technologically advanced militaries

Use Case	China	Russia	South Korea	United Kingdom	United States
Procurement and Logistics	✓		✓		✓
Secure Communication Networks				✓	✓
Cyber Defence and Information Security	✓	✓			✓
Drone swarms and micro-UAV management	✓				

Source: Authors' analysis

The Use of Blockchain in Military Procurement and Logistics

Procuring weapons, ammunition, equipment, and rations is a central aspect of military operations. The supply chain and logistics network for the military are sensitive as they necessitate measures for both security and secrecy (4). These include a requirement for verifying the identities of individuals through the chain of procurement and tracking material provenance and location (preferably in real-time), which can be challenging (5). There is also a need to balance considerations of transparency to prevent resource leakage against those of national security.

The incorporation of blockchain technology can potentially address a number of these challenges. It can, for instance, enable the verification of identities of parties involved in defence procurement to plug potential leakages (6). Combining blockchain with other tracking technologies, such as Radio Frequency Identification, enables militaries to keep an eye on weapons stock by tracking items in real-time (7). It also limits the possibility of compromised records. Additionally, the tamper-resistant and immutable nature of the blockchain ensures that procurement-related documents cannot be manipulated to facilitate corruption (8).

These considerations possibly prompted the US Air Force and the South Korean military to initiate programmes to develop blockchain-based procurement networks. The US Air Force contracted with SIMBA Chain, a company providing government blockchain services, to develop a blockchain-based supply chain network that enables risk identification and mitigation of vulnerabilities in weapons and other equipment (9). Similarly, the South Korean Defense Acquisition Program Administration is working with other government entities and private companies to develop a DLT-based weapons logistics network that helps reduce fraud and increase overall efficiency (10).

Importantly, no technological solution is a silver bullet. Blockchain technology can enable internal transparency and informational immutability by enabling the creation of a network of nodes corresponding to relevant stakeholders, i.e., each important stakeholder represents a separate node. However, it can also be compromised if more than 50 percent of these nodes wish to override the system (either to delete or alter information). Similarly, while blockchain technology enables provenance tracking and identity verification, it will not be able to solve offline leakages or internal compromises where weapons stock is taken before it is entered into the system.

Secure Communication Networks

Similar to procurement, military communications require a high degree of security. Broadly, these networks may be prone to two types of attacks, depending on the degree of centralisation and/or lack of encryption. One, adversaries may use attacks to disrupt communications infrastructure to paralyse the relay of information between armed personnel (11). Two, communication systems may be compromised and used to provide combatants with incorrect information. Illustratively, a 2017 report by the Army Design Bureau, which spearheads technology acquisition and R&D efforts for the Indian military, suggests the Indian army's communication systems were riddled with security loopholes and were susceptible to infection with malware (12). The report states that these vulnerabilities arise due to the army's dependence on imported technology, which can be riddled with malware.

Blockchain-based frameworks may address these issues. They are encrypted, distributed, and decentralised, securing communications and mitigating against the limitations of a centralised system with a single point of failure.

The UK's Ministry of Defence has established a Cryptography Management System (CMS) that helps secure the sovereign security architecture used by all three of its military services. The CMS is a distributed application that gives the Ministry of Defence lifecycle control over communications equipment and encryption keys to help protect sensitive information from evolving global cybersecurity threats (13). The US Defense Advanced Research Projects Agency similarly issued a notice in 2016 seeking pitches for a secure messaging system that would use a decentralised ledger to broadcast secrets in an encrypted manner (14).

However, most blockchains suffer from the "Oracle problem." This refers to the inherent inability of blockchains to access external data as they are isolated networks bereft of connections to external data sources (15). It is this isolation that ensures their security and resilience. Oracles, or third-party middleware, are typically used to bridge the gap between blockchains and external data sources (16). As such, military blockchain communication networks will also need to use Oracles to monitor and transmit relevant data. However, relying on Oracles that are centralised or vulnerable to cyber threats can undo the security benefits of using a blockchain-based communication network in the first place (17).

Blockchain-based communication networks will also have to deal with "51 percent attacks," which occur when an adversary gains control of more than half of a network's validating nodes (18). Control over 51 percent or more of a blockchain's nodes allows the controlling entity to manipulate the consensus mechanism, effectively allowing them to alter or falsify records and transactions within the blockchain (19). This could lead to unauthorised access to confidential information, alteration of messages, or the complete disruption of communication channels (20). As such, militaries adopting blockchain networks for secure communications will have to carefully identify and authenticate the nodes responsible for validating information on the blockchain networks underlying their communication systems.

Cyber Defence

In addition to communication networks, weapons systems, navigation equipment, and other aspects of military operations are now digitalised and reliant on data, which makes them vulnerable to cyberattacks. Indeed, military and government entities have increasingly been the target of cyberattacks by state and non-state actors. For instance, in 2013, Indian Army personnel were targeted by a phishing attack that lured them into downloading and opening a malicious file that subsequently compromised their systems (21). Similarly, the notorious SolarWinds hack, carried out between March and June 2020, targeted a security vendor that provided services to the US Pentagon and other important departments (22).

Unlike the data environment currently used by military technologies, the blockchain is relatively more resilient and robust as it aggregates the power of the entire network to fend off malicious attacks (23). Moreover, the distributed and peer-to-peer network of blockchain networks helps ensure that any unauthorised tampering or reconfiguration of data by cyber attackers is immediately noticed (24).

These characteristics of blockchain networks have prompted the US, China, and Russia to explore their utilisation as cyber defence mechanisms. The Russian Ministry of Defence set up a specialised lab to examine the application of DLT to mitigate cybersecurity attacks in 2018 (25). Chinese media reports suggest that the nation's military is also exploring adopting blockchain to protect information systems and improve data reliability on the network (26). In the US, the National Defense Authorization Act of 2018 required the Secretary of Defense to brief Congress on blockchain technology's offensive and defensive cyber capabilities (27).

Drone Swarms and Micro-UAV Management

Militaries worldwide now use drones and unmanned aerial vehicles (UAVs) for surveillance and warfare operations. Such drones are remotely controlled and typically rely on wireless networks to receive information and instructions. However, research indicates that many drones used for military operations have serious design flaws and do not feature wireless security protection and encryption (28). The flaws make drones prone to interception, manipulation, and hijacking (29).

The underlying characteristics of blockchain technology, namely hashing, encryption, and decentralisation, can provide an effective solution for the security of drones. A 2019 paper suggests that blockchain-based hashing and encryption can form the basis for secure and resilient communications between drones and controlling stations, preventing interference by third parties (30). Moreover, DLTs could also form the basis for secure communication within a swarm of drones and UAVs. While there is limited information on the actual use of blockchain technology for drone swarm management, media reports from China suggest that the military is working on applying blockchain technology for the operational control of swarms (31).

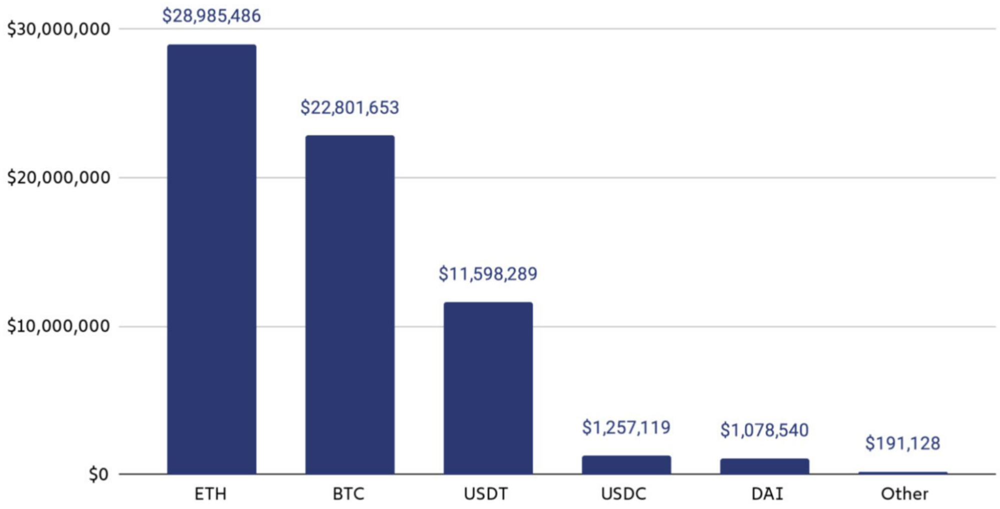
Case Study: Use of Blockchain and Crypto-Assets in the Ukraine-Russia War

The Ukraine-Russia war provides live examples of how these blockchain and crypto-asset technologies can be used during war.

Fundraising and Donations

Ukraine has turned to crypto assets to bolster its war efforts. Latest reports suggest that over US$212 million has been raised through various crypto assets, showcasing a significant contribution to the country's military and humanitarian needs (32). This includes direct financial support to the Ukrainian government for purchasing vital military equipment such as bulletproof vests, helmets, demining tools, and drones (33). Furthermore, the United Nations High Commissioner for Refugees, the premier international organisation for refugees, also accepts donations in more than 70 crypto assets to help deliver humanitarian aid in Ukraine (34). The fundraising efforts have also extended to the creative use of blockchain-based non-fungible tokens (NFTs), unique digital assets representing ownership of specific items. One notable instance was the auctioning of a Ukrainian flag NFT for US$6.5 million (35).

Figure 1: Cryptocurrency sent to Ukraine donation wallets (February 2022-February 2023)



Source: Chainalysis (36)

Conversely, approximately 100 pro-Russian groups raised nearly US$5.4 million through digital currencies (37). These funds, channelled primarily through Russian crypto-asset exchanges, have been used to support the operation of the Russian military and other sanctioned para-military organisations, such as the Wagner Group (38).

Statements from government officials and humanitarian organisations suggest that the inherently transparent nature of blockchain-based crypto-asset transfers makes them suitable for fundraising and donations (39). The blockchain is a decentralised and distributed ledger of all transactions conducted over a particular network. Anyone with access to the network can view the entire history of transactions using the blockchain. As such, donors enjoy greater visibility over how their contributed funds are being used (40). The relatively fast and seamless nature of cross-border crypto-asset transfers also makes them a viable option for donations. Unlike other forms of cross-border payments, crypto-asset transfers do not involve intermediaries like banks and payment networks, whose functioning may be unreliable during wartime (41).

However, using crypto-assets for wartime fundraising is not without its risks. Indeed, the value of crypto-assets is inherently volatile and can prompt fluctuations in the corpus of donated funds.

Sanctions Evasion

Financial sanctions have become a critical tool in modern warfare, allowing nations to exert economic pressure and influence without resorting to military force. They are used to restrict access to financial resources, impede economic activities, and isolate individuals or entities involved in aggression or other illicit activities (42). In the context of the Ukraine-Russia war, crypto-assets have emerged as a potential means to circumvent sanctions imposed on the Russian government and known supporters of the government. Their decentralised and pseudonymous nature can facilitate cross-border transactions outside traditional banking channels, potentially bypassing regulatory oversight (43). However, an analysis of blockchain data does not show a marked increase in the flow of crypto-assets to and from Russia in the aftermath of the sanctions, suggesting that the use of such assets for sanctions evasion may not be widespread. Moreover, the limited liquidity of crypto-asset markets precludes their use for constantly mobilising large sums of money, as sanctions evasion would require (44).

Recording Human Rights Abuses

The recording of war crimes is an intricate and delicate process. Inaccessible war zones, time-sensitive materials, and the need for diverse and specialised collection methods often hinder evidence gathering. Furthermore, verification poses challenges in ensuring authenticity, maintaining an unbroken chain of custody, and navigating technological intricacies (45).

Blockchain technology has emerged as a potential solution to these challenges. For instance, Stanford-USC non-profit Starling Lab has documented war crimes committed by Russia in Ukraine using blockchain technology to prevent tampering (46). By placing evidence in a distributed ledger where multiple copies are kept and verified, the integrity of the truth is preserved. This process establishes the provenance of the data and allows prosecutors to show that it has not been tampered with from the field to the courtroom (47).

Conclusion

Overall, blockchain technology is relatively untested as nations explore its potential utility. Another important consideration is that these systems are not foolproof. Further, most use cases are largely experimental. Thus, it remains to be seen whether their deployment will be institutionalised in global militaries.

In the context of permissionless networks, there is some indication that technologies operating outside the financial mainframe of different countries can provide succour, particularly in wartime, where traditional institutions such as banks may be functioning erratically. At the same time, however, the small size of the crypto-asset market, relative to the intensive expenditure and cost of war, is likely to be a key limiting factor.

Meghna Bal *is the Head of Research and Fellow at the Esya Centre.*

Mohit Chawdhry *is a Fellow at the Esya Centre, specialising in digital assets, data protection, and digital antitrust.*

Endnotes

(1) Salvador Llopis Sanchez, "Blockchain Technology in Defence," European Defence Matters, 2017, https://eda.europa.eu/webzine/issue14/cover-story/blockchain-technology-in-defence.

(2) Satoshi Nakamoto, "Bitcoin: A Peer to Peer Electronic Cash System," 2008, https://bitcoin.org/bitcoin.pdf.

(3) Dylan Yaga et al., *Blockchain Technology Overview*, Maryland, National Institute of Standards and Technology, October 2018, https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf.

(4) Felix K. Chang, "Incentives Matter: Military Procurement Problems in India, Malaysia, and the United States," Foreign Policy Research Institute, January 3, 2014, https://www.fpri.org/article/2014/01/incentives-matter-military-procurement-problems-in-india-malaysia-and-the-united-states/.

(5) Linda Zamengo et. al., "Blockchain on Defence: A Breakthrough?" Finabel - European Army Interoperability Centre, September 8, 2020, https://finabel.org/wp-content/uploads/2020/09/FFT-Blockchain.pdf.

(6) Zamengo et. al., "Blockchain in Defence: A Breakthrough?"

(7) Rosanna Cole, Mark Stevenson, and James Aitken, "Blockchain Technology: Implications for Operations and Supply Chain Management," *Supply Chain Management: An International Journal*, no. 4 (June 11, 2019): 469–83, https://doi.org/10.1108/scm-09-2018-0309.

(8) Zamengo et. al., "Blockchain in Defence: A Breakthrough?"

(9) Danny Nelson, "US Air Force Gives Blockchain Firm $1.5M to Build Supply Chain Network," *CoinDesk,* June 16, 2020, https://www.coindesk.com/markets/2020/06/15/us-air-force-gives-blockchain-firm-15m-to-build-supply-chain-network/.

(10) Miranda Wood, "South Korea Reveals Blockchain Plans for Defense and Arms Procurement," *Ledger Insights,* August 6, 2019, https://www.ledgerinsights.com/south-korea-blockchain-defense-arms-procurement/.

(11) Y Zhu et. al., "A Study of Blockchain Technology Development and Military Application Prospects," *Journal of Physics: Conference Series* 1507, no. 5 (April 1, 2020), https://doi.org/10.1088/1742-6596/1507/5/052018.

(12) Rahul Singh, "Chinese Hackers Can Disrupt Indian Army's Communication Network: Report," *Hindustan Times*, January 20, 2017, https://www.hindustantimes.com/india-news/security-flaws-report-warns-chinese-malware-could-bring-indian-army-to-a-standstill/story-H2ckzU6xpZSIOTaHyldu6K.html.

(13) "UK MOD Hires CGI to Support its Cryptography Management System," Consultancy.uk, August 4, 2016, https://www.consultancy.uk/news/12368/uk-mod-hires-cgi-to-support-its-cryptography-management-system#:~:text=The%20UK%20Ministry%20of%20Defence,deal%20has%20not%20been%20disclosed.

(14) Stan Higgins, “DARPA Seeks Blockchain Messaging System for Battlefield Use,” *CoinDesk*, April 25, 2016, https://www.coindesk.com/markets/2016/04/25/darpa-seeks-blockchain-messaging-system-for-battlefield-use/.

(15) Chainlink, “What Is the Blockchain Oracle Problem?” October 3, 2023, https://chain.link/education-hub/oracle-problem#:~:text=The%20blockchain%20oracle%20problem%20refers,of%20markets%20and%20use%20cases.

(16) Chainlink, “What Is the Blockchain Oracle Problem?”

(17) Vinoth Venkatesan, “Oracles in the Crypto World,” *Australian Cybersecurity Magazine*, February 23, 2022, https://australiancybersecuritymagazine.com.au/oracles-in-the-crypto-world/.

(18) MIT Digital Currency Initiative, “51% Attacks,” https://dci.mit.edu/51-attacks.

(19) Tam T. Huynh, Thuc D. Nguyen, and Hanh Tan, “A Survey on Security and Privacy Issues of Blockchain Technology,” in *2019 International Conference on System Science and Engineering (ICSSE)*, 362–67, 2019, https://doi.org/10.1109/ICSSE.2019.8823094.

(20) Zamengo et. al., “Blockchain in Defence: A Breakthrough?”

(21) IANS, “Pak-Based Hackers Target Indian Army, Education Sector in New Cyber Attack,” *Economic Times*, June 24, 2023, https://government.economictimes.indiatimes.com/news/secure-india/pak-based-hackers-target-indian-army-education-sector-in-new-cyber-attack/101235241.

(22) Dina Temple-Raston, “A ‘Worst Nightmare’ Cyberattack: The Untold Story of the SolarWinds Hack,” *NPR*, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

(23) Zhu et al., “A Study of Blockchain Technology Development and Military Application Prospects”

(24) Neil B. Barnas, *Blockchains in National Defense: Trustworthy Systems in a Trustless World*, Maxwell Air Force Base Alabama, Air Command and Staff College, Blue Horizons Program, June 2016, https://www.jcs.mil/Portals/36/Documents/Doctrine/Education/jpme_papers/barnas_n.pdf.

(25) Muyao Shen, “The Russian Military is Building a Blockchain Research Lab,” *CoinDesk*, July 2, 2018, https://www.coindesk.com/markets/2018/07/02/the-russian-military-is-building-a-blockchain-research-lab/.

(26) Takahiro Tsuchiya, “China Promotes Emerging Technology for Dual Use: The Case of Blockchain Technology,” Japan Institute of International Affairs, 2021, https://www.jiia.or.jp/en/column/2021/05/06-china-promotes-emerging-technology-for-dual-use-the-case-of-blockchain-technology.html#sdfootnote9sym.

(27) “H.R.2810 - National Defense Authorization Act for Fiscal Year 2018,” December 12, 2017, https://www.congress.gov/bill/115th-congress/house-bill/2810#:~:text=The%20National%20Defense%20Authorization%20Act,Department%20of%20Energy%20(DOE).

(28) Jean-Paul Yaacoub et al., “Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations,” *Internet of Things* 11 (May 8, 2020), https://www.sciencedirect.com/science/article/pii/S2542660519302112#sec0033.

(29) Kim Hartmann and Keir Giles, “UAV Exploitation: A New Domain for Cyber Power” (paper presented at the 8th International Conference on Cyber Conflict, Tallinn, Estonia, May 31–June 3, 2016), https://ccdcoe.org/uploads/2018/10/Art-14-Assessing-the-Impact-of-Aviation-Security-on-Cyber-Power.pdf.

(30) Tarun Rana et al., “An Intelligent Approach for UAV and Drone Privacy Security Using Blockchain Methodology” (paper presented at the 9th International Conference on Cloud Computing, Data Science & Engineering, 2019), https://doi.org/10.1109/CONFLUENCE.2019.8776613.

(31) Tsuchiya, “China Promotes Emerging Technology for Dual Use”

(32) “A Year into Russia’s War on Ukraine, Cryptocurrencies Continue to Play a Key Role,” *Chainanalysis*, February 24, 2023, https://blog.chainalysis.com/reports/russia-ukraine-war-cryptocurrency-one-year/.

(33) Spencer Feingold, “Why the Role of Crypto is Huge in the Ukraine War,” World Economic Forum, March 16, 2023, https://www.weforum.org/agenda/2023/03/the-role-cryptocurrency-crypto-huge-in-ukraine-war-russia/.

(34) “Help Ukrainian Families Forced to Flee,” United Nations High Commissioner for Refugees, https://donate.unhcr.org/crypto/en/ukraine-emergency.

(35) Jason Nelson, “Ukraine DAO’s Flag NFT Sells For $6.75 Million,” Decrypt, March 4, 2022, https://decrypt.co/94353/ukraine-daos-flag-nft-sells-for-6-75-million.

(36) “A Year into Russia’s War on Ukraine, Cryptocurrencies Continue to Play a Key Role”

(37) “A Year into Russia’s War on Ukraine, Cryptocurrencies Continue to Play a Key Role”

(38) Elliptic Research Team, “Crypto Donations to Ukraine and Russia: Breaking Down the Numbers,” Elliptic Connect, https://hub.elliptic.co/analysis/crypto-donations-to-ukraine-and-russia-breaking-down-the-numbers/.

(39) Anna Baydakova, “Where the Coins Go: Inside Ukraine’s $135M Wartime Fundraise,” *CoinDesk,* June 11, 2022, https://www.coindesk.com/layer2/2022/06/10/where-the-coins-go-inside-ukraines-125m-wartime-fundraise/.

(40) Ananya Kumar and Nikhil Raghuveera, “Can Crypto Deliver Aid Amid War? Ukraine Holds the Answer,” *Atlantic Council: New Atlanticist*, April 4, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/can-crypto-deliver-aid-amid-war-ukraine-holds-the-answer/.

(41) Luke Winkie, “Every Bitcoin Helps: Why Ukraine is Soliciting for Cryptocurrency Donations,” *The Guardian*, March 3, 2022, https://www.theguardian.com/technology/2022/mar/03/bitcoin-donations-cryptocurrency-support-ukraine.

(42) Kimberly Ann Elliott, Gary Clyde Hufbauer, and Barbara Oegg, “Sanctions,” Library of Economics and Liberty, https://www.econlib.org/library/Enc/Sanctions.html.

(43) William Alan Reinsch and Andrea Leonard Palazzi, “Cryptocurrencies and U.S. Sanctions Evasion: Implications for Russia,” The Center for Strategic and International Studies, December 20, 2022, https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-

evasion-implications-russia#:~:text=Russia%20may%20use%20cryptocurrencies%20to,transfer%20details%20to%20IP%20addresses.

(44) "A Year into Russia's War on Ukraine, Cryptocurrencies Continue to Play a Key Role"

(45) Lila Carrée, "The Role Of Technology in the Exposition of War Crimes in Ukraine: How the Use of Cutting-Edge Technologies and Open-Sources Investigations Can Expose Human Rights Violations," London School of Economics and Political Science Human Rights Blog, February 2, 2023, https://blogs.lse.ac.uk/humanrights/2023/02/02/the-role-of-technology-in-the-exposition-of-war-crimes-in-ukraine-how-the-use-of-cutting-edge-technologies-and-open-sources-investigations-can-expose-human-rights-violations/.

(46) Deborah Yao, "Russian War Crimes in Ukraine Documented on Blockchain," AI Business, June 11, 2022, https://aibusiness.com/responsible-ai/russian-war-crimes-in-ukraine-documented-on-blockchain.

(47) "Hala Systems: Blockchain Case Study for Saving Lives and Mitigating War Crimes," *ConsenSys Media*, February 19, 2020, https://consensys.net/blockchain-use-cases/social-impact/hala-systems-case-study/.

Biotechnology and the Return of Biological Warfare

Shruti Sharma

THE DEBATE AROUND THE ORIGINS OF THE COVID-19 pandemic is a grave reminder of threats emerging from biological research and the need to address them (1). While most scientists argue that the pandemic originated from natural sources (2), speculations still exist about it being a human-made virus (3). Additionally, the Russia-Ukraine war has also sparked fears about the potential misuse of biological research to develop biological weapons during wars or conflicts (4). While the debate around the use of biological weapons during the Russia-Ukraine war has largely been dismissed as disinformation, biological warfare is a serious threat that cannot be ignored.

Defined succinctly, "Biological warfare is the deliberate use of disease-causing biological agents such as bacteria, virus, rickettsiae, and fungi, or their toxins, to kill or incapacitate humans, animals, or plants as an act of war" (5). This essay highlights the evolution of biological warfare and the role of biotechnology in the development and production of biological weapons.

History of Biological Warfare

Infectious diseases have been used to inflict pain and death during wars or conflicts since 600 BCE. Such attacks were often not targeted and usually involved either deliberate poisoning of food and water or the use of contaminated humans, animals, or plants to spread infectious diseases. For example, in 1347, the Mongol forces catapulted plague-infested bodies over

Caffa, a besieged city in Crimea, to transmit disease to their inhabitants. The survivors of the disease fled to parts of the Mediterranean Basin, thereby spreading the disease to a lot of European countries (6).

This practice changed in the latter half of the nineteenth century after the discovery of Robert Koch's "germ theory," which established that specific germs cause specific diseases (7), consequently leading to the evolution of biological warfare. The discovery, coupled with advances in microbiology and the study of microscopic organisms, opened new opportunities to identify, isolate, produce, and stockpile specific pathogens for biological attacks. While the intentional use of biological weapons to inflict harm was not common, targeted attempts using specific pathogens were observed, which led the world towards modern biological warfare.

For example, during the First World War, the German army attempted to ship horses and cattle infected with anthrax and glanders to the US and other countries (8). While such attempts did not result in successful military implications, they demonstrate the pivot towards the targeted use of infectious agents for biological attacks.

Further development in technologies led to an increased interest in other countries to pursue active biological weapons research after the First World War. For example, in 1928, the Soviet Union started using naturally occurring pathogens that had caused epidemics during the First World War to initiate their biological weapons programme (9). Similarly, Japan set up Unit 731, its dedicated biological weapons research programme, in 1930, which was later used to deliberately poison Chinese prisoners of war with infectious particles (10). Thereafter, Japan continued to develop and use biological weapons until the end of the Second World War (11).

During the Second World War, the US also developed an offensive biological warfare programme (12). Even as the US agreed to terminate their biological weapons programme in 1969, the erstwhile Soviet Union leveraged advancements in biotechnology to continue its illegal and clandestine biological weapons programme until the 1990s (13). For example, in the 1980s, the Soviet Union had successfully developed antibiotic-resistant strains of plague, anthrax, tularaemia, and glanders. Similarly, after 1985, Iraq developed and tested biological agents such as anthrax, botulinum, aflatoxin, and ricin for offensive purposes (15).

After the end of the Cold War, the US witnessed one of the worst biological attacks in history. A week after the September 2001 terrorist attacks, letters contaminated with anthrax were deliberately distributed through the postal system, leading to five fatalities and 22 anthrax infections (16).

Not only have countries pursued a biological weapons programme, but several terrorist organisations have also expressed interest in using biological weapons to inflict harm. For example, in the mid-2000s, al-Qaeda tried to seek information from a Malaysian researcher to develop anthrax biological weapons and relied on a researcher from a university in the US to lead their biological weapons programme (17).

How Biotechnology Changed the Biological Warfare Landscape

Advancements in biotechnology have enabled the scientific community worldwide to fundamentally engineer biological systems. These developments have made it faster, cheaper, and easier to read, write, and edit genetic material, which are blueprints for all living systems on Earth. Paired with advances in artificial intelligence (AI), this has led to large-scale engineering of biological systems. AI leverages machine learning algorithms to analyse large data sets to identify patterns that are not apparent to humans. This analysis can then aid drug discovery, facilitate accurate diagnosis of medical conditions, and help develop personalised medicines (18).

While generally used for the good of society, some of these tools and technologies can be used to tinker with living systems to make pathogens that are more virulent and transmissible in the human population, more resistant to medical countermeasures like vaccines, or have a wider host range. For instance, in 2014, a professor at Emory University in the US experimented with the influenza virus, SARS virus, and MERS virus to make them more transmissible in humans. While these studies were conducted to develop more effective vaccines or other medical countermeasures, concerns about misusing this study evoked a temporary pause on such research (19).

More specifically, however, developments in genome sequencing, gene editing, and synthetic biology have led to the emergence of biological warfare—from using dead bodies to contaminate food or water supplies to developing targeted biological weapons for covert use.

This section will explain how these three technologies make it easier for malicious actors to develop and produce biological weapons.

First, genome sequencing methods have enabled researchers to gather more information about the functionality of specific genes in an organism's genome. This enables them to identify genes that cause specific diseases and allows them to develop personalised treatments according to a person's genetic makeup. Even as this technology is a huge development in the study of genetic diseases, it can be manipulated by nefarious actors to identify and isolate a specific gene to cause diseases or create biological weapons that target a specific race or ethnic group. For instance, in 2017, a Chinese general who was the head of the National Defence University in Beijing emphasised in his book that gene sequencing and gene editing technologies could be used to develop biological weapons that target a specific ethnic group (20). Although a cumbersome exercise in itself, the possibility of developing targeted biological weapons is not a farfetched reality. Advances in genome sequencing can also be leveraged to access genomic sequences of dangerous pathogens. While this sequence information is essential to support disease surveillance and to develop medical countermeasures (21), the same data can be manipulated by nefarious actors to produce biological weapons. In addition, these genomic databases are also vulnerable to cyberattacks, where people with malignant intentions can either tamper with the information in the database or hack the data to compromise its integrity and accessibility (22).

Second, advancements in gene editing technologies, such as clustered regularly interspaced short palindromic repeats (CRISPR) and CRISPR-associated protein 9 (Cas 9), allow researchers to tinker with gene sequences. This ability to manipulate genes can enable nefarious actors to create new pathogenic characteristics, such as enhanced virulence, pathogenicity, survivability, infectivity, and drug resistance. For example, the controversial gain-of-function experiments to enhance the transmissibility of bird flu virus among humans highlight the dangerous risk posed by gene editing in the biological warfare landscape (23). On the one hand, such experiments are needed to understand the behaviour of viruses to ensure that measures can be adopted to prevent the next pandemic. On the other, these efforts to produce exceptionally dangerous pathogens enhances the ability of malicious forces to create deadlier biological weapons.

Third, developments in synthetic biology perhaps hold the most dangerous potential. This is because improvements in DNA synthesis have given researchers the ability to write genes, making experimentation with synthetic genes easier and more accessible. Researchers can now order DNA fragments online and artificially create or recreate a virulent organism in labs (24). For instance, researchers at the State University of New York developed a live synthetic strain of poliovirus in 2002 using publicly available genetic information (25). In another study, a team at the University of Alberta in the US recreated an infectious horsepox virus, a close relative of smallpox, which is a deadly biological weapon agent, using DNA fragments ordered online (26). While these developments are critical to advance biomedical research to develop more effective and targeted vaccines and other medical countermeasures, these advancements carry the foreboding potential to create biological weapons. This is because, without synthetic biology, actors who develop biological weapons will depend on either nature or research labs to acquire pathogens. However, with synthetic biology techniques, they can order DNA fragments online to assemble them to recreate virulent pathogenic strains or artificially develop lethal pathogens by using genomic information available online (27). In some cases, these actors can also leverage the cyber vulnerabilities of research labs to acquire sensitive information (28). Since there is little or no regulation to screen DNA synthesis orders and their customers, there is very little that one can do to prevent a malicious actor from developing biological weapons from scratch.

International Mechanisms to Address Biological Warfare

The increase in the adoption of biological weapons after the establishment of the germ theory of diseases led to two international declarations—the Brussels Declaration in 1874 and the Hague Declaration in 1899. Although the two declarations did not explicitly mention the terms biological weapons or biological warfare, both declarations laid the laws and customs of war and banned the use of poison or poisonous weapons. These two declarations, however, were not ratified by all signatories and did not reap any significant benefits (29). Due to this shortcoming, a second Hague Convention was signed in 1907 that reiterated the earlier bans on the use of poison or poisonous weapons. However, this version also lacked an implementation clause (30). These conventions resulted in providing only lip service to the goal of eliminating biological weapons from a nation's arsenal.

The Geneva Protocol, introduced in 1925, was the first diplomatic attempt to explicitly prohibit the use of biological weapons. While this protocol explicitly banned the use of biological weapons, it did not prohibit its development, production, or stockpiling (31). Moreover, countries such as France, which had an advanced biological weapons programme, reserved the right to retaliate using biological weapons in case they were attacked first. This led to a complete failure of the Geneva Protocol, which shifted the international norm from a complete ban on the use of biological weapons to a "no first use policy." The shift was then leveraged by other countries such as the UK and the Soviet Union to justify their biological weapons programme (32). In addition, the protocol only applied to conflicts between countries adhering to the agreement, meaning it posed no binding constraints on using biological weapons in internal conflicts or for use against countries that were not signatories (33).

These shortcomings were later addressed by the Biological Weapons Convention (BWC) that came into force in 1975. This legally binding treaty bans the development, stockpiling, acquisition, retention, and production of biological weapons. While not explicitly prohibiting the use of biological weapons, it reaffirms the Geneva Protocol that bans the use of biological weapons, but with certain exceptions, as discussed earlier. Further, the prohibition of the use of biological weapons was discussed in the BWC's review conference in 1996, which restated that the use of biological weapons was a violation of the BWC (34).

Even though this is a legally binding treaty, it has its own shortfalls.

First, this treaty does not ban biodefence programmes, thereby allowing countries to pursue biological research for peaceful purposes, which can be converted into offensive programmes, if needed (35). Furthermore, the

BWC only prohibits the production, development, stockpiling, or acquisition of biological agents above a certain quantity, which is not explicitly stated in the convention. Moreover, the definition does not include a list of specifically prohibited biological agents or their quantities, making it ambiguous for states to comply (36).

Second, the treaty does not have a formal verification protocol to ensure compliance, but rather relies on states self-reporting their uses and governance frameworks. Efforts to develop a verification protocol since 1991 have not been successful yet. This is primarily because it is difficult to strike a balance between the need for transparency to ensure compliance to the protocol versus secrecy of research to protect states' proprietary information (37). This is because states would have to declare their research facilities, thereby allowing access to sensitive research and placing biodefence research at risk (38).

Third, the treaty lacks a formal reporting mechanism in case of non-compliance. In case of any suspected violation, the treaty only allows member states to lodge a complaint with the United Nations Security Council (UNSC) to investigate such complaints. It, however, selectively empowers the permanent members of the UNSC to veto Security Council decisions to conduct investigations (39). This power was not invoked until recently when the Russian Federation proposed a resolution to set up a commission to investigate its complaint about non-compliance to the BWC by the US and Ukraine (40). Apart from the UNSC mechanism to address violations of the convention, the ninth review conference of the BWC, held in 2022, finally reached a consensus to develop a working group to set up a formal review and verification mechanism (41). While the exact constitution of this working group is still in process, this might be one step forward in establishing an enforcement mechanism to ensure compliance with the convention.

Fourth, the BWC is poorly funded compared to the Chemical Weapons Convention (CWC). The Implementation Support Unit of the BWC only has a staff of three to four people compared to a large group working at the CWC secretariat. Moreover, unlike the CWC, the BWC does not have a scientific body to brief the unit about the advances in biotechnology and their implications for biological warfare (42). Even though periodic science and technology review mechanisms exist under the BWC, experts have often argued for a more systematic approach to strengthen the convention (43).

To further limit the use of biological weapons in wars, Australia and other Western countries established an informal forum of countries, in 1985, called the Australia Group (AG), to harmonise export control regimes to ensure that exports do not contribute to the development of biological weapons. Given the informal nature of this grouping, its effectiveness only depends on the member countries' shared commitments to non-proliferation goals and has no legally binding obligations (44). This grouping is established to support the objectives of the BWC by strengthening the effectiveness of national export licensing measures (45).

The failure of these conventions to limit or prohibit the use of biological weapons led to UNSC Resolution 1540. Passed in 2004, this resolution is a binding instrument that strengthened international efforts to combat the development, proliferation, delivery, and illicit trafficking of biological weapons. Moreover, Resolution 1540 strengthened several points in the BWC by providing an explicit focus on non-state actors; applicability to states not parties to the BWC; more specific measures that states must take to prevent bioterrorism, including measures regarding security, physical protection, and border and export controls; and a very limited verification and enforcement mechanism (46).

However, this resolution also has its own shortcomings, further complicating the biological warfare landscape.

First, the committee set up under the UNSCR 1540 also relies on national reports to determine the degree of compliance with the resolution. Since these reports are made internally, there is always an element of bias with the tendency to mask areas of non-compliance. Second, the countries' compliance to the UNSCR 1540 depends on the availability of funds, human resources, and the degree of technological advancement in different states. The universal application of this resolution does not consider the difficulties resource-constrained nations face in implementing measures to comply with the resolution. It is, therefore, important to promote and develop personalised standards to specifically address capacity issues of states with lesser resources and capability (47).

Biological Warfare: Current Scenario and the Road Ahead

Pathogens, as they exist in their natural forms, can be manipulated using the combined power of genome sequencing, gene editing, and synthetic biology advancements. This gradually leads the world towards modern biological warfare, which would have been inconceivable without these developments. Consequently, it is imperative to establish norms and standards to prevent misuse of these technologies.

This section emphasises specific recommendations that can be adopted to regulate advances in the field of genome sequencing, gene editing, and synthetic biology to minimise the risks of biological warfare.

Fast, affordable, and efficient sequencing of pathogen genomes, along with the easy availability of these sequences online, makes it easier for researchers to develop diagnostics, vaccines, or other medical countermeasures. Open science may be necessary for researchers to work collaboratively, but it is mandatory to protect this information from nefarious actors (48). It is, therefore, important to implement cybersecurity safeguards to prevent these databases from cyberattacks at two levels. One, collaboration between researchers and representatives from the information technology department should be encouraged in all research laboratories to identify sensitive, valuable assets in an organisation and implement appropriate cybersecurity safeguards (49). Second, research publishing platforms should develop significant access controls to allow access to only legitimate researchers.

With respect to gene editing technologies, initiatives should be taken to ensure transparency in gene editing research at both national and global levels. Risk assessment should be introduced at the beginning of each gene editing experiment to evaluate potential unexpected outcomes from engineering pathogens. Furthermore, from planning, project implementation, and project execution in research labs or commercial facilities to publishing and sharing of findings and commercialisation of technology, a risk–benefit analysis should be conducted at all stages. Reducing risks incrementally in each step with adequate oversight mechanisms will allow for overall risk mitigation (50).

Specific to DNA synthesis and synthetic biology technologies, no specific safeguards exist to prevent access to DNA sequences of dangerous pathogens to malicious actors. Moreover, no country has any legal obligation to screen DNA synthesis orders (51). While members of the International Gene Synthesis Consortium, an industry group, voluntarily screen customer orders for DNAs at their own expense, the declining costs of DNA synthesis are making it financially challenging for the consortium to screen all orders (52). Therefore, DNA synthesis companies, laboratories ordering custom-made DNAs, non-profit organisations, and governments internationally need to come together to establish a more affordable mechanism that makes it mandatory for DNA suppliers to screen their sequences against known or dangerous pathogens before dispatching them (53). An appropriate authority should also be established at the national level for DNA suppliers to report any suspicious orders. Additionally, this authority should also create a mechanism to enforce stringent background checks to ensure the legitimacy of customers ordering DNA. Moreover, monetary incentives can be introduced for researchers and laboratories following DNA screening procedures to ensure better compliance with the protocol. These measures can prevent access to dangerous pathogens by nefarious actors, thereby minimising the possibility of deliberate misuse.

Conclusion

Considering the dangerous potential of biological agents, stringent oversight measures and compliance mechanisms should be established to strengthen the norm that biotechnology shall be used only to advance prosperity, health, sustainability, and science, not to cause harm, at least in technologically advanced countries.

Shruti Sharma *is a fellow with the Technology and Society Program and senior convenor for the Global Technology Summit at Carnegie India.*

Endnotes

(1) Max Kozlov, "US Congressional Hearing Produces Heat but No Light on COVID-Origins Debate," *Nature* 619, no. 7970 (2023): 444–45, https://doi.org/10.1038/d41586-023-02261-w; "An Acrimonious Debate About Covid's Origins Will Rumble On: Trials of the Zoonati," *The Economist,* June 26, 2023, https://www.economist.com/science-and-technology/2023/06/26/an-acrimonious-debate-about-covids-origins-will-rumble-on

(2) "Covid-19 Found in Raccoon Dogs in China, Strengthens Natural Origin Theory: Report," *The Times of India,* March 17, 2023, https://timesofindia.indiatimes.com/home/science/covid-19-found-in-raccoon-dogs-in-china-strengthens-natural-origin-theory-report/articleshow/98732130.cms?from=mdr

(3) "Covid-19 was a 'Man-Made' Virus, Claims Scientist Who Worked at the Wuhan Lab," *The Indian Express,* December 6, 2022, https://indianexpress.com/article/world/covid-19-man-made-virus-scientist-wuhan-lab-8308520/

(4) Riley Griffin, "US Says it Fears Russia May Use Biological Weapons in Ukraine," *Bloomberg*, November 30, 2022, https://www.bloomberg.com/news/articles/2022-11-30/us-says-it-fears-russia-may-use-biological-weapons-in-ukraine-war#xj4y7vzkg; Olga Robinson, Shayan Sardarizadeh, and Jake Horton, "Ukraine War: Fact-Checking Russia's Biological Weapons Claims," *BBC*, March 15, 2022, https://www.bbc.com/news/60711705

(5) M. Balali-Mood, M. Moshiri, and L. Etemad, "Bio Warfare and Terrorism: Toxins and Other Mid-Spectrum Agents," in *Encyclopedia of Toxicology* (3rd ed.): 503–8, https://doi.org/10.1016/B978-0-12-386454-3.00589-3

(6) Mark Wheelis, "Biological Warfare at the 1346 Siege of Caffa," *Emerging Infectious Diseases* 8, no. 9 (2002), 971–75, https://doi.org/10.3201/eid0809.010536

(7) National Research Council (US) Committee to Update Science, Medicine, and Animals, "A Theory of Germs" (Washington, DC: National Academies Press, 2004), https://www.ncbi.nlm.nih.gov/books/NBK24649/

(8) R. Roffey, A. Tegnell, and F. Elgh, "Biological Warfare in a Historical Perspective," *Clinical Microbiology and Infection* 8, no. 8 (2002): 450–54, https://doi.org/10.1046/j.1469-0691.2002.00501.x

(9) Raymond A. Zilinskas, "The Soviet Biological Weapons Program and its Legacy in Today's Russia," Center for the Study of Weapons of Mass Destruction Occasional Paper No. 11 (2016).

(10) Howard Brody et al., "United States Responses to Japanese Wartime Inhuman Experimentation After World War II: National Security and Wartime Exigency," *Cambridge Quarterly of Healthcare Ethics* 23, no. 2 (2014): 220–30, https://doi.org/10.1017/S0963180113000753

(11) G. W Christopher, "Biological Warfare. A Historical Perspective," *JAMA: the Journal of the American Medical Association* 278, no. 5 (1997): 412–17, https://doi.org/10.1001/jama.278.5.412

(12) Jonathan B. Tucker, "A Farewell to Germs: The U.S. Renunciation of Biological and

Toxin Warfare, 1969-70," *International Security* 27, no. 1 (2002): 107–48, https://doi.org/10.1162/016228802320231244

(13) Tucker, "A Farewell to Germs,"111.

(14) Jonathan B. Tucker, "Biological Weapons in the Former Soviet Union: An Interview with Dr. Kenneth Alibek," *The Nonproliferation Review* (Spring-Summer 1999): 1–10, https://doi.org/10.1080/10736709908436760

(15) Nuclear Threat Initiative, "Fact Sheet: Iraq Biological Overview," https://www.nti.org/analysis/articles/iraq-biological/

(16) James M. Hughes and Julie Louise Gerberding, "Anthrax Bioterrorism: Lessons Learned and Future Directions," *Emerging Infectious Diseases* 8, no. 10 (2002): 1013–14, https://doi.org/10.3201/eid0810.020466

(17) V. Arianti, "Biological Terrorism in Indonesia," *The Diplomat*, November 20, 2019, https://thediplomat.com/2019/11/biological-terrorism-in-indonesia/

(18) Yashica Chopra, "The Power of AI in Biotechnology: Revolutionizing Innovation," May 19, 2023, https://www.datatobiz.com/blog/ai-in-biotechnology/

(19) Jocelyn Kaiser, "Moratorium on Risky Virology Studies Leaves Work at 14 Institutions in Limbo," *Science,* November 17, 2014, https://www.science.org/content/article/moratorium-risky-virology-studies-leaves-work-14-institutions-limbo

(20) Jim Geraghty, "The Coming Threat of a Genetically Engineered 'Ethnic Bioweapon'," *National Review,* April 10, 2023, https://www.nationalreview.com/corner/the-coming-threat-of-a-genetically-engineered-ethnic-bioweapon/

(21) Jennifer L. Gardy and Nicholas J. Loman, "Towards a Genomics-Informed, Real-Time, Global Pathogen Surveillance System," *Nature Reviews Genetics* 19, no. 1 (2018): 9–20, https://doi.org/10.1038/nrg.2017.88

(22) Boris A. Vinatzer et al., "Cyberbiosecurity Challenges of Pathogen Genome Databases," *Frontiers in Bioengineering and Biotechnology* 7: 106, https://doi.org/10.3389/fbioe.2019.00106

(23) Jocelyn Kaiser, "EXCLUSIVE: Controversial Experiments that Could Make Bird Flu More Risky Poised to Resume," *Science,* February 8, 2019, https://www.science.org/content/article/exclusive-controversial-experiments-make-bird-flu-more-risky-poised-resume

(24) Ronit Langer and Shruti Sharma, "The Blessing and Curse of Biotechnology: A Primer on Biosafety and Biosecurity," *Carnegie Endowment for International Peace,* November 20, 2020, https://carnegieendowment.org/2020/11/20/blessing-and-curse-of-biotechnology-primer-on-biosafety-and-biosecurity-pub-83252

(25) Andrew Pollack, "Traces of Terror: The Science; Scientists Create a Live Polio Virus," *New York Times*, July 12, 2002, https://www.nytimes.com/2002/07/12/us/traces-of-terror-the-science-scientists-create-a-live-polio-virus.html

(26) Diane DiEuliis, Kavita Berger, and Gigi Gronvall, "Biosecurity Implications for the Synthesis of Horsepox, an Orthopoxvirus," *Health Security* 15, no. 6 (2017): 629–37, https://doi.org/10.1089/hs.2017.0081

(27) Stefan A. Hoffmann et al., "Safety by Design: Biosafety and Biosecurity in the Age of Synthetic Genomics," *iScience* 26, no. 3 (2023): 106165, https://doi.org/10.1016/j.isci.2023.106165

(28) Hoffmann et al., "Safety by Design," 7

(29) International Committee of the Red Cross, "Project of an International Declaration concerning the Laws and Customs of War. Brussels, 27 August 1874," https://ihl-databases.icrc.org/en/ihl-treaties/brussels-decl-1874

(30) International Committee of the Red Cross, "Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations Concerning the Laws and Customs of War on Land. The Hague, 18 October 1907," https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907?activeTab=undefined

(31) P. R. Chari and Arpit Rajain, eds., *Preface to Biological Weapons: Issues and Threats* (Delhi: India Research Press, 2003), iii–viii.

(32) Jeanne Guillemin, "Scientists and the History of Biological Weapons. A Brief Historical Overview of the Development of Biological Weapons in the Twentieth Century," *EMBO Reports* 7, no. S1 (2006): S45–S49, https://doi.org/10.1038/sj.embor.7400689

(33) W. Seth Carus, *A Short History of Biological Warfare: From Pre-History to the 21st century* (Washington D.C: National Defense University Press, 2017)

(34) "Biological Weapons Convention," Nuclear Threat Initiative, https://www.nti.org/education-center/treaties-and-regimes/convention-prohibition-development-production-and-stockpiling-bacteriological-biological-and-toxin-weapons-btwc/

(35) Eric Merriam, "The International Legal Regime Affecting Bioterrorism Prevention," *National Security Law Journal* 3, no. 1 (2014), https://ssrn.com/abstract=2478444; Thomas Douglas, "The Dual-Use Problem, Scientific Isolationism and the Division of Moral Labour," *Monash Bioethics Review* 32, no. 1–2 (2014): 86–105, https://pubmed.ncbi.nlm.nih.gov/25434066/

(36) Eric Merriam, "The International Legal Regime Affecting Bioterrorism Prevention," *National Security Law* Journal 3, no. 1 (2014), https://ssrn.com/abstract=2478444

(37) Chari and Rajain, eds., *Preface to Biological Weapons: Issues and Threats*

(38) Olivia Bauer, "The Toothless Convention: The Lack of Political Will to Update the Biological Weapons Convention," *Paideia* 2, no. 1 (2015), https://doi.org/10.15368/paideia.2015v2n1.6

(39) "The Biological Weapons Convention at a Glance," Arms Control Association, https://www.armscontrol.org/factsheets/bwc

(40) "Security Council Rejects Text to Investigate Complaint Concerning Non-Compliance of Biological Weapons Convention by Ukraine, United States," United Nations Security Council 9180th Meeting (SC/15095, November 2, 2022), https://press.un.org/en/2022/15095.doc.htm

(41) Biological Weapons Convention, "Working Group on the Strengthening of the Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction," Biological Weapons Convention, BWC/WG/1/WP.1, March 2023,

(42) Shambhavi Naik, "Gene Editing and the Need to Reevaluate Bioweapons," in *Future Warfare and Technology: Issues and Strategies*, ed. Rajeswari Pillai Rajagopalan (ORF and Global Policy Journal, 2022), 117–23, https://www.orfonline.org/wp-content/uploads/2022/11/GP-ORF-Future-Warfare-and-Technology-01.pdf

(43) James Revill, Alisha Anand, and Giacomo Persi Paoli, "Exploring Science and Technology Review Mechanisms Under the Biological Weapons Convention," UNIDIR, June 15, 2021, https://doi.org/10.37559/SECTEC/2021/SandTreviews/01

(44) The Australia Group, "Introduction," Department of Foreign Affairs and Trade, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/introduction.html

(45) The Australia Group, "Relationship with the Biological Weapons Convention," Department of Foreign Affairs and Trade, https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/bwc.html

(46) Braden Leach, "Necessary Measures: Synthetic Biology & the Biological Weapons Convention," *Stanford Technology Law Review* 25, no. 1 (2021): 141–66, https://law.stanford.edu/wp-content/uploads/2021/12/FINAL-ROUND_Leach-1.pdf

(47) Huma Rehman and Afsah Qazi, "Significance of UNSCR 1540 and Emerging Challenges to its Effectiveness," *Strategic Studies* 39, no. 2 (2019): 48–66, https://www.jstor.org/stable/48544299

(48) James Andrew Smith and Jonas B. Sandbrink, "Biosecurity in an Age of Open Science," *PLoS Biology* 20, no. 4 (2022): e3001600, https://doi.org/10.1371/journal.pbio.3001600

(49) Shruti Sharma, "Cyber-Biosecurity: How Can India's Biomedical Institutions Develop Cyber Hygiene?" Carnegie Endowment for International Peace India, July 12, 2023, https://carnegieindia.org/2023/07/12/cyber-biosecurity-how-can-india-s-biomedical-institutions-develop-cyber-hygiene-pub-90157

(50) Shruti Sharma, "Safeguarding Biotechnology Innovation and Boosting the Bioeconomy: The Road to G20," in *Global Technology Summit 2022 Action Points*, Carnegie Endowment for International Peace India, March 7, 2023, https://carnegieindia.org/2023/03/07/global-technology-summit-2022-action-points-pub-89171#Sharma

(51) Jamie M. Yasif et al., "Preventing the Misuse of DNA Synthesis Technology," Nuclear Threat Initiative, https://www.nti.org/about/programs-projects/project/preventing-the-misuse-of-dna-synthesis-technology/; Kelsey Piper, "The Next Deadly Pathogen Could Come from a Rogue Scientist. Here's How We Can Prevent That," *Vox*, February 11, 2020, https://www.vox.com/future-perfect/2020/2/11/21076585/dna-synthesis-assembly-viruses-biosecurity

(52) Kevin M. Esvelt, "Credible Pandemic Virus Identification Will Trigger the Immediate Proliferation of Agents as Lethal as Nuclear Devices," Senate Homeland Security and Governmental Affairs Committee: Subcommittee on Emerging Threats and Spending Oversight, https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Esvelt%20Testimony.pdf; Diane DiEuliis, Sarah R. Carter, and Gigi Kwik Gronvall, "Options for Synthetic DNA Order Screening, Revisited," *mSphere* 2, no. 4 (2017), https://doi.org/10.1128/mSphere.00319-17

(53) For more details on known or dangerous pathogens, see the pathogens listed under the U.S. regulated pathogens (select agents), Australia Group list agents, U.S. Commerce Control List (CCL) controlled sequences, and European Union (EU) sequences. DiEuliis, Carter, and Gronvall, "Options for Synthetic DNA Order Screening, Revisited".

Assessing the Military Applications of Generative AI

Amoha Basrur

GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI) has been one of the most prominent developments of the current AI boom. Popular platforms such as ChatGPT, DALL-E, and Midjourney mainstreamed the use of GenAI for commercial and creative purposes (1), but the technology holds immense potential beyond these realms. GenAI is a powerful tool for enhancing capabilities, augmenting datasets, and improving human-machine communication, all valuable features for innovation. AI has the potential to revolutionise the way nations prepare for, conduct, and respond to armed conflicts, but it also presents complex ethical, strategic, and security challenges that require careful consideration. This essay explores the military uses of GenAI, the potential risks involved in its adoption, and technological deficiencies that need to be addressed.

Understanding Generative AI

Machine learning can be viewed as having two approaches: discriminative and generative (2). GenAI is created by generative modelling, a branch of machine learning that involves training a model to produce new data that is similar to a given data set (3). These models can produce data in various forms, such as text, audio, imagery, or software code, that are hard to distinguish from samples created by humans. It is trained to learn the underlying statistical properties of large data sets and then recreates these patterns to create outputs that closely resemble the training data.

Until recently, developments in discriminative modelling led the wave of progress in machine learning (4). These AI models are designed for specific tasks like classification and prediction. GenAI, on the other hand, produces new content by mimicking probabilities. Traditionally, discriminative models were both easier to create and more readily applicable to problems faced across industries. Rapid progress in generative modelling, however, has increased the possibilities for AI applications and is considered a significant step on the way to creating artificial general intelligence (5).

A key component in selecting the right GenAI model is its architecture—the basic structure or design, including how its layers or neural networks and components are organised (6). GenAI can be classified based on this architecture:

1. Variational autoencoders (VAEs) are probabilistic generative models. They consist of an encoder and a decoder network. The encoder maps the input data into a latent space (7) as a probability distribution. The decoder then generates data samples from the latent representations. VAEs use variational inference to learn the underlying distribution of the data in the latent space.

2. Generative adversarial networks (GANs) consist of two neural networks, a generator, and a discriminator, all trained simultaneously against each other. The generator creates data samples, such as images, from random noise. The discriminator distinguishes between data from the training set and data from the generator. The generator improves the quality of data it produces by trying to fool the discriminator, while the discriminator gets better at discerning real data from fake data. This competition leads to the generation of increasingly convincing data samples.

3. Normalising Flow Models transform simple probability distributions into more complex ones through invertible transformations. They can then map these transformations backwards to efficiently compute probabilities.

4. Diffusion models are based on the concept of data diffusion, where a dataset is transformed from a simple to complex distribution. The model optimises itself iteratively to reduce discrepancies between the training and generated data, and to make the generation process reversible.

5. Transformer models excel at capturing long-range dependencies in sequences. Unlike traditional recurrent networks, transformers process

all input elements simultaneously rather than sequentially. This parallel processing results in faster training and inference compared to recurrent models.

These models can also be combined to create hybrid models.

Military Applications of GenAI

Defence agencies worldwide began using AI long before their commercial popularity for purposes such as target recognition, drone swarms, data processing, and transportation. Recognising the power of this emergent modelling system, militaries around the world have begun research to explore their own uses of GenAI. A wide range of companies, such as Palantir Technologies Inc., Anduril Industries Inc., and Microsoft, are either developing AI-based decision platforms for the Pentagon or are already working with the US Defence Department to provide AI solutions. US Air Force Colonel Matthew Strohmeyer stated that “the long-term aim of such exercises is to update the US warhorse to use AI-enabled data in decision-making, sensors, and, ultimately, firepower.” (8) In October 2022, the UK announced plans to invest £900 million to build its own ‘BritGPT’ amid fears of lagging behind Big Tech and China (9). The government outlined plans to develop an exascale computer that can carry out more than one billion simple calculations a second. Such a supercomputer would have numerous scientific and military applications. This section investigates the current experiments with GenAI in the military and conducts prospective analysis for further applications.

Wargaming and Simulations

GenAI has huge potential in enhancing wargaming and other training simulations. It can enhance realism, adaptability, and complexity in simulations, including creating multidimensional and multipolar scenarios (10). In the US, the Marine Corps University (MCU) is experimenting with large language models that they believe will completely transform military wargaming (11). The MCU uses an application called *Command: Professional Edition* that can rapidly customise its open-source database of platforms, sensors, weapons, and ground formations for each user (12). Subject matter experts hope that, at some point in the future, wargaming simulations have an interface between the AI and software so that a trainer can simply input their desired scenario using natural language and the programme will create a customised simulation (13).

Autonomous Agents and Assistants

One of the greatest utilities of GenAI is its facilitation of human-machine communication. Researchers around the world have been developing technology for people to interact with the systems they use as well as complex autonomous agents such as robots. In 2019, Russia launched the MiG-35 fighter jet that had an integrated AI pilot assistant called Rita that makes recommendations to the pilot in critical flight situations and during combat (14). This technology has the potential to make twin-pilot crafts redundant, thereby greatly increasing efficiency.

The US Army Combat Capabilities Development Command is developing the Joint Understanding and Dialogue Interface, a prototype that enables bi-directional conversation between soldiers and autonomous systems (15). The interface is equipped to recognise intent in spoken dialogue and act to realise the underlying intention along with the instructions. This technology can be integrated into combat vehicles and autonomous systems to allow advanced real-time conversations in soldier-agent teams. Soldiers will not require any additional training to interact with these systems because of their ability to process natural and noisy speech. The classifier, however, requires additional linguistic representation to be more widely adaptable. The system can also be improved by integrated interaction modalities like gaze and gestures.

Adaptive Decision-Making

The US Air Force has been experimenting using large language models (LLMs) for military tasks (16). AI-based decision platforms are able to sort through information that would typically take human hours in just a few minutes. A team's experiments involved asking the test LLMs to plan a military action in response to an escalating global crisis in the Indo-Pacific region; for instance, Bloomberg News fed 60,000 pages of data, including US and Chinese military documents, to Donavon, an LLM platform by Scale AI that is part of the Air Force trials. The model was able to ingest the documents and answer questions about a US-Taiwan-China conflict within seconds (17). The information digestion efficiency of these models can be leveraged to enhance decision-making in a range of dynamic conflict scenarios.

Data Augmentation

GenAI, especially GANs, can be used to augment datasets for training AI models, especially for object recognition-related tasks. Complex object characteristics and backgrounds make detection challenging, especially for remote sensing images or video (18). Detection models require millions of parameters and, therefore, massive quantities of data to train to generalise accurately. Collecting and labelling images is time-consuming, expensive, and requires domain knowledge (19). GANs are a cost-effective and energy-saving (20) way of generating synthetic training data and improving the quality of existing data through reconstruction, super-resolution, enhanced realism, and image-to-image translation (21).

Information Warfare

GenAI is a double-edged sword for information warfare (22). AI tools can be used to fake information and influence perceptions. AI generated pictures and videos, such as deepfakes, grant false authenticity to misinformation. Deepfakes are hyper-realistic videos that replicate the likeness of a person. Soon after the start of the Russia-Ukraine war in 2022, a deepfake was circulated of Ukrainian President Volodymyr Zelenskyy telling his soldiers to surrender to Russia (23). Although this specific instance was quickly debunked, as the quality of such videos improve, they will become harder to detect. Additionally, automated content creation and bots can rapidly produce and amplify large volumes of fake media. Bots can flood social media feeds and create the illusion of widespread support for a particular narrative. For instance, a pro-China operation was documented using AI-generated videos of fictitious people lauding China's role in geopolitics while undercutting the US (24). Generative AI's affordability and accessibility have lowered the barrier to entry for disinformation campaigns. The Venezuelan state media used AI-generated videos of news anchors from a non-existent channel to spread pro-government messages (25). In the US, AI-manipulated videos and images of political leaders have been circulated on social media, especially in relation to the upcoming 2024 election (26). A combination of human and bot campaigns have been used to manipulate online discussions, with at least 47 governments deploying commentators to spread propaganda in 2023 (27) . Although there is limited information in the public domain about militaries using GenAI for information warfare, the plethora of examples of governments and politicians doing so leaves no doubt that militaries worldwide are far ahead of this curve. Ease of generation also creates the potential for social engineering and personalised propaganda that is more effective in resonating with target audiences (28). The flip side of this technological development is that AI will also play an important role in detecting and countering such content. An example is Data Robot, a military tool created to trawl social media websites and spot misleading content to provide an overlay of accurate information to commanders and ensure sound decision-making (29).

The Future of Warfare

GenAI lies at the intersection of machine learning and natural language processing. It is a powerful technology because of its increasing ability to analyse unstructured data and produce novel outputs. It will initially work to enhance human capacities but also has broad applications in areas where it can surpass human cognitive capacities, such as data analysis (30). GenAI's integration in military operations has significant implications for intelligence, deterrence, and the security dilemma.

GenAI systems have the potential to revolutionise military intelligence gathering and analysis. Information overload and attention fragmentation have been persistent problems in military decision-making (31), not only in the context of conflict situations, but during peace-time activities like logistics, training, and administration. While it is tempting to include data from the widest number of sources, military leaders are limited by the human capacity to synthesise information (32). GenAI can overcome these limitations by integrating and processing vast amounts of data quickly, allowing for more sophisticated pattern identification and predictive analysis that can enhance decision-making. A wider range of data sources and advanced pattern recognition would also boost intelligence operations.

However, the dual-use potential of this technology means that while it would open doors to greater sources of intelligence, it also makes it easier to lie persuasively (33). Fake news is increasingly becoming a tool of irregular warfare (34). GenAI's use in information warfare introduces a new dimension to perception management. GenAI can be used not only to identify and combat misinformation but also as a tool for psychological deterrence to influence adversaries' perception of the costs and risks of conflict. Nations will use these tools to manipulate perceptions, challenging traditional deterrence methods. This means that GenAI can produce targeted cyber intelligence to be consumed for defence or offence purposes, i.e., to enhance or compromise networks, information, and users' security (35).

Any use of AI in offence has the potential to lead to inadvertent escalation. High-speed decision-making without human oversight risks leading to misguided actions or unintended ambiguity that could increase the propensity for conflicts.

Autonomous agents and assistants can greatly improve operational efficiency, especially if human-machine teaming is expanded through emerging technologies like brain computer interface (36). This would be accompanied by novel ethical, legal, and cyber risks but would provide significant efficiency boosts in communication, situational awareness, autonomous system management, human cognition, and training techniques that could potentially reduce casualty rates with improved medical outcomes (37).

The rapid advancement of GenAI technologies poses significant risks in the realm of biosecurity. The convergence of AI with life sciences and bioengineering raises concerns about the misuse of AI technologies to create harmful biological agents (38). Furthermore, experts have warned that within a few years, AI systems could potentially create bioweapons themselves (39). Currently, AI systems can aid in some steps of producing biological agents, though not completely or reliably. However, as AI systems continue to evolve, there is a substantial risk that they will be able to complete all necessary steps for bioweapon production independently. This development could broaden the range of actors capable of conducting large-scale biological attacks, especially if appropriate safeguards are not established.

The power and dual-use nature of AI technologies call for careful consideration, rigorous ethical standards, and robust regulatory frameworks to mitigate these risks.

Risks and Considerations

Causal Analysis: The most important thing to bear in mind while deploying AI systems is that while they are extremely powerful in processing and analysing large datasets, they do not inherently generate meaning or provide causal analysis (40). AI relies on data-driven analytics and pattern recognition rather than an understanding of underlying meanings. AI and machine learning, particularly when augmented with human intelligence capabilities, have shown significant promise in managing and interpreting complex data sets. However, it is in keeping a human in the loop that operations can minimise risks and ensure coherence in decision-making.

Training Data Considerations: Generative models can train using unsupervised or weakly supervised learning methods, which offer distinct advantages over discriminative models that depend on fully labelled data and supervised learning techniques. This flexibility in training means that models require less manual data preparation and can find previously unknown patterns in data, which is impossible with supervised machine learning models (41). However, unlike commercial models that use data scraped from the internet, the sensitivity of certain applications, such as those in military or critical infrastructures, requires careful consideration. It is crucial to ensure that the training data is free from any form of manipulation or poisoning, which could lead to flawed or biased outcomes. This raises a critical question for military applications of whether these models should be trained on specially vetted data instead of general internet-sourced data. The challenge would then lie in the availability of sufficient, relevant, and high-quality data points that are necessary to build a robust and functional model.

Evaluation Metrics: A significant concern with GenAI is the lack of effective evaluation metrics (42). Current methods of assessing these AI systems may not adequately capture their capabilities or pitfalls, particularly in complex and nuanced environments. This limitation underscores the need for developing more sophisticated metrics that can effectively evaluate the performance and reliability of generative AI models. There is also the issue of being able to identify AI-generated content. It is vital to possess effective detection mechanisms to ensure content integrity and prevent misuse (43).

Explainability: The inability of AI systems to explain the reasoning behind their decision-making to human operators is a significant challenge in the field of machine learning, particularly with deep learning models like deep neural networks (DNN) (44). For example, a DNN used in controlling a self-driving car might require hundreds of thousands of parameters (45), but this complexity is amplified in LLMs like ChatGPT-3, which operates with approximately 175 billion parameters (46). Such intricate structures make it difficult to interpret outputs of the invisible processes of AI systems, leading to a lack of transparency, risking biased decision-making and limited capability to identify and troubleshoot structural issues within the model.

Hallucination: Hallucination is when AI perceives incorrect patterns and generates false or misleading information. This is a significant challenge to the reliability of models, especially for high-stakes decision-making. To mitigate this, data selection for training these models must be meticulous, and the model's objectives must extend beyond mere imitation of the dataset (47). This approach is crucial to improve the accuracy and truthfulness of the generated content, especially to prevent the amplification of biases and the relay of incorrect information.

Deployment Risks: In practical applications, especially in sensitive areas such as military or critical infrastructure, the risks associated with AI systems include accidents due to malfunctions, inadvertent escalation, and unintentional conflict (48). Malfunctions can result from software bugs, hardware failures, or unforeseen interactions with the environment that can impair models. Inadvertent escalation takes place when situations are intensified by operators or leaders using AI systems inappropriately. Unintentional conflict occurs when uncertainties in algorithm behaviour hinder effective communication or produce unintended adversary signalling, which increases the likelihood of conflict even when it is not the intention of the involved states. Addressing these challenges requires a comprehensive approach that encompasses not just technological solutions but also ethical considerations, training of personnel, and international cooperation.

Cybersecurity: The sensitive nature of military data amplifies the potential consequences of security breaches for AI systems tailored for military applications. A notable risk associated with GenAI in the military is the potential for cyberattacks that have evolved to become more sophisticated, making them harder to detect and mitigate. The rapid advancement of GenAI technologies can lead to more complex attack vectors. These include evasion strategies where attackers use GenAI to create malicious inputs that bypass detection systems, or adaptation and automation where threat actors use AI to generate personalised phishing messages or automate the creation of malware variants (49). Additionally, GenAI can be used for polymorphism (50), allowing malware to self-mutate and evade traditional signature-based antivirus detection. To prevent such eventualities, additional security layers are needed for models trained on sensitive or classified data.

Conclusion

The evolution of AI can be imagined in three waves (51). The first wave involved rule-based systems, where sets of predefined rules and logic drove AI. The second wave focuses on statistical learning, involving machine learning models that use large amounts of data to learn and make decisions but lack contextual understanding and adaptability. The third wave aims to create systems that can understand and adapt to changing environments, offering more contextual and explanatory capabilities. We are currently in the second wave of AI where systems still require a high degree of human supervision and intervention to ensure that AI actions are aligned with human intentions. The main advantages at this stage will arise in AI-assisted administration, logistics, and training. We are not yet in a place where AI can—or even should—be trusted with autonomous decision-making. As we move towards a third wave, which could possibly involve underlying models for reasoning and improved uncertainty handling, the advantages and risks of GenAI will increase, making it vital that ethical considerations and safety measures keep pace with technological advancements to minimise the unintended consequences stemming from misalignment.

Amoha Basrur *is a Research Assistant at ORF's Centre for Security, Strategy and Technology.*

Endnotes

(1) Michael Chui et al., "The State of AI in 2023: Generative AI's Breakout Year," McKinsey & Company, August 1, 2023, .https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year#widespread

(2) Tony Jebara, *Machine Learning: Discriminative and Generative* (Dordrecht: Kluwer Academic Publishers, 2004). *Generative Deep Learning: Teaching Machines to Paint, Write, Compose, and Play* (Sebastopol: O'Reilly Media Inc., 2023).

(4) Foster, *Generative Deep Learning: Teaching Machines to Paint, Write, Compose, and Play*

(5) Chaoning Zhang et al., "One Small Step for Generative AI, One Giant Leap for AGI: A Complete Survey on ChatGPT in AIGC Era," arXiv, April 4, 2023, https://arxiv.org/abs/2304.06488

(6) Ajay Bandi et al., "The Power of Generative AI: A Review of Requirements, Models, Input–Output Formats, Evaluation Metrics, and Challenges," *Future Internet,* July 31, 2023, https://www.mdpi.com/1999-5903/15/8/260

(7) Latent space is an abstract multidimensional store of compressed representations of input data. This space captures the underlying structures of the data.

(8) Katrina Manson, "The US Military is Taking Generative AI Out for a Spin," *Bloomberg*, July 5, 2023, https://www.bloomberg.com/news/newsletters/2023-07-05/the-us-military-is-taking-generative-ai-out-for-a-spin

(9) Dan Milmo and Alex Hern, "UK to Invest £900m in Supercomputer in Bid to Build Own 'BritGPT'," *The Guardian*, March 15, 2023, https://www.theguardian.com/technology/2023/mar/15/uk-to-invest-900m-in-supercomputer-in-bid-to-build-own-britgpt

(10) Paul Davis and Paul Bracken, "Artificial Intelligence for Wargaming and Modeling," *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* (2022), https://www.rand.org/content/dam/rand/pubs/external_publications/EP60000/EP68860/RAND_EP68860.pdf

(11) Brandi Vincent, "How Marine Corps University is Experimenting with Generative AI in Simulations and Wargaming," *DefenseScoop*, June 28, 2023, https://defensescoop.com/2023/06/28/how-marine-corps-university-is-experimenting-with-generative-ai-in-simulations-and-wargaming/

(12) MCWL Wargaming Division, "Wargaming with Command Professional Edition," *Marine Corps Gazette,* February 2021, https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://mca-marines.org/wp-content/uploads/18-Wargaming-with-Command-Professional-Edition.pdf&ved=2ahUKEwiYt6Ka3cqAAxXaMHAKHauaCwMQ5YIJKAB6BAg3EAA&usg=AOvVaw3l3G QX3Gf_YIwzvU44G88K.

(13) Vincent, "How Marine Corps University is Experimenting with Generative AI in Simulations and Wargaming"

(14) "Russia's Newest Fighter the MiG-35 Integrates Basic AI as Pilot Assistant," *Military Watch*, June 10, 2020, https://militarywatchmagazine.com/article/russia-s-latest-fighter-mig-35-integrates-basic-ai-as-pilot-assistant

(15) "Army Researchers Create Pioneering Approach to Real-Time Conversational AI," U.S. Army, April 19, 2021, https://www.army.mil/article/245363/army_researchers_create_pioneering_approach_to_real_time_conversational_ai

(16) Manson, "The US Military is Taking Generative AI Out for a Spin" *Remote Sensing*, 2022, https://www.mdpi.com/2072-4292/14/10/2385

(19) Liqin Liu et al., "Physics-Informed Hyperspectral Remote Sensing Image Synthesis with Deep Conditional Generative Adversarial Networks," Tr*ansactions on Geoscience and Remote Sensing* 60 (2022), https://ieeexplore.ieee.org/abstract/document/9770778

(20) Fan-jie Meng et al., "Visual-Simulation Region Proposal and Generative Adversarial Network Based Ground Military Target Recognition," *Defence Technology* 18 (2022), https://www.sciencedirect.com/science/article/pii/ S2214914721001239#bib2.

(21) Peter Svenmarck et al., "Possibilities and Challenges for Artificial Intelligence in Military Applications" (paper presented at NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting, Bordeaux, France, May 2018), https://www.researchgate.net/publication/326774966_Possibilities_and_Challenges_for_Artificial_Intelligence_in_Military_Applications.

(22) Wesley Moy and Kacper Gradon, "Artificial Intelligence in Hybrid and Information Warfare: A Double-Edged Sword," in *Artificial Intelligence and International Conflict in Cyberspace*, ed. Fabio Cristiano et al. (London: Routledge, 2023).

(23) Bobby Allyn, "Deepfake Video of Zelenskyy Could be 'Tip of the Iceberg' in Info War, Experts Warn," *NPR*, March 16, 2022, https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia

(24) Adam Satariano and Paul Mozur, "The People Onscreen Are Fake. The Disinformation is Real," *New York Times,* February 7, 2023, https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html.

(25) "Venezuelan Government Spreads Propaganda with AI-Generated Avatars," *LatAm Journalism Review,* February 20, 2023, https://latamjournalismreview.org/news/venezuelan-government-promotes-propaganda-with-artificial-intelligence-generated-avatars/

(26) Alexandra Ulmer and Anna Tong, "Deepfaking It: America's 2024 Election Collides with AI Boom," *Reuters,* May 31, 2023, https://www.reuters.com/world/us/deepfaking-it-americas-2024-election-collides-with-ai-boom-2023-05-30/

(27) Allie Funk, Adrian Shahbaz, and Kian Vesteinsson, "The Repressive Power of Artificial Intelligence," Freedom House, 2023, https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence.

(28) David Wright, "AI and Information Warfare in 2025," IEEE, 2019, https://ieeexplore.ieee.org/document/9060412

(29) Colin Demarest and Jaime Moore-Carrillo, "US Military Targets Deepfakes, Misinformation with AI-Powered Tool," C4ISRNET, August 1, 2023, https://www.

c4isrnet.com/information-warfare/2023/08/01/us-military-targets-deepfakes-misinformation-with-ai-powered-tool/

(30) Atul Pant, "Future Warfare and Artificial Intelligence: The Visible Path," Institute for Defence Studies and Analyses, August 2018, https://idsa.in/system/files/opaper/op-49-future-warfare-and-artificial-intelligence.pdf

(31) Dhruv Katoch, "Future Conflict, Information Overload and the Rise of Generation C," Centre for Land Warfare Studies, 2011, https://archive.claws.in/images/journals_doc/1395650340Dhruv%20C%20Katoch%20%20CJ%20Summer%202011.pdf

(32) Katoch, "Future Conflict, Information Overload and the Rise of Generation C"

(33) Greg Allen and Taniel Chan, "Artificial Intelligence and National Security," Belfer Center for Science and International Affairs, 2017, https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

(34) Peter Singer, Emerson Brooking, *Likewar: The Weaponization of Social Media* (Boston: Houghton Mifflin Harcourt, 2018).

(35) Matteo Bonfanti, "Artificial Intelligence and the Offense–Defense Balance in Cyber Security," in *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, ed. Myriam Dunn Cavelty and Andreas Wenger (London: Routledge, 2022), https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003110224-6/artificial-intelligence-offense%E2%80%93defense-balance-cyber-security-matteo-bonfanti

(36) Anika Binnendijk, Timothy Marler, and Elizabeth Bartels, "Brain-Computer Interfaces: U.S. Military Applications and Implications," RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RR2996.html

(37) Patrick Cutter, "The Shape of Things to Come: The Military Benefits of the Brain-Computer Interface in 2040," Defense Technical Information Center, April 2015, https://apps.dtic.mil/sti/citations/AD1012768

(38) Sarah Carter et al., "The Convergence of Artificial Intelligence and the Life Sciences: Safeguarding Technology, Rethinking Governance, and Preventing Catastrophe," Nuclear Threat Initiative, 2023, https://www.nti.org/analysis/articles/the-convergence-of-artificial-intelligence-and-the-life-sciences/

(39) Katyanna Quach, "AI Drug Algorithms Can be Flipped to Invent Bioweapons," *The Register*, March 18, 2022, https://theregister.com/2022/03/18/ai_weapons_learning/

(40) Daniel Araya and Meg King, "The Impact of Artificial Intelligence on Military Defence and Security," Centre for International Governance Innovation, March 2022, https://www.cigionline.org/static/documents/no.263.pdf

(41) Nuria Caballé et al., "Machine Learning Applied to Diagnosis of Human Diseases: A Systematic Review," *Applied Sciences* (2022), https://www.researchgate.net/publication/343235054_Machine_Learning_Applied_to_Diagnosis_of_Human_Diseases_A_Systematic_Review

(42) Jon Harper, "Pentagon Testing Generative AI in 'Global Information Dominance' Experiments," *DefenseScoop*, July 14, 2023, https://defensescoop.com/2023/07/14/pentagon-testing-generative-ai-in-global-information-dominance-experiments/

(43) Lamiaa Basyoni and Junaid Qadir, “AI Generated Content in the Metaverse: Risks and Mitigation Strategies,” International Symposium on Networks, Computers and Communications, 2023, https://ieeexplore.ieee.org/abstract/document/10323860.

(44) Svenmarck et al., “Possibilities and Challenges for Artificial Intelligence in Military Applications”

(45) Mariusz Bojarski et al., “End to End Learning for Self-Driving Cars,” arXiv, April 25, 2016, https://arxiv.org/abs/1604.07316

(46) Tom Brown et al., “Language Models are Few-Shot Learners,” arXiv, July 22, 2020, https://arxiv.org/abs/2005.14165

(47) Stephanie Lin, Jacob Hilton, and Owain Evans, “TruthfulQA: Measuring How Models Mimic Human Falsehoods,” arXiv, May 8, 2022, https://arxiv.org/abs/2109.07958

(48) Michael Horowitz and Lauren Kahn, “Leading in Artificial Intelligence through Confidence Building Measures,” *The Washington Quarterly* 44, no. 4 (2021), https://doi.org/10.1080/0163660x.2021.2018794

(49) Subash Neupane et al., “Impacts and Risk of Generative AI Technology on Cyber Defense,” arXiv, June 22, 2023, https://ar5iv.labs.arxiv.org/html/2306.13033

(50) Syed Ali and Frank Ford, “Generative AI and Cybersecurity: Strengthening Both Defenses and Threats,” Bain & Company, Septermber 18, 2023, https://www.bain.com/insights/generative-ai-and-cybersecurity-strengthening-both-defenses- and-threats-tech-report-2023/

(51) John Launchbury, “A DARPA Perspective on Artificial Intelligence,” YouTube video, February 16, 2017, https://www.youtube.com/watch?v=-O01G3tSYpU

Space and Counterspace Technologies in Future Warfare

Victoria Samson

WHILE THE ROLE OF SPACE AND COUNTERSPACE TECHNOLOGIES in future warfare will only grow with time, it is important to clarify what the phrases currently mean. Space technologies have long been important parts of the warfighting network. Satellites have been used for decades to collect intelligence, share military communications, and target weapons. Even counterspace technologies are not new. As long as humanity has been going into space, efforts have been undertaken to disrupt space capabilities.

What is new is the proliferation of counterspace capabilities beyond the Cold War superpowers, as well as the increased importance space plays for many countries. This means that not only the incentive to interrupt countries' ability to utilise space has grown, but also the tools for responding accordingly.

Counterspace Capabilities

"Counterspace" is preferred over "space" because the issue is not just that the technology is space-related but that there is an attempt to interfere with it, which is more disruptive to global stability. "Space weapons" is also an outdated term as it does not reflect the space threat environment as it currently exists. What we have are capabilities, some of which are deployed in space, and some of which are not, which can be used in a dual-purpose way: benign or aggressive, or for defensive or offensive goals. It is not so much the technology that is the concern but rather the intent behind it and how it is used.

The Secure World Foundation puts out an annual open source assessment of counterspace capabilities of 11 countries (1). We have divided up these capabilities into five categories: co-orbital (objects that are placed into orbit and then manoeuvre to approach their target spacecraft to interfere in ways that can be destructive and non-destructive); direct ascent (ground-, air-, and sea-launched missiles that destroy their target spacecraft through kinetic impact); directed energy (systems that use focused energy, such as laser, particle, or microwave beams, to destroy or interfere with space systems); electronic warfare (radiofrequency interference with satellite communications); and cyber (systems that use network and software techniques to interfere with or destroy computer systems relevant to space capabilities). We also track their space situational awareness (SSA) capabilities, because while simply having an SSA programme does not necessarily indicate that they will be used in a counterspace manner, but if one was interested in those sorts of capabilities, having an indigenous SSA programme would be a key part of that effort.

While there is a wide variety of research and development being done on a broad spectrum of counterspace capabilities, there has not been any use of destructive counterspace capabilities in active military conflicts (2). We have seen direct-ascent anti-satellite (DA-ASAT) tests held by four countries—chronologically, the US, the Soviet Union, China, and India—destroy only their own satellites in low Earth orbit (LEO – 100-2000 kilometres in altitude) and primarily 1000 kilometres and below. We have seen three countries—the US, Russia, and China—conduct co-orbital activities at both LEO and geostationary Earth orbit (GEO – roughly 36,000 kilometres in altitude). Space-related directed energy research is thought to be conducted by four countries (the US, Russia, China, and France), although it is expected that others are exploring it. Non-destructive counterspace capabilities like electronic warfare are used almost universally across the board, and while it is difficult to find open-source information about cyber counterspace capabilities, the general assumption is that multiple countries likely possess cyber capabilities that could be used against space systems.

A well-known incident of the latter type of capability demonstrates that counterspace capabilities can block the use of space capabilities even when they do not target objects in orbit. In February 2022, right before

Russia invaded Ukraine, a cyber-attack was released against ViaSat's KA-SAT satellite communications service. This was done to interfere with Ukrainian military communications, and it was effective: it took out tens of thousands of end-user modems, affecting users not just in Ukraine but all across Europe (3). It did not permanently harm the modems, but it did take some time for them to either get back online or be replaced by working versions. While no one ever officially took credit for the attack, US and other Western officials announced in May 2022 that Russia was behind it (4).

This also demonstrates what many wargaming scenarios have indicated: if counterspace capabilities are to be used against an enemy's capability in an active conflict, they most likely will be of the kind that can be reversed (i.e., not create permanent damage to or destruction of their target) and their target may not necessarily be a spacecraft. Temporary and reversible counterspace capabilities are deemed to be much more usable than kinetic options.

In fact, it could be said that the military utility of DA-ASATs is dropping. They create debris on orbit that threatens all actors at the altitude of interception and below (and frequently even above; the force of impact often spits debris further out to higher altitudes and thus gives it a much longer lifespan (5)). Debris is apolitical. It does not care if you are an ally or a competitor to the creator of the debris. If you are in the way of the debris, the laws of orbital mechanics are the only things that matter. Additionally, these types of counterspace capabilities are, by and large, not temporary. If the goal is to physically impact and destroy a satellite, that is irreversible and permanent.

Furthermore, there is no plausible deniability about who the responsible party is like there is with cyber or even electronic warfare counterspace capabilities. There is also no plausible deniability about intent like there is (at least minimally) with co-orbital counterspace technologies. A destructive ASAT test is not even needed to determine the effectiveness of the interceptor, as modelling and simulation can create the same results without cluttering the space environment. This means that using a DA-ASAT would be an extremely inflammatory step that would be hard to de-escalate, and the country developing it is sinking a lot of money and resources into a largely unusable capability that can be demonstrated through other methods. If other counterspace capabilities can achieve the same outcome as a DA-ASAT system but not carry all the negative consequences of them, then it is possible that countries may move away from developing this sort of counterspace capability to ones that are deemed to be more usable, less damaging to the orbital environment, and not as rigidly escalatory.

Russia's invasion of Ukraine in 2022 also put a spotlight on how the commercial sector is playing an increasingly interwoven role in national security issues. The first example of this is the role of SpaceX in helping with Ukrainian military communications. Its Starlink ground terminals (needed to process the satellite communications) were sent very quickly at the beginning of the conflict directly in response to a tweet pleading with SpaceX's Elon Musk to expedite the process (6). At one point, Ukraine had thousands of Starlink ground terminals in the country, and while multiple governments were paying for most of the ground terminals, SpaceX was, according to some reports, largely paying for most of the internet connectivity itself (7). SpaceX ran out of patience—with the rising costs of maintaining Ukraine's access to Starlink ground terminals (writing to the Pentagon in September 2022 that the cost could be US$120 million through the end of 2022 (8)) and also with its network being used in an active military conflict. It was reported that SpaceX owner Elon Musk refused to activate Starlink coverage to the Crimean coast, as he was worried that Ukrainian drones attacking Russia's submarine fleet there would, in the words of Musk's biographer, "cause a major war" (9).

Russian government officials also began to grumble about the role of Western space companies in military conflicts and started to warn opaquely that they could be perceived as targets, given their roles in the active military conflict (10). The commercial sector has played a part in wars before; 80 percent of US military satellite communications have been carried over commercial satellites, but the war in Ukraine is probably the most prominent example of it doing so.

The Role of SSA

There is one capacity that already has a big role to play in space and counterspace capabilities that will only become more important as time goes on: the ability to collect and interpret space situational awareness

(SSA). SSA—the identification, classification, and tracking of objects in Earth orbit, which includes both active satellites and space debris—is done for various reasons. It can be done for basic spaceflight safety, carrying out complicated activities in space like on-orbit servicing of satellites, or targeting other spacecraft. Hence, while states may want it for non-aggressive reasons, if one is going to be carrying out counterspace activities, SSA is non-negotiable. Historically, it was only the Cold War superpowers who had SSA capacity as it was an offshoot of radars and telescopes intended to keep watch for ICBMs coming over the North Pole; now we are seeing the increasing proliferation of this capacity around the world amongst established space actors building up their military space capabilities.

Most of the SSA data that is shared globally is collected and disseminated by the US via its Space Force's 18th Space Defense Squadron. The US is working to change its internal process for sharing SSA data to one where the Department of Commerce is the main outward facing agency, but for now, it is the US military who is doing this (in the name of spaceflight safety). The 18th Space Defense Squadron monitors 48,000 pieces of debris, but there are anticipated to be hundreds of thousands (if not millions) of debris that are too small to track but could still impact, perhaps in a lethal way, a satellite. Additionally, as of writing (December 2023), there are over 9200 active satellites in orbit (11), of which a majority comes from one entity: SpaceX's Starlink constellation, which contains roughly 5170 active satellites (12). This is an incredibly complicated space traffic picture, and spaceflight safety only gets increasingly challenging as more actors, satellites, and debris get in orbit. As such, it is possible that this could be a flashpoint between two rivals if there are competing ideas of how close satellites are getting to each other or if there is an impact on a satellite from a piece of orbital debris. And if countries deliberately create debris through ASAT tests, that only ratchets up the difficulty of operating in orbit. These tests, since the beginning of the Space Age, have created 6850 pieces of trackable debris, of which, nearly 3500 are still in orbit and most likely will be for years to come (13).

Congestion on and Around the Moon

One place where there is potential for conflict is on and around the Moon. This is due to several reasons. The first is that the actors on the Moon are changing. We have gone from a few missions by the geopolitical superpowers to a situation with a much broader spectrum regarding countries and technical capabilities indicating that they have Moon missions. The Center for Strategic and International Studies released a report in 2022 that counted 106 planned cislunar and lunar missions by 19 countries and one multilateral organisation (the European Space Agency) over the next decade. Four countries have now successfully conducted soft landings on the Moon (14), with India becoming the fourth in August 2023 (interestingly enough, it did so just a few days after Russia crashed its Moon lander, 47 years after it last was able to conduct a controlled landing there).

Another change we see is the type of actor on the Moon. During the early parts of the Space Age, the only actors were civil space agencies conducting scientific and exploratory missions (although there were geopolitical undercurrents to their actions). Now we are seeing commercial missions to the Moon, and, in fact, two of the most recent countries that attempted and failed to achieve a soft landing on the Moon—Israel in 2019 and Japan in 2023—did not use their respective space agencies in their attempts but rather actors in their commercial sectors.

There have even been rumblings about possible military activities on or around the Moon, although that is most likely just speculation by enthusiasts looking to get more money for their particular Moon missions. Article IV of the Outer Space Treaty makes very clear that the Moon and other celestial bodies are to be used for peaceful purposes only; it goes on to say, “The establishment of military bases, installations and fortifications, the testing of any type of weapons, and the conduct of military manoeuvres on celestial bodies shall be forbidden” (15). Most likely, what will be seen are types of activities similar to what the US Space Force talks about in terms of improving cislunar situational awareness, something that, given the spiralling number of missions and actions on the Moon, is helpful from a spaceflight safety perspective; India’s Chandrayaan-2 lunar orbiter had to move three times to avoid other lunar orbiters (as of July 2023) (16).

But even without explicit military missions on the Moon, there are unavoidable geopolitical implications to activities there. This can be seen by the unease expressed about China’s lunar activities: the fact that it landed a lander on the far side of the Moon, something other countries have not accomplished, is viewed through the lens of suspicion thanks to political tensions on Earth.

Another potential source of friction is diverging governance mechanisms regarding the Moon. While the Outer Space Treaty obviously applies to the Moon and other celestial bodies, the new uses of actors in space make how it applies not entirely clear. As such, the US launched its Artemis Accords in October 2020, intended to make explicit guidelines, principles, and best practices for civil space exploration on the Moon and beyond; they are non-legally binding (17). Pulling largely from principles already enshrined in the Outer Space Treaty, the Artemis Accords also cover deconfliction of activities, protecting heritage sites, dealing with space resources, and sharing space data. As of December 2023, 33 countries, including India, have signed the Artemis Accords (18).

The Artemis Accords, in theory, are open to whichever countries are interested in signing them, including Russia and China. That said, while over two decades of experience co-operating in the International Space Station (ISS) has helped NASA build the infrastructure to handle a Russian participant, it is unclear how it would set up something similar for China. Additionally, the impetus for the US Congress's 2011 Wolf Amendment, establishing speed bumps for the US to conduct bilateral activities with China in space, was the idea that China would become a partner in the ISS; it is unclear how well the current iteration of Congress will respond to China potentially being a participant in US activities on the Moon.

Then there is the planned Chinese-Russian International Lunar Research Station (ILRS), details of which were first made public in March 2021. Following a series of Moon missions planned by both Russia and China through the end of the decade, the ILRS is intended to create a crewed base on the Moon in the 2030s. While this initiative is also open to whoever is interested in joining it, as of December 2023, there has been a more muted response, with only eight signatories in total (19). Part of this reluctance may stem from the concern that working with China on space issues may hamper working with the US on space issues; for example, the UAE (one of the original signatories of the Artemis Accords) was supposed to have a payload on a Chinese lunar lander but pulled out in March 2023, citing concerns about how it might run afoul of US export control restrictions (20). It may also be affected by a reluctance by some countries to formally establish ties with Russia after its February 2022 invasion of Ukraine. If so, this at least may not be an issue for much longer: given the unexpectedly truncated ending of Russia's Luna-25 Moon lander and financial and quality control issues with Russia's civil space programme, Russia is unlikely to be able to contribute much in the future. This might explain why Chinese presentations at the 2023 International Astronautical Congress, held in September 2023, did not mention Russia in their ILRS slides (21).

There is no reason that these two governance mechanisms—the Artemis Accords and the ILRS—cannot complement each other; indeed, it would make sense if they had similar principles guiding their behaviour. Yet, it is not outside the realm of possibility that they could turn into competing governance mechanisms. Given the harsh rhetoric used to ascribe intentions to the geopolitical rivals' efforts on the Moon, what we very well may end up seeing are the political complications on Earth being replicated off it, paving the way for conflict there to reach back and engulf the Earth. At the very least, it can make working in the already harsh operating environment of the Moon even harder and more dangerous.

Conclusion

Space is continuing to grow in importance for national security, how economies function, and how societies communicate. As such, ways in which nations can interfere with rivals' access to space data and capabilities will also be of increasing interest.

Additionally, the evolution in how countries use space is leading to a cluttered space traffic management picture, both in Earth's orbit and on and around the Moon, opening more ways in which conflict can extend to Earth from space (or vice versa). National actors should examine their goals for their space programmes to ensure that they do not inadvertently exacerbate existing tensions and create conflict in space.

Victoria Samson *is Chief Director, Space Security and Stability, at the Secure World Foundation, a non-profit that promotes the long-term sustainable use of space.*

Endnotes

(1) Brian Weeden and Victoria Samson, eds., "Global Counterspace Capabilities: An Open Source Assessment," Secure World Foundation, 2023, https://swfound.org/media/207567/swf_global_counterspace_capabilities_2023_v2.pdf

(2) For a visual demonstration of the extent of these capabilities, please see the chart, "2023 Global Assessment," Secure World Foundation, https://swfound.org/counterspace

(3) Viasat, "KA-SAT Network Cyber Attack Overview," Viasat, March 30, 2022, https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

(4) Dan Goodin, "US and its Allies Say Russia Waged Cyberattack That Took Out Satellite Network," *Ars Technica*, May 10, 2022, https://arstechnica.com/information-technology/2022/05/us-and-its-allies-say-russia-waged-cyberattack-that-took-out-satellite-network/

(5) Secure World Foundation, "SWF Releases New Infographic on Anti-Satellite Weapons and Space Sustainability," Secure World Foundation, June 7, 2022, https://swfound.org/news/all-news/2022/06/swf-releases-new-infographic-on-anti-satellite-weapons-and-space-sustainability/

(6) Mykhailo Federov (@FederovMykhailo), Twitter, February 26, 2022, https://twitter.com/FedorovMykhailo/status/1497543633293266944?s=20&t=c9Uc7CDXEBr-e5-nd2hEtw

(7) Alex Marquardt, "Exclusive: Musk's SpaceX Says it Can No Longer Pay for Critical Satellite Services in Ukraine, Asks Pentagon to Pick Up the Tab," *CNN*, October 14, 2022, https://www.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html

(8) Alex Marquardt, "Exclusive: Musk's SpaceX Says it Can No Longer Pay for Critical Satellite Services in Ukraine"

(9) Walter Isaacson (@WalterIsaacson), Twitter, September 8, 2023, https://twitter.com/WalterIsaacson/status/1700342242290901361

(10) Guy Faulconbridge, "Russia Warns West: We Can Target Your Commercial Satellites," *Reuters*, October 27, 2023, https://www.reuters.com/world/russia-says-wests-commercial-satellites-could-be-targets-2022-10-27/

(11) T.S. Kelso, "SATCAT Boxscore," CelesTrak, December 10, 2023, https://celestrak.org/satcat/boxscore.php

(12) Jonathan McDowell, "Starlink Statistics," Jonathan's Space Pages, December 10, 2023, https://planet4589.org/space/con/star/stats.html

(13) "Table 5-1 - Orbital Debris Caused by ASAT Tests in Space," in *Global Counterspace Capabilities: An Open Source Assessment*, eds. Brian Weeden and Victoria Samson (Secure World Foundation, April 2023), 154, https://swfound.org/media/207567/swf_global_counterspace_capabilities_2023_v2.pdf

(14) Kaitlyn Johnson, “Fly Me to the Moon: Worldwide Cislunar and Lunar Missions,” Center for Strategic and International Studies, 2022, https://www.csis.org/analysis/fly-me-moon-worldwide-cislunar-and-lunar-missions

(15) United Nations General Assembly, “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies,” United Nations General Assembly, 1967, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html

(16) Indian Space Research Organisation, “Current Space Situation Around the Moon: An Assessment,” Indian Space Research Organisation, August 8, 2023, https://www.isro.gov.in/Current_Space_Situation_around_Moon_Assessment.html

(17) National Air and Space Administration, “NASA, International Partners Advance Cooperation with First Signings of Artemis Accords,” National Air and Space Administration, October 13, 2020, https://www.nasa.gov/news-release/nasa-international-partners-advance-cooperation-with-first-signings-of-artemis-accords/

(18) Roxana Bardan, “NASA Welcomes Angola as Newest Artemis Accords Signatory,” National Air and Space Administration, December 1, 2023, https://www.nasa.gov/general/nasa-welcomes-angola-as-newest-artemis-accords-signatory/

(19) Andrew Jones, “Egypt Joins China’s Moon Base Initiative,” *Space News*, December 7, 2023, https://spacenews.com/egypt-joins-chinas-ilrs-moon-base-initiative/

(20) Ling Xin, “US Tech Rules Bar UAE Moon Rover from China’s Chang’e 7 Mission: Sources,” *South China Morning Post*, March 23, 2023, https://www.scmp.com/news/china/science/article/3214396/us-tech-rules-bar-uae-moon-rover-chinas-change-7-mission-sources

(21) Andrew Jones (@AJ_FI), Twitter, October 3, 2023, https://twitter.com/AJ_FI/status/1708940207351910611

GENERAL STRATEGIC PERSPECTIVES

Should India Publicly Attribute International Cyber Incidents?

Arindrajit Basu

WE LIVE IN AN AGE OF CYBER 'UNPEACE' (1) where modern mid-spectrum rivalry "fits neither the destructive criteria [and violence] of war nor the acceptable boundaries of peace." (2) As the introductory note to this special issue suggests, the blurring of cyber boundaries brought about by asymmetry allows both states and nation-states to attain international economic and geo-political objectives without engaging in traditional kinetic warfare.

This new reality compels holistic and cohesive thinking from policy-makers world over on how to exploit opportunities and ward off threats posed by the pervading uncertainty of cyber 'unpeace'. International cyber operations, frequently undertaken by states, state-backed actors, or independent non-state actors, provide asymmetric advantages to entities that may not boast traditional military or technological power. The many challenges of effectively attributing attacks to a perpetrator or group compounds geopolitical uncertainty.

A bevvy of literature documents the technical constraints on attribution. Cyberattacks span stages, steps, and jurisdictions (3). This adds several layers of complexity to the attribution process. The system deploying the offensive capability is usually several degrees removed from the computer or computer network being infiltrated. Attackers can obfuscate using different technical means like botnets, spoofing, and false flag techniques to deceive the forensic analyst, not to mention the use of proxy networks (4). States or private actors can likewise use varied technical means to trace the attack's origins, but accurate attribution remains a cumbersome and challenging process (5).

Given these impediments, some experts argue that attribution is as much an art as it is a science (6). No technical cyber forensic analysis can fully solve the attribution challenge in cyberspace. Some analysts have, however, highlighted the benefits of public attribution. Researchers at the RAND Corporation believe that public attribution furthers credibility, enables information exchange that improves the quality of attribution, and can potentially deter future adversaries by signalling that existing mechanisms can detect and retaliate against attacks. Others are more circumspect about these benefits (7) and highlight the potential costs of publicly attributing, including misattribution and escalation (8).

Scholarship published in the past two years recognises both arguments and suggests frameworks to guide decision-makers on publicly attributing cyber incidents (9). As noted by the editors of this Special Issue, the transformation of warfare and the age of unpeace demands an arsenal of strategic options to counter cyber incidents and secure India's burgeoning digital economy. Public attribution, undertaken coherently and underscored by logical and robust decision-making, can be a useful tool. Thus far, India has not publicly attributed a specific international cyber incident to a specific private perpetrator or nation-state. By using and applying the models put out by Western scholars, this chapter proposes some suggestions on how India can think about the public attribution of cyber-attacks.

Cyber Threat Landscape in India

Increased digitisation combined with its geopolitical location amidst two adversarial neighbours has left India facing a significant number of cyber-attacks every year (10). Check Point Research released a report stating that organisations in the country faced an average of 2108 cyberattacks weekly in the first quarter of 2023, marking a 15 percent increase compared to the same period in previous years (11). Critical infrastructure has often been at the receiving end of several cyberattacks. Notable attacks (12) include the Cosmos bank fraud where a malware attack authorising fraudulent transactions causing the bank to lose INR 94 crores in 2018 (13); the D-Track malware attack that breached the Kudankulam reactor's administrative network in 2019 (14), and the disruption of the IT network of AIIMS, one of India's leading government-run hospitals in 2022 (15).

Officials have acknowledged that finding the necessary evidence to attribute cyberattacks to a specific perpetrator is challenging (16). Lt. General Pant, then India's National Cybersecurity Coordinator, specifically highlighted the hurdles posed by the cumbersome Mutual Legal Assistance Treaty (MLAT) process in obtaining information from international partners.

While India has yet to publicly attribute an international cyberattack or cyber incident, it came close to doing so in 2018 when a report shared with the National Security Council Secretariat by CERT-In claimed that 35 percent of cyberattacks on official Indian websites originated from China followed by 17 percent from US, 15 percent from Russia, 8 percent from Pakistan, 7 percent from Canada, and 5 percent from Germany (17). However, the full text, along with any possible accompanying evidence, is not in the public domain. Information can only be gleaned from media reports. Thus, it is unclear whether CERT-In has attributed specific attacks to specific perpetrators or countries. Therefore, this cannot be considered an intentional public attribution.

In fact, politicians and officials have made a conscious effort not to name the perpetrator or state of origin when acknowledging and characterising cyber-attacks or attempts to conduct cyberattacks. For example, the government explicitly denied a Chinese role in a cyberattack that temporarily brought down the Maharashtra electricity grid despite findings by threat intelligence company Recorded Future suggesting that was the case (18). Again, with the more recent AIIMS cyber-attack, in a written reply to the Rajya Sabha Minister of State Rajeev Chandrashekhar publicly forensically characterised the "sophisticated ransomware" attack claiming it was a "conspiracy and planned by [significant] forces" (19) He also divulged vulnerabilities in network segmentation that enabled the perpetrators to conduct the attack but stopped short of attributing the attack to a non-state actor or a nation state.

Perspectives of States, Non-State Actors and Global Forums on Public Cyber Attribution

State Practice

While India has taken a clear stance to not publicly attribute, others have taken a different route. Several countries have expressed national positions on attribution, either in statements on the applicability of international law to cyberspace or in their national cybersecurity strategies (20). France (21), Germany (22), Finland (23), and Italy (24) clearly state that the choice to publicly attribute or not is a national sovereign prerogative and an independent decision to be made by each nation-state. While all states refer to the applicability of the existing international law on cyber attribution to cyberspace, some states underscore the relevance of the political aspects of cyber attribution. France and Finland explicitly state that the decision to attribute a cyberattack originating in another state is a national political decision that must take several circumstances and evidence into account.

The Netherlands has considered public attribution a cornerstone of cyber defence. In their latest Cyber Defense Strategy, it argues that "An active political attribution policy contributes to the deterrent ability and makes the Netherlands less attractive as a target of cyberattacks. A state actor who is held accountable for his actions will make a different assessment than an attacker who can operate in complete anonymity." (25) The 2015 United States Department of Defense's Cyber Strategy further acknowledges the role of attribution in establishing a credible cyber deterrence strategy and goes on to clearly articulate the US's cyber attribution capacity "On matters of intelligence, attribution, and warning, DoD and the intelligence community have invested significantly in all source collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace" (26).

State-led public attributions for cyberattacks thus far have mostly been carried out by the US, the EU, and their NATO partners (27). With notable exceptions such as Brazil and Pakistan, these are the same states that have weighed in officially on the applicability of existing international law standards to cyberspace.

Other states, such as China, are more circumspect about the public attribution of cyberattacks by the United States and its partners in the Five Eyes intelligence alliance (Australia, Canada, New Zealand, and the UK) (28). In Beijing's view, public attributions by the US are underscored by unclear norms regarding the acceptable limits of offensive cyber operations and act as both a legal weapon to legitimise future indictments and sanctions against China and a political weapon to inflict reputational costs on the adversary (29). This position need not be taken at face value, though. Beijing itself participates in much offensive cyber activity, and the claim of politicisation itself could be used to delegitimise US attribution and follow-up action, even if they are in line with accepted standards of international law.

International Legal Standards

The international law on attribution for the purpose of affixing state responsibility is relatively well-settled, although its application to specific contexts, including in the cyber realm, remains a challenge. As per international law, state responsibility is premised on two components: an act or omission that amounts to the breach of an international obligation and an attribution of said act or omission to a state in question. The acts of a private person are not attributable to a state unless the private actor is within the "effective control" of the state; that is, it is "in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct" (30).

The law of state responsibility does not, however, weigh in on evidentiary standards or burdens of proof. Further, there is no international legal obligation to provide evidence backing up a public attribution (31). Standards of "sufficient levels of confidence" (32) or "sufficient certainty" (33) have been proposed to assess evidence before a decision to publicly attribute is made.

Global Forums

Global forums fermenting responsible state behaviour in cyberspace have recognised the relevance of attribution to these debates. The 2015 consensus report of the United Nations Group of Governmental Experts (UN-GGE), set up to identify norms for responsible state behaviour in cyberspace, suggested a norm on cyberattack attribution (34). Norm 13 (b) reads "In the case of ICT incidents, States should consider all relevant information including the larger context of the event, the challenges of attribution in the ICT context, and the nature and extent of the consequences." The 2021 UN-GGE report provided further guidance on aspects that states may consider in the decision-making process, such as the technical attributes of the attack, scope, scale and impact, consultations between the states, and the wider contextual implications on international peace and security (35).

The 2021 report also recommended cooperation between Computer Emergency Response Teams that could improve state capacity in detecting and investigating malicious attacks. Finally, it recommended that states proactively use regional, bilateral, and multilateral forums to exchange best practices and cast some light on national approaches to attribution with the overarching goal of fostering common understandings and an exchange of best practices on attribution.

Private Sector Attribution

It is also worth noting that several public attributions have been conducted by private sector actors. Cybersecurity firms Mandiant (36) and Crowdstrike (37) have published detailed reports attributing high-profile cyber incidents to China and Russia, respectively. Recorded Future, another US-based cybersecurity firm, has attributed the continuous targeting of critical infrastructure in India, including electricity grids, to Chinese state-sponsored groups (38). With the ongoing armed conflict in Ukraine, US-based technology companies such as Microsoft and Google have published detailed blog posts publicly attributing aggressive, offensive cyber activity to Russian-backed cyber actors looking to gain a decisive war-time advantage. Non-governmental organisations such as Citizen Lab (39), Electronic Frontier Foundation (40), and Amnesty International (41) have also publicly attributed the deployment of offensive cyber capabilities, largely in instances where these capabilities have been deployed against journalists, politicians or other human rights defenders.

Given their role in the growing ecosystem of “decentralised cyber attribution” (42), these private actors have also weighed in on the necessary methods, processes, and evidentiary considerations for public attribution. For example, in a detailed blog post titled ‘Navigating the trade-offs of cyber attribution,’ Mandiant researchers highlight four trade-offs for security leaders when making the decision to publicly attribute (43). These include the allocation of resources, the trade-off between analytical independence and neglecting important insights from other actors also involved in the attribution processes, between making rash attribution judgments that risk misattribution and an overly cautious approach that prevents the detection and necessary action regarding a cyberattack, and, finally, the decision to go public itself. On going public, Mandiant recommends considering several factors, including source sensitivities, a victim's reaction, the impact on the attacker's geopolitical context and implications for ongoing cyber engagements. Compared to the broader guidelines articulated in the 2021 UN-GGE report, Mandiant offers more specific guidance which may be operationally useful for decision-makers.

A Decision-Making Framework

The decision-making framework for publicly attributing cyber incidents should appreciate the multiple possible goals of cyber attribution, utilise India's institutional architecture effectively, and have clear criteria in place at each step of the detection and attribution process. Most significantly, decision-makers must remember that publicly attributing a cyber-attack does not signal a cyber defence failure to the Indian public or the wider world (44). Cyberattacks and breaches are an accepted part and parcel of today's geopolitical scenario. A well-articulated cyber attribution could signal that the Indian institutional architecture and forensic capability are resilient enough to deal with this new reality.

As articulated by Egloff and Smeets, public attribution could be considered by decision-makers looking to pursue one or more goals (45). Drawing from their work, policymakers could consider the following objectives listed below:

Deterrence: Public attribution could deter adversaries from carrying out future attacks as they fear getting caught and facing punitive measures. Most analysts, however, disagree with the deterrence potential of mere 'naming and shaming.' In fact, some argue that mere naming and shaming without follow-up action, such as sanctions, may end up encouraging adversaries to continue their exploits. Even if followed up with sanctions, the costs imposed may not be significant enough to alter macro decision-making on continuing to undertake offensive cyber operations, given the gains to be made through espionage or other forms of offensive operations (46). Further, as is the case with the India-Pakistan context, in several instances, cyber proxies may be operating at an arm's length from the state and have little to lose if sanctions or reputational costs are imposed on the state.

Causing friction: Publicly revealing evidence regarding an adversary's capabilities could serve counter-threat objectives as the adversary would need to develop new capabilities to avoid detection in the future. Friction does not prevent adversaries from mounting continuous action but imposes operational hurdles.

Building resilience across the ecosystem: Public attribution and disclosure of evidence on capabilities and vulnerabilities could help network owners both in the public and private sectors to audit and secure their own hardware and software systems accordingly.

Norm-building: Naming and shaming behaviour that violates norms agreed upon at international forums strengthens the norm by "demarcating what is appropriate behaviour" and publicly pushing countries to comply. Of course, norm-building works best if norms of responsible state behaviour or prevailing understandings of international law are explicitly referenced in the statement attributing specific cyber incidents.

Community and international cooperation: Attribution published to the general public or shared with trusted partners in the research community, or the Computer Emergency Response Teams (CERTs) could jointly strengthen attribution capabilities and aid in detecting cyber threats. Further, such information-sharing mechanisms could help build international credibility and confidence among partners in plurilateral mechanisms such as the Quadrilateral Security Dialogue.

Domestic criminal law enforcement: With enough forensic evidence to justify violating domestic criminal law, states may publicly attribute a cyberattack through an indictment before the judiciary. The US Department of Justice announced indictments against 41 criminal actors based in Russia, China, Iran and North Korea (47) and also indicted officers of the Russian Main Intelligence Directorate Unit in 2020 (48).

Institutional Architecture and Decision-Making Framework on Cyber Attribution

Several bodies in India's institutional architecture for cybersecurity should play a coordinated role in the proposed cyber attribution model. This includes the Prime Minister's Office comprising the technical intelligence agency National Technical Research Organization and the National Critical Information

Infrastructure Protection Centre (NCIIPC) (49). India's computer emergency response team falls within the jurisdiction of the Ministry of Electronics and Information Technology and is responsible for detecting, mitigating and preventing cybersecurity incidents. Finally, there is the Defence Cyber Agency, first announced in 2018, which draws armed force personnel from all three branches and falls within the Ministry of Défense.

A cyber incident would generally be detected by CERT-In or the NCIIPC in the case of critical infrastructure. After the forensic characterisation, decision-makers may choose to go public based on several factors, including the level of confidence in the characterisation; the need to protect sensitive sources; geopolitical considerations such as whether the attack originates from an adversarial or friendly country; available response options that could be undermined by a public attribution; the severity of the attack and risks of escalation.

If the decision to go public is made, the attribution format is equally important. Policymakers could consider one of four options. The first option is a criminal indictment that can be exercised if the law enforcement authorities have sufficient evidence to prosecute under the Indian Penal Code or Information Technology Act. The second option is international legal attribution to a state as per the evidentiary standards of international law: the attribution statement should be put out by the office of the National Cybersecurity Coordinator, either jointly or in close consultation with the Ministry of External Affairs and relevant legal experts, either working full-time in the Ministry or as consultants.

The third option is a political attribution at the Ministerial level that need not reference international law or meet evidentiary standards. Instead, the goal is to win "the hearts and minds of audiences that open up with public attribution." (50) Indeed, most public cyber attributions have not referenced domestic or international law (51).

A fourth option is to rely on third-party attribution. As discussed before, the private sector and civil society have been doing an effective job of publicly attributing cyberattacks as well as crafting their own policy and strategies on the same. A potential option here for the Indian government in cases where an initial attribution has been done by a private actor such as Mandiant or Recorded Future could be to "acknowledge" the report but neither confirm nor deny its findings.

Conclusion

None of these available options, either individually or in concert, will necessarily achieve the set-out goals given the variables at play. However, bearing this framework in mind provides decision-makers with more options. For example, a criminal indictment underscored by a strong public statement by the National Cyber Security Coordinator could demonstrate India's capabilities while undermining that of adversaries even if no one faces a single day in court. To implement a model and attribute both effectively and responsibly, India must create coordination mechanisms that bring all relevant government and non-government entities into the decision-making spectrum. CERT-In should certainly be involved with any such process given their role and existing capacity, but sector-specific stakeholders and government entities must also play their part. Further, effective characterisation of a cyber incident and consequent public attribution can be furthered by regularly discussing methodological challenges, and opportunities, and sharing intelligence with trusted partners such as the Quadrilateral Security Dialogue, which already has avenues for exchanges between the top cybersecurity personnel of the respective countries, and has also envisaged greater cooperation between the respective CERTs. While sharing threat intelligence is easier among formalised military alliances, there is enough trust between Quad partners in the security and technological domains to create appropriate processes and mechanisms.

Given its geopolitical position in cyberspace, India cannot afford to not use the critical option of public attribution, when deemed effective, to navigate the uncertainty of cyber unpeace and further its strategic interests. Cyber 'unpeace' is here to stay, and we cannot wish it away. We can use institutions, norms and capabilities, however, to mitigate its impact.

Arindrajit Basu *is a PhD candidate at the Faculty of Global Governance and Affairs, Leiden University.*

Endnotes

(1) Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017), 78.

(2) Lucas Kello, "Cyber Legalism: Why it Fails and What to Do About it," *Journal of Cybersecurity* 7 (2021), https://academic.oup.com/cybersecurity/article/7/1/tyab014/6343244.

(3) David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, ed. Committee on Deterring Cyberattacks (Washington, DC: The National Academies Press 2010), 25–40.

(4) Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38 (2015).

(5) Clark and Landau, "Untangling Attribution"

(6) Rid and Buchanan, "Attributing Cyber Attacks"

(7) John S. Davis II et al., *Stateless Attribution: Toward International Accountability in Cyberspace* (Santa Monica: RAND Corporation, 2017).

(8) Izumi Nakamitsu, "Remarks at the UN Securiry Council Open Debate on Cyber Security: Maintaining International Peace and Security in Cyberspace" (speech, VTC, June 29, 2021), UNODA, https://un.mfa.ee/wp-content/uploads/sites/57/2021/06/Nakamitsu-29-June.pdf.

(9) Florian J. Egloff and Max Smeets, "Publicly Attributing Cyber Attacks," *Journal of Strategic Studies* 46, no. 3 (2023), https://www.tandfonline.com/doi/full/10.1080/01402390.2021.1895117; Ariel (Eli) Levite and June Lee, "Attribution and Characterization of Cyber Attacks," in *Managing U.S.-China Tensions Over Public Cyber Attribution*, ed. Ariel E. Levite et al. (Washington DC: Carnegie Endowment for International Peace, 2023), https://carnegieendowment.org/2022/03/28/attribution-and-characterization-of-cyber-attacks-pub-86698; Dennis Broeders, Els De Busser, and Patryk Pawlak, "Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates," The Hague Program for Cyber Norms, 2020, https://www.universiteitleiden.nl/en/research/research-output/governance-and-global-affairs/three-tales-of-attribution-in-cyberspace.-criminal-law-international-law-and-policy-debates.

(10) K. V. Kurmanath, "India Emerges as Top-3 Target for Nation-State Driven Cyber Attacks," *Business Line*, October 6, 2023, https://www.thehindubusinessline.com/info-tech/india-emerges-as-top-3-target-for-nation-state-driven-cyber-attacks/article67387522.ece.

(11) Tech Desk, "Cyber Attacks Increased by 18 Per Cent This Year Alone in India," *Indian Express*, May 7, 2023, https://indianexpress.com/article/technology/tech-news-technology/cyber-attacks-in-india-increased-by-18-per-cent-in-2023-check-point-8596348/.

(12) See for a detailed coverage of notable cyber incidents, Sameer Patil, *Securing India in the Cyber Era* (Oxon: Routledge,2022).

(13) Express News Service, "Cosmos Bank Malware Attack: Pune Court Convicts 11 Accused," *Indian Express*, April 23, 2023, https://indianexpress.com/article/cities/pune/cosmos-bank-malware-attack-pune-court-convicts-11-accused-8570830/.

(14) Melissa Robbins, "Cyberattack Hits Indian Nuclear Plant," *Arms Control Today*, December 2019, https://www.armscontrol.org/act/2019-12/news/cyberattack-hits-indian-nuclear-plant.

(15) Ashish Aryan, "AIIMS Cyber Attack Took Place Due to Improper Networks Segmentation," *Economic Times*, February 10, 2023, https://economictimes.indiatimes.com/tech/technology/aiims-cyber-attack-took-place-due-to-improper-network-segmentation-govt-in-rs/articleshow/97805598.cms?from=mdr.

(16) Soumik Ghosh, "Lack of Cyber Attribution a Major Challenge for India: Lt. Gen Pant," CSO, September 2, 2020, https://www.csoonline.com/article/569797/lack-of-cyber-attribution-a-major-challenge-for-india-lt-gen-pant.html.

(17) Mahender Singh Manral, "35 Percent of Cyber Attacks on Indian Sites from China: Official Report," *Indian Express*, August 23, 2018, https://indianexpress.com/article/india/35-of-cyber-attacks-on-indian-sites-from-china-official-report/.

(18) ANI, "'Human Error, Not Chinese Cyber Attack,' Says Union Power Minister on Mumbai 2020 Blackout," *Economic Times*, May 3, 2021, https://energy.economictimes.indiatimes.com/news/power/human-error-not-chinese-cyber-attack-says-union-power-minister-on-mumbai-2020-blackout/81303209.

(19) Aryan, "AIIMS Cyber Attack Took Place Due to Improper Networks Segmentation"

(20) NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "Attribution," in *NATO CCDCOE Excellence Cyber Law Toolkit Database*, https://cyberlaw.ccdcoe.org/wiki/Attribution; NATO CCDCOE Cyber Law Toolkit, https://cyberlaw.ccdcoe.org/wiki/Main_Page.

(21) Ministry of Defense of France, International Law Applied to Operations in Cyberspace, September 9, 2019.

(22) Federal Government of Germany, "On the Application of International Law in Cyberspace," 2021, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

(23) Ministry of Foreign Affairs, "Finland Published its Positions on Public International Law in Cyberspace," Finnish Government, October 15, 2020, https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace.

(24) Italian Ministry for Foreign Affairs and International Cooperation, "Italian Position Paper on International Law and Cyberspace," 2021, https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.

(25) Ministerie van Defensie, „Defensie Cyber Strategie 2018: Investeren in Digitale Slagkracht Voor Nederland," trans. Egloff and Smeets, 2018.

(26) The Department of Defense, *The Department of Defense Cyber Strategy* (Washington DC: Department of Defense), https://www.hsdl.org/c/view?docid=764848.

(27) Lu Chuanying, „A Chinese Perspective on Cyber Attribution," in *U.S.-China Tensions over Public Cyber Attribution*, ed. Ariel E. Levite et al., (Washington DC: Carnegie Endowment for International Peace, 2023)

(28) Chuanying, „A Chinese Perspective on Cyber Attacks"

(29) Levite and Lee, „Attribution and Characterization of Cyber Attacks"

(30) International Law Commission, „Responsibility of States for Internationally Wrongful Acts 2001," United Nations, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf; Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), Rule 17.

(31) NATO CCDCOE, „Attribution"

(32) Federal Government of Germany, "On the Application of International Law in Cyberspace"

(33) NATO CCDCOE, "National Position of the Netherlands (2019) in the NATO CCDCOE Cyber Law Toolkit Database," https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_Netherlands_(2019); NATO CCDCOE Cyber Law Toolkit, https://cyberlaw.ccdcoe.org/wiki/Main_Page.

(34) "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015, https://digitallibrary.un.org/record/799853?ln=en.

(35) "Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security," July 14, 2021, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.

(36) APT1: Exposing One of China's Espionage Units," *Mandiant*, December 30, 2021, https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units.

(37) Brian Ross et al., "'Beyond a Reasonable Doubt' Russians Hacked DNC, Analyst Says," *abc News*, July 26, 2016, https://abcnews.go.com/International/reasonable-doubt-russians-hacked-dnc-analyst/story?id=40863292.

(38) INSIKT Group, "Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Groups," *Recorded Future*, April 6, 2022, https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets.

(39) "NSO Group," The Citizen Lab, https://citizenlab.ca/tag/nso-group/.

(40) Cooper Quintin and Eva Galperin, "Dark Caracal: You Missed a Spot," Electronic Frontier Foundation, December 10, 2020, https://www.eff.org/deeplinks/2020/12/dark-caracal-you-missed-spot.

(41) Amnesty International, "The Pegasus Project: How Amnesty Tech Uncovered the Spyware Scandal-New Video," Amnesty International, March 23, 2022, https://www.amnesty.

org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/.

(42) Kristen. E. Eichensehr, "Decentralized Cyber Attack Attribution," AJIL Unbound, June 24, 2019, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/decentralized-cyberattack-attribution/36189FEEC7937C0588C1A782BD BB4395.

(43) Jamie Collier and Shanyn Ronis, "Navigating the Trade-Offs of Cyber Attribution," *Mandiant*, January 17, 2023, https://www.mandiant.com/resources/blog/trade-offs-attribution#:~:text=Attribution%20percent20matters%20percent2C%20 percent20but%20percent20to%20percent20what,regularly%20percent20involves%20 percent20difficult%20percent20trade%20percent2Doffs.

(44) Sameer Patil (discussion with author, October 18, 2023).

(45) Egloff and Smeets, "Publicly Attributing Cyber Attacks"

(46) Jack Goldsmith and Robert D. Williams, "The Failure of the United States' Chinese-Hacking Indictment Strategy," *Lawfare*, December 28, 2018, https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy.

(47) Garrett Hinck and Tim Maurer, "Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity," *Journal of National Security Law and Policy* 10 (2020): 528.

(48) Department of Justice, Government of the United States, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

(49) For details on India's cybersecurity architecture, see Arindrajit Basu, *India's International Cyber Operations: Tracing National Doctrine and Capabilities*, United Nations Institute for Disarmament Research, Geneva, UNIDIR, 2022, https://www.unidir.org/cyberdoctrines/India.

(50) Broeders, De Busser, and Pawlak, "Three Tales of Attribution in Cyberspace"

(51) Dan Efrony and Yuval Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice," *American Journal of International Law* 112, no. 4 (2018), https://www.cambridge.org/core/journals/american-journal-of-international-law/article/abs/rule-book-on-the-shelf-tallinn-manual-20-on-cyberoperations-and-subsequent-state-practice/54FBA2B30081B53353B5D2F06F77 8C14.

How the US Should Prepare for Space Warfare: Illustrated by Countering Rendezvous Spacecraft Threat

Brian G. Chow

IN 2007, AFTER CHINA SUCCESSFULLY TESTED its ground-launched direct-ascent antisatellite (ASAT) missile, the US realised that it needed to enhance its space power after spending decades optimising its satellites for performance while neglecting their resilience under attack. In the years since, the US has directed significant additional resources—both monies and talents—to counter existing and emerging space threats. For example, the Space Force budgets have steadily risen since its establishment. Its first budget in fiscal year 2021 was US$15.3 billion, grew to US$18 billion in 2022, jumped to US$26.3 billion in 2023, and hits US$30 billion (as a budget request) in 2024 (1).

While these commitments are promising, the devil is in the details, especially when the US's overall space resilience is only as strong as its weakest link. Feeble protection of critical satellites creates a susceptibility that can be exploited by an aggressor country to prevent the US from defending the alliances that form the foundation of its national security strategy. Two main root causes could leave a few serious ASATs unattended. First, the US no longer reigns supreme in military power. Defence Secretary Lloyd J. Austin believes China is a pacing challenge for the Pentagon (2). Space is no exception. China has been following an asymmetric strategy, of which counterspace is a key component. Currently, China can pose ASAT threats with ground-based jammer, ground-launched direct-ascent

ASAT missile, ground-based laser blinding, cyber-attack on command-and-control links for satellites (3) and satellite ground systems (4), and high-altitude nuclear electromagnetic pulse (5). The emerging threats in this decade are rendezvous spacecraft (R-spacecraft), ground-based high-power laser (to damage the exterior of low-earth-orbit satellites) (6), and space-based high-power microwave beams (to damage or interfere with the electronics of other satellites) (7). Further down the road will be the placement of smaller-version of ground-based ASATs in orbit (to be closer to their targets). In addition, as NASA's Artemis Program has opened the door for commercial operations on the moon, there may arise conflicts that laws or diplomacy cannot resolve, making space warfare on the moon and in the transfer orbits to and from the moon possible. Russia, Iran, and North Korea also pose counterspace threats (8). As the US faces many space threats with different characteristics, each individual threat calls for an in-depth analysis and tailored solution.

Second, the US's historically complacent posture against adversaries amplifies its vulnerability. During the Cold War, according to nuclear strategist Albert Wohlstetter, the US "systematically underestimated the number of vehicles the Soviet Union would deploy" (9) and assumed that its adversaries would follow "Western-preferred Soviet strategies" (10) or what it wished they would do, as opposed to what they would do according to their own "interest," "technical alternatives," and opportunities. Wohlstetter concluded that the US "must expect a vast increase in the weight of attack which the Soviets can deliver with little warning, and the growth of a significant Russian capability for an essentially warningless attack" (11). Sixty-five years later, the US remains similarly clueless about the possibility of a warningless attack taking the shape of a space Pearl Harbor. In the foreword to Roberta Wohlstetter's *Pearl Harbor: Warning and Decision*, Nobel Laureate Thomas Schelling (12) stated that "there is a tendency in our planning to confuse the unfamiliar with the improbable. The contingency we have not considered seriously looks strange; what looks strange is thought improbable; what is improbable need not be considered seriously." The US's current perspective about the unlikely prospects of a space Pearl Harbor within this decade may be foolish optimism, as warned by these prominent thinkers of the nuclear age.

In July 2023, the US military apparently went all-in on space resilience, with over 300 mentions of the term in the Space Force's 2024 budget documents (13). In addition, Lt. Gen. DeAnna Burt, deputy chief of space operations, cyber and nuclear, stated that the US needs "to prevent a Pearl Harbor-style attack in space" (14). The dual-use spacecraft (R-spacecraft) capable of rendezvous and proximity operations (RPO) is the practical ASAT to materialise such a threat within this decade.

R-spacecraft are already being developed or were deployed by not only China and Russia, but also the US, European Union, Japan, and other nations. They can be used to refuel, repair, and upgrade another satellite or to grab and remove space debris from space traffic lanes. These functions are critical to providing prosperity to the world. On the other hand, an adversary's R-spacecraft can be pre-positioned close to the US's critical satellites during peacetime or crisis, as there is no prohibiting rule. These already closed-in spacecraft can quickly reach the US's satellites to bend or disconnect antennae and solar panels or spray paint sensors, thus disabling American satellites with little space debris generated. Alternatively, these R-spacecraft can simply tow the US's satellites into 'useless' orbits where they can no longer perform their intended missions. To boot, this alternative disablement generates no space debris. In contrast, China's successful 2007 demonstration of its ASAT capability with a kinetic kill promptly drew worldwide condemnation on the huge amount of space debris generated, some of which will remain in orbit for decades. Thus, R-spacecraft might well be China's ASAT weapon of choice to mount a space Pearl Harbor within this decade.

In the spirit of wargames and planning scenarios, quantification should be attempted as much as possible, including appraisals of the date and size of threats. Though these are uncertain estimates, specific input assumptions provide concrete targets upon which to base discussion and collaboration for a better solution. For example, a suggestion that the R-threat could occur as early as 2026 hopefully prompts space experts to argue that the date should be, say, 2031 instead. Then, constructive discussions ensue: Why 2031? Even so, can preparation be delayed by five years? Or should a response be ready by 2026, just in case?

Since these dual-use spacecraft provide critical services to space sustainability, they clearly cannot be banned outright, and the global community must find a safe way to live with them.

China’s R-Spacecraft Development

Space robotic arm technology is critical for the development of dual-use R-spacecraft. Kevin Pollpeter (15) observed that China began researching this technology in the 1980s. Apparently, two decades later, this robotic technology and that of rendezvous, including docking, had matured enough for system testing of R-spacecraft as a whole. According to Brian Weeden (16), between 2008 and 2020, China conducted six series of tests of satellite technologies for RPO. The author found that the BX-1 chaser satellite (17) (September 2008 test) had a mass of 40 kg, well below 180 kg (18), the threshold of a small satellite as defined by NASA. Another of the three chaser satellites, CX-3 (19), in the July 2013-May 2016 tests, was also appraised as a small satellite. China’s forethought in developing small R-spacecraft, usable as ASATs, is important to recognise because these R-spacecraft can be quickly and inexpensively manufactured in large quantities and can overwhelm expensive bodyguard spacecraft used to protect US satellites. Even better for China, the US’s current course of action is unlikely to ready such bodyguards, whether expensive or cheap, by the time R-spacecraft come.

In January 2022 (20), China successfully docked with a non-responsive satellite in a geosynchronous orbit (GEO) and manoeuvred it to a higher orbit, less than two years behind the US doing the same. Moreover, in April 2022, Andrew Jones (21) reported that the China Academy of Space Technology will be capable of producing more than 200 small satellites each year. This adds to the capability developed by the China Aerospace Science and Industry Corporation to manufacture 240 small satellites each year. In February 2023, Stephen Chen (22) reported that China aims to launch nearly 13,000 satellites quickly to prevent SpaceX from hogging ‘low-orbit resources’, according to People’s Liberation Army space scientists. Thus, estimating that China will be able to develop and deploy about 200 R-spacecraft (23) by 2026 is conservative, especially when China has great incentive to do so given how this ASAT capability can aid its Taiwan ‘reunification’ effort, a diplomatic thorn in China’s side for seven decades.

Parallel to developing R-spacecraft for peaceful and hostile uses, China has been hard at work at the UN and other multilateral forums. It stated that “the UN should play its role as the central platform for outer space governance in order to ensure extensive participation, fairness and inclusiveness in related international rule-making process" (24). UN decisions are made by consensus except in its UN Security Council, where China has veto power. No surprise that China wants the UN to play the central role, as it has positioned itself to decline any actions it deems unfavourable.

Moreover, China stated that it "has consistently advocated the peaceful uses of outer space and firmly opposed the weaponization of and an arms race in outer space" (25). Indeed, China, as well as Russia, participated in the development of 21 Guidelines for the Long-term Sustainability of Outer Space Activities in 2008 as well as its updated 2014 iteration. China and Russia have also taken the lead in proposing a draft Treaty on the Prevention of the Placement of Weapons in Outer Space and the Threat or Use of Force against Outer Space Objects (PPWT). In 2022, however, US Mission Geneva summarised the view of four successive US administrations that, "given the dual-use nature of many space systems, it is impossible to define a 'weapon in space,' which may lead to legal divergence and opening the door to the intentional evasion of legal obligations" (26).

This 'impossibility' or inherent ambiguity in defining a space weapon is advantageous to China and Russia and detrimental to the US. China can claim the high ground in space arms control by proposing to prohibit weapons in space, while developing R-spacecraft, the crown jewel of its counterspace strategy, under cover of peaceful pretence. Many in the US, as well as other countries, have long abhorred weapons in space and still believe that space weapons can somehow be banned, even in the presence of dual-use space systems such as R-spacecraft that can be switched at will between peaceful and hostile actions without warning. Worse yet, they do not want the US to develop R-spacecraft into small and cheap bodyguard spacecraft to defend against China's hostile R-spacecraft because China will certainly define our bodyguard spacecraft as space weapons. Perhaps they are worried that this turn of events could prevent a space agreement with China and Russia.

In 2018, Russia blocked voluntary "measures for the safe conduct of proximity space operations" (27) from being added to the 21 Guidelines. Moreover, during the third session (30 January to 3 February 2023) of the Open-Ended Working Group on Reducing Space Threats, Cuba, "Algeria, India, Brazil, Mexico, and the Philippines expressed support for the PPWT" (28). China and Russia continue to promote PPWT with their unsupported and even outlandish definitions of space weapons and non-weapons. For example, China labelled the US Mission Extension Vehicle (MEV), which is designed for on-orbit satellite servicing—China is also developing similar capabilities—as a "weapon" (29). The fourth and final session (28 August to 1 September 2023) was now over. Yet, the Group was still "unable to reach consensus on the final report, largely due to intransigence by the Russian delegation" (30). As Russia and China are likely to continue blocking measures for safe RPO, there is little hope that such provisions will appear when the Group concludes by 2025. While active participations in the UN and other multilateral forums are necessary and attractive, the US must complement these activities with other means (31) to deal with adversaries' RPO, which can generate the rendezvous spacecraft threat.

US Responses to China's R-Spacecraft Development

Gen. John Hyten (32), former vice chairman of the Joint Chiefs of Staff and the US's second highest-ranking military officer at the time, said on the eve of his retirement in 2021 that "although we're making marginal progress, the DoD [Department of Defense] is still unbelievably bureaucratic and slow" in its response to China's rapidly advancing space weapons.

In November 2015, the US-China Economic and Security Review Commission released its annual report to Congress, stating "since 2008, China has also conducted increasingly complex tests involving spacecraft in close proximity to one another; these tests have legitimate applications for China's manned space program, but are likely also used for the development of co-orbital counterspace technologies" (33). As the Commission relied on US intelligence for this information, the Department of Defense would have known the same well before November 2015 and most likely close to 2008 when these tests were detected. Yet, US officials made few public statements about this serious threat for the ensuing decade (34). Instead, the statements about the ASAT threat largely focused on China's successful and highly visible ground-launched ASAT in 2007, while China had probably already turned to the R-spacecraft, a better stealth weapon of choice to execute a far more militarily effective 'Space Pearl Harbor' (35), the key concern raised in the 164-page report of the Rumsfeld Commission in 2001. Nonetheless, there was finally a surge of government statements between June 2018 and February 2020, in which at least 11 space officials and intelligence agencies at the highest level (including Vice President Mike Pence; Daniel Coats, director of national intelligence; Lt Gen Robert Asley, director of the Defense Intelligence Agency; and Gen. John Raymond, the first chief of space operations of the US Space Force) expressed serious concerns about this proximity (i.e., R-spacecraft) threat (36). Since then, other senior officials have followed suit with little dissension.

With this consensus of the R-threat across the Trump administration and the Biden administration, one would expect a timely and effective solution to the R-spacecraft danger. Unfortunately, the second root cause—the habit of confusing unfamiliar threat with improbable threat—are making us inefficient and inept in our preparations to counter the R-threat.

In March 2020, Brian Weeden said "in my opinion, the RPO [i.e., R-spacecraft] threat is misunderstood and overblown. It is so much more difficult technically to pull this off than most of the non-experts realize" (37). His argument was based on his talking to Northrop Grumman experts participating in the historic docking of a servicing satellite, MEV-1 with Intelsat 901 on 25 February 2020, and he said that "it was an extraordinarily complicated mission." If it were indeed such a difficult mission, his message could mean that China would take many more years for its R-spacecraft to succeed in docking and thus threaten US satellites. Yet, it took slightly less than two years for China to repeat the docking feat sometime in January 2022 (38). With so much at stake, the key question is not when China is expected to mount a space Pearl Harbor but when China has a distinct probability (i.e., far less than 50 percent) to mount it. Considering Chinese President Xi Jinping's order to accelerate the timeline for attaining the operational capability to seize Taiwan to 2027 from the previous timeline of 2035 (39), an estimate of a roughly 200 R-spacecraft ASAT capability as early as 2026, and the poor status of our preparedness against R-threat, the US should use 2026 as a reasonable and achievable target date for readiness.

Ever since 2007, if not as early as the 1980s, China has been progressing methodically and rapidly toward a bolt-out-of-the-blue attack capability.

The Trump administration reminisced the glorious first fifty years of the space age when the US dominated the space militarily and commercially. President Trump (40) envisioned that establishing the Space Force would make the US dominant in space once again and deter its adversaries from daring to cross swords with it. However, the internecine fights over how best to organise the Space Force and efforts to achieve space dominance are consuming so much financial and political capital that two of the four pillars underlying his 2018 National Space Strategy: 1) "transform to more resilient space architectures", and 2) "strengthen U.S. and allied options to deter... and counter threats" (41) are hardly getting the attention they deserve (42). In sum, the Trump administration's programme for space dominance, even if it will result in space resilience, will take at least a decade to accomplish. It will not provide adequate help to counter R-threat in the 2020s.

The Biden administration takes a dovish approach—the opposite of the hawkish one that aims at space dominance—to protect satellites. The current strategy is to replace legacy constellations (already in orbit) and their legacy-like follow-ons (already decided to be soon in orbit), which are composed of a small number of expensive large satellites with proliferated constellations of many cheap small satellites. However, a paper from the author in January 2023 has shown (43) that deployment of such proliferated constellations does not have enough time to replace many critical but vulnerable legacy constellations within this decade.

Ironically, the two administrations' approaches (hawkish or dovish) will end up with the same problem: offering a window of satellite vulnerability during this decade that encourages China to develop and mount a space Pearl Harbor as a precursor of its campaign to seize Taiwan.

Modifications to US Preparation for Countering Space Threats

Modifying Preparation for Countering R-threat: The US's readiness strategy to counter the R-threat should combine bilateral and multilateral diplomacy and its own unilateral justifiable and fair measures. The US should favour the use of the most stabilising defences at the start, followed by gradual escalations to maximise the opportunity for enemies to take off ramps and avoid further bloodshed.

The US should make the Pentagon's guidance on responsible behaviours in space (updated on 3 March 2023 (44)) transparent, observable and enforceable as soon as possible. Otherwise, China can take advantage of the lax rule to preposition, in peacetime, some or all its 200 R-spacecraft threateningly close to our critical satellites.

A stick-and-carrot approach has been proposed to induce China and Russia to join a space traffic management regime (45). They will not be allowed to participate in the lucrative Western space markets if they refuse to stay at least a short distance (e.g., 50 km at the geosynchronous orbits) away from a selected number of our critical satellites at orbits higher than the low-earth orbits. Moreover, whether or not they agree, the US will deploy small and cheap bodyguard spacecraft (46) derived from their own R-spacecraft. These spacecraft should be commanded to typically use harmless tactics to keep the invaders outside American self-defence zones—for example, catch invaders inside our zones and release them outside self-defence zones without damaging them.

Modifying Preparation to Counter Other Threats: The following principles and general measures that can be applied against most, if not all, space threats:

- Dovish (or hawkish) principles and measures are necessary, but far from sufficient alone, for effective defence. Facing a pacing challenger such as China, the US must use the strengths from both ideologies;
- Each space threat needs an individualised in-depth analysis and a tailored solution;
- Defence should be justifiable, fair, crisis-stabilising and off-ramp-feasible for the enemy;
- Quantifying input assumptions encourage constructive criticism and collaboration;
- An adversary can use lax peacetime rules in space to pre-position its ASATs for surprise attacks;
- A carrot-and-stick approach is a useful strategy to inspire an adversary's compliance;

- Heed Wohlstetter's warning of underestimating threats;
- Heed Schelling's warning of confusing unfamiliar with improbable;
- An offender has the first-mover advantage;
- Defence is only as strong as its weakest link;
- Cheap ASATs can overwhelm expensive defence.

Even special measures such as self-defence zones and bodyguard spacecraft have wide applications to counter other threats, especially those from dual-use space systems.

Conclusion

The ineffectual current course of action to counter the threat from dual-use spacecraft (R-spacecraft) capable of RPO creates a window of US vulnerability, encouraging a space Pearl Harbor sometime in the second half of 2020s. While the current US course will leave it unready, taking certain actions now can reshape preparedness. Furthermore, the principles and measures recommended for countering this threat have wide applications to other space threats as well. Increased awareness of the distinct possibility of a space Pearl Harbor will propel collaboration among interested parties to work towards global policy that will address and prevent the apocalypse lurking at the door of the free world.

Brian G. Chow *(PhD in physics, MBA with distinction, Ph.D. in finance) is an independent policy analyst.*

Endnotes

(1) Sandra Erwin, "U.S. Space Force Budget Hits $30 Billion In 2024 Proposal," *Space News,* March 13, 2023, https://spacenews.com/u-s-space-force-budget-hits-30-billion-in-2024-funding-proposal/#:~:text=Space%20Force%20budgets%20have%20steadily,to%20%2418%20billion%20in%202022.

(2) David Vergun, "China Remains 'Pacing Challenge' for US, Pentagon Press Secretary Says," US Department of Defense, November 16, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2845661/china-remains-pacing-challenge-for-us-pentagon-press-secretary-says/.

(3) Brian Weeden and Victoria Samson, editors, *Global Counterspace Capabilities: An Open Source Assessment*, Secure World Foundation, April 2023, 13-04, https://swfound.org/media/207567/swf_global_counterspace_capabilities_2023_v2.pdf#page=196.

(4) Weeden and Samson, "Global Counterspace Capabilities," 13-05.

(5) James Conca, "China Has 'First-Strike' Capability To Melt U.S. Power Grid With Electromagnetic Pulse Weapon," June 25, 2020, https://www.forbes.com/sites/jamesconca/2020/06/25/china-develops-first-strike-capability-with-electromagnetic-pulse/?sh=314ce9ce1908.

(6) Defense Intelligence Agency, *Challenges to Security in Space*, January 2019, https://media.defense.gov/2019/Feb/11/2002088710/-1/-1/1/SPACE-SECURITY-CHALLENGES.PDF#page=20.

(7) Weeden and Samson, "Global Counterspace Capabilities," 03-19.

(8) *Global Counterspace Capabilities*, 02-01 to 02-38, 08-01 to 08-05, 10-01, and 10-05.

(9) Albert Wohlstetter, "Is There a Strategic Arms Race?" *Foreign Policy*, no. 15, Summer 1974, and no. 16, Fall 1974, https://www.tandfonline.com/doi/epdf/10.1080/00396337408441511?needAccess=true.

(10) Albert Wohlstetter, "The Delicate Balance Of Terror (1958)," P-1472, Santa Monica, CA: RAND Corporation, November 6, 1958, revised December 1958, p. 184, https://npolicy.org/wp-content/uploads/2021/06/Nuclear-Heuristics-Selected-Writings-of-Albert-and-Roberta-Wohlstetter.pdf#page=196.

(11) Wohlstetter, "Delicate Balance," 184

(12) Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford University Press, 1962), vii, https://www.amazon.com/Pearl-Harbor-Decision-Roberta-Wohlstetter/dp/0804705984.

(13) Sandra Erwin, "U.S. Sharpens Plan for Military Space Race," *SpaceNews,* July 11, 2023, https://spacenews.com/u-s-sharpens-plan-for-military-space-race/.

(14) Erwin, "U.S. Sharpens Plan"

(15) Kevin Pollpeter, "China's Space Robotic Arm Programs," *SITC Bulletin Analysis*, October 2013, 3, https://escholarship.org/content/qt2js0c5r8/qt2js0c5r8_noSplash_308ba05cdedfb90ab23d648da59e3bb6.pdf#page=3.

(16) Brian Weeden, "Chinese Military and Intelligence Rendezvous and Proximity Operations," Secure World Foundation, May 2022, https://swfound.org/media/207367/swf-chinese-militarintel-rpo-may-2022.pdf.

(17) Gunter's Space Page, "BanXing 1 (BX 1), Gunter's Space Page," July 2, 2023, https://space.skyrocket.de/doc_sdat/banxing.htm.

(18) NASA, "What are SmallSats and CubeSats?" February 20, 2015, https://www.nasa.gov/content/what-are-smallsats-and-cubesats.

(19) "International Space Station," *Jonathan's Space Report* no. 683, July 30, 2013, https://planet4589.org/space/jsr/back/news.683.txt.

(20) Andrew Jones, "China's Shijian-21 Towed Dead Satellite to a High Graveyard Orbit," *SpaceNews*, January 27, 2022, https://spacenews.com/chinas-shijian-21-spacecraft-docked-with-and-towed-a-dead-satellite/.

(21) Andrew Jones, "New Chinese Small Sat Manufacturing Capacity Could Have International Ramifications," *SpaceNews*, April 6, 2022, https://spacenews.com/new-chinese-small-sat-manufacturing-capacity-could-have-international-ramifications/. Elon Musk's Starlink, Researchers Say," *SCMP*, February 24, 2023, https://www.scmp.com/news/china/article/3211438/china-aims-launch-nearly-13000-satellites-suppress-elon-musks-starlink-researchers-say.

(23) Brian G. Chow and Brandon W. Kelley, "Two Recent Wargames Hold Timely Lessons for Space Resilience," *SpaceNews*, April 7, 2023, https://spacenews.com/two-recent-wargames-hold-timely-lessons-for-space-resilience/.

(24) Permanent Mission of the People's Republic of China to the UN, "Document of the People's Republic of China Pursuant to UNGA Resolution 75/36 (2020)," April 30, 2021, http://un.china-mission.gov.cn/eng/chinaandun/disarmament_armscontrol/unga/202105/t20210501_9126875.htm#:~:text=China%20has%20actively%20participated%20in,Sustainability%20of%20Outer%20Space%20Activities.

(25) Permanent Mission of China, "Document of the People's Republic of China"

(26) U.S. Mission Geneva, "U.S. Remarks for Conference on Disarmament Subsidiary Body 3-Prevention of an Arms Race in Outer Space," https://geneva.usmission.gov/2022/03/22/cd-prevention-of-an-arms-race-in-space/.

(27) Committee on the Peaceful Uses of Outer Space, *Draft Guidelines for the Long-Term Sustainability of Outer Space Activities*, June 27, 2018, https://www.unoosa.org/res/oosadoc/data/documents/2018/aac_1052018crp/aac_1052018crp_21_0_html/AC105_2018_CRP21E.pdf#page=7.

(28) Jessica West, "The Open-Ended Working Group On Reducing Space Threats: Recap of the Third Session," *Ploughshares*, June 1, 2023, https://www.ploughshares.ca/reports/the-open-ended-working-group-on-reducing-space-threats-recap-of-the-third-session. At the end of the Summary, click "Read the full report" to see 18.

(29) West, "Open-Ended Working Group," 16

(30) Brian Weeden, "Insight – Takeaways from the UN Open-Ended Working Group On Reducing Space Threats," Secure World Foundation, October 12, 2023, https://swfound.org/news/all-news/2023/10/insight-takeaways-from-the-un-open-ended-working-group-on-reducing-space-threats.

(31) For example, means or measures based on incentives, zones, or bodyguard spacecraft are suggested in Brian Chow, “U.S. Partisan Divide Is Impairing Space Preparedness,” The National Interest, September 15, 2023, https://nationalinterest.org/feature/us-partisan-divide-impairing-space-preparedness-206805.

(32) Sandra Erwin, “Hyten Blasts ‘Unbelievably’ Slow DOD Bureaucracy as China Advances Space Weapon,” *SpaceNews*, October 28, 2021, https://spacenews.com/hyten-blasts-unbelievably-slow-dod-bureaucracy-as-china-advances-space-weapons/.

(33) U.S.-China Economic and Security Review Commission (USCC), *2015 Report to Congress of the U.S.-China Economic and Security Review Commission*, November 2015, 16, https://www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF#page=28.

(34) Brian G. Chow, “Space Traffic Management in the New Space Age,” *Strategic Studies Quarterly*, Winter 2020, Vol. 14, No. 4, 74-102, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-14_Issue-4/Chow.pdf#page=1.

(35) *Report of the Commission to Assess United States National Security Space Management and Organization*, January 11, 2001, https://aerospace.csis.org/wp-content/uploads/2018/09/RumsfeldCommission.pdf#page=19.

(36) Chow, “Space Traffic Management,” 74

(37) “Transcript of a Discussion between Dr. Brian Chow and Dr. Brian Weeden on Space Zones and Bodyguards for Proximity Operations,” moderated by Henry Sokolski and co-sponsored by the Nonproliferation Policy Education Center and the American Bar Association Standing Committee on Law and National Security in Washington DC, March 2, 2020, https://npolicy.org/article.php?aid=1465&rid=5.

(38) Public data did not indicate the precise date of docking. On the other hand, since Andrew Jones reported that Shijian-21 approached the defunct Beidou-2 G2 navigation satellite for eventual docking in late December 2021 and Brien Flewelling of ExoAnalytic Solutions said that on 22 January 2022 Shijian-21 performed a large burn taking G2 above the GEO belt, ‘sometime in January 2022’ should be a reasonable estimate for docking. (See Jones, “China’s Shijian-21”)

(39) Sam LaGrone, “Milley: China Wants Capability to Take Taiwan by 2027, Sees No Near-Term Intent to Invade,” *USNI News*, June 23, 2021, https://news.usni.org/2021/06/23/milley-china-wants-capability-to-take-taiwan-by-2027-sees-no-near-term-intent-to-invade.

(40) U.S. Space Command, “Remarks by President Trump at Event Establishing the U.S. Space Command,” August 29, 2019, https://www.spacecom.mil/Newsroom/Speeches/Speech-Display/Article/2388821/remarks-by-president-trump-at-event-establishing-the-us-space-command/.

(41) The White House, “President Donald J. Trump is Unveiling an America First National Space Strategy,” March 23, 2018, https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/.

(42) Brian G. Chow and Henry Sokolski, "Priority-One for Space Policy Should be to Protect U.S. Satellites," *SpaceNews*, October 12, 2019, https://spacenews.com/op-ed-priority-one-for-space-policy-should-be-to-protect-u-s-satellites/.

(43) Brian Chow, "The Critical Importance of Resiliency for US Missile Warning Satellites," *The Space Review*, January 3, 2023, https://www.thespacereview.com/article/4505/1.

(44) U.S. Space Command, "USSPACECOM Releases Specific Behaviors," March 3, 2023, https://www.spacecom.mil/Newsroom/News/Article-Display/Article/3318606/usspacecom-releases-specific-behaviors/; and Sandra Erwin, "DoD Releases Updated Guidance On 'Responsible Behaviors in Space'," *SpaceNews*, March 3, 2023, https://spacenews.com/dod-releases-updated-guidance-on-responsible-behaviors-in-space/.

(45) Brian G. Chow and Brandon W. Kelley, "Three Rules for Peace in Orbit in the New Space Era," *The Space Review,* February 27, 2023, https://www.thespacereview.com/article/4538/1.

(46) Brian G. Chow and Brandon W. Kelley, "Peace in the Era of Weaponized Space," *SpaceNews*, July 28, 2021, https://spacenews.com/op-ed-peace-in-the-era-of-weaponized-space/; and Chow, "Space Traffic Management," 79-80.

Decoding China’s Nuclear Modernisation

Rajeswari Pillai Rajagopalan

FOR SEVERAL DECADES AFTER CHINA went nuclear in the 1960s, Beijing was thought to have stayed with what Mao Zedong had famously said—”Six are enough”—to maintain a relatively small nuclear arsenal (1). Until recently, this was thought to number less than 300. China had also stuck to a ‘minimum deterrent’ posture, along with a no-first-use (NFU) policy. A small arsenal of under 300 nuclear weapons appeared to provide sufficient credibility to China’s stated posture. However, China now appears to be moving away from that approach; if one is to go by reports over the last few years, Beijing appears to be undertaking a significant expansion of its nuclear arsenal.

There are additional concerns that China’s expansion also indicates a possible shift in its NFU policy. The drivers of China’s nuclear expansion itself are unclear, but if it is driven by a desire to achieve some level of parity with the US and Russia, then Beijing could strive to reach parity in terms of strategy as well. This is one possible pathway, but Beijing could also take the moral high route and continue to maintain the NFU policy on paper even as it develops launch on warning capabilities. Both scenarios, with China’s giving up on its NFU or Beijing developing a launch on warning capability, make for less stable dynamics in the Indo-Pacific neighbourhood and beyond. China is essentially of the notion that “its robust nuclear weapons program is essential to counter the U.S. in the near future in order to achieve what its leaders have deemed ‘great power status’” (2). Gen. Anthony J. Cotton, head of the US Strategic Command, stated that the current expansion to achieve “quantitative and qualitative parity” with the US “already exceed those needed for its long-professed policy of 'minimum deterrence'" and China's "capabilities continue to grow at an alarming rate" (3) He also referred to the significant investment that China is making in its delivery systems and the associated infrastructure to cater to an expanding force.

A significant expansion of the kind that China has undertaken will likely have implications at multiple levels, from an arms race spiral in the Indo-Pacific to an enhanced great power competition, including in the strategic domain and its impacts on the global non-proliferation order and arms control deliberations. The US will come under enormous pressure to augment its nuclear arsenal, including the modernisation of its forces. But at the regional level, this could trigger neighbours such as India to enhance their capabilities, especially its delivery systems.

This essay scans the recent changes in China's nuclear capability, including the size of the arsenal and the improvements in the delivery systems. Given the opacity and lack of information from Chinese sources around China's nuclear weapons, the essay relies on Western sources that are considered credible, such as the *Bulletin of Atomic Scientists*. It analyses the rationale of China's nuclear expansion, including the limited debates on Beijing's true intentions. The essay concludes with an analysis of what China's nuclear expansion means for India, the broader Indo-Pacific region, and the global non-proliferation regime. At the regional level, this could kickstart a new round of proliferation, with Japan and South Korea exploring nuclear options.

Recent Developments with Regards to China's Nuclear Weapons

In a rather sudden move, China appears to be undertaking a vast nuclear expansion. There appears to be "at least three vast missile silo fields under construction near Yumen, Hami, and Ordos in north-central China" (4) The Federation of American Scientists (FAS) using satellite imagery analysis has confirmed that China's nuclear expansion is likely to at least double the size of its nuclear warhead stockpile in the coming decade (5). This is something that various US government reports and officials have said for many years. The FAS confirms that there is important progress being undertaken at the missile silo sites and a People's Liberation Army (PLA) Rocket Force training centre near Jilantai. That China has not denied these reports possibly confirms that it is on a path of expansion-cum-modernisation. The missile silo site near Yumen was revealed by the Middlebury Institute in June, which said that there are about 120 silos at the site. The second missile silo field near Hami, disclosed by the FAS in late-July 2023, has 110 silos. The third site near Ordos was disclosed by a military research unit at Air University and reportedly has about 40 silos. The *Bulletin of American Scientists* noted that each of these silo sites possibly has several nuclear-associated facilities that might be launch control centres, bases, and support facilities (6).

China's nuclear expansion seems rather sudden because even until a few years ago, its nuclear stockpile numbers appeared to be under 300. The FAS in 2019 said that China had "a stockpile of approximately 290 nuclear warheads for delivery by 180 to 190 land-based ballistic missiles, 48 sea-based ballistic missiles, and bombers" (7). The US Defense Intelligence Agency Director agreed with this assessment that China's warheads are "in the low couple hundreds" (8). According to the 2020 Nuclear Notebook, FAS had revised its estimates indicating that "China has a produced a stockpile of approximately 350 nuclear warheads, of which roughly 272 are for delivery by more than 240 operational land-based ballistic missiles, 48 sea-based ballistic missiles, and 20 nuclear gravity bombs assigned to bombers. The remaining 78 warheads are intended to arm additional land- and sea-based missiles that are in the process of being fielded." The 2020 Notebook also said that China's "stockpile is projected to increase further in the next decade" even though it would be considerably below that of both Russia and the US (9). A similar assessment in the 2023 Nuclear Notebook states that China will continue to increase, but the stockpile for 2023 "includes roughly 410 nuclear warheads with more in production" (10).

While the size of China's nuclear arsenal is significant, a more important update is that China has been undertaking important quantitative and qualitative upgradation to improve the survivability of its nuclear forces. China analysts argue that this did not mean a change as far as China's NFU policy is concerned and that it is simply a means for Beijing to have adequate "surviving forces to inflict a retaliatory second strike on its opponent" if it comes under a nuclear strike (11). This has made China focus a great deal on the delivery systems for strengthening its rudimentary nuclear triad, in particular reinforcing a weak aerial element. China nuclear watchers also argue that the sea-based nuclear force is also in a “rudimentary” stage compared to the US’s advanced sea-based capabilities (12).

Commenting on China’s land-based missiles, in March 2023, Gen. Cotton revealed to the Senate Committee on Armed Services that “the number of land-based fixed and mobile [intercontinental ballistic missile] ICBM launchers in the PRC now exceeds the number of ICBM launchers in the US” (13). He added that China “currently has an arsenal of approximately 1,000 medium- and intermediate-range ballistic missiles, many of which are dual capable (i.e., able to be armed by either conventional or nuclear warheads) and able to inflict significant damage to US, Allied, and partner forces in the Indo-Pacific.” However, FAS, which made one of the silo discoveries, suggests that there are “several unknowns” as “it is unknown how many of the new silos will be filled with missiles, how many warheads each missile will carry, and how many warheads China can actually produce over the next decade” (14). Nevertheless, Hans Kristensen of the FAS points out, “It is increasingly difficult to square this trend with China’s declared aim of having only the minimum nuclear forces needed to maintain its national security” (15).

China’s primary emphasis is on its land-based ballistic missiles although the sea-leg of the triad has become more consequential in the last few years. Until the sea leg becomes credible, China’s nuclear forces are likely to depend heavily on its land-based missiles. China will likely have a potentially credible sea-based nuclear deterrent capability too. The air-based platforms are possibly the weakest currently, but this is an area that China is expected to strengthen with a new strategic bomber that can reach the continental US.

Currently, from an Indian perspective, China’s land-based nuclear-tipped missiles are of most concern. That China has developed missiles for every possible range is alarming. It has both long-range ICBMs and intermediate-range ballistic missiles (IRBMs), which are primarily meant for regional deterrent purposes. China’s ICBM fleet includes several variations of DF-5/CSS-4 missiles, but Beijing appears to be moving to the DF-31 missiles, which have longer-range at 7,000 kms and are solid-fuelled mobile missiles, unlike the DF-5 which were liquid-fuelled and silo-based. The latter have several disadvantages in a crisis situation, such as the time taken to fuel them as well as the vulnerability of being in a fixed point. It appears that China is also deploying DF-41 missiles, which have around 12,000 km range and are rail and road mobile. However, from an Indian perspective, the earlier DF-4, the later DF-21, and the more recent DF-26 IRBMs are most concerning. The DF-21s with a range of 2,000 kms have limitations vis-a-vis India unless deployed close to the Sino-Indian border. Even if they are deployed in Delingha in Tibet, they can cover only northern India. The earlier rumours about them deployed in Delingha have not been verified. But that they are road-mobile missiles gives China options to move them fairly close to Indian territory. However, a bigger worry about the DF-21 is that it is a dual-use missile that can carry both nuclear and conventional warheads, creating problems of discrimination (16) if they are used during a conflict. The escalation dynamics are higher because it will put the Indian decision-makers, for instance, in a bind, unable to say with certainty if the incoming missiles are conventionally armed or a nuclear one. Worse, recent reports suggest that the DF-21s are now being replaced with the DF-26 IRBMs, which are also solid-fuelled and is also dual-use missiles that can carry both nuclear and conventional warheads, creating the problem of discrimination like the DF-21. The DF-26s have a range of 4,000 kms, double that of the DF-21.

As for China's sea-based deterrent capabilities, they may be considered rudimentary in relation to the US's advanced capabilities, but they could be quite effective against India. China's sea-based nuclear forces include six Jin-class Type 094 nuclear submarines equipped with long-range nuclear missiles. Each of the Jin-class submarines can carry twelve JL-2/ CSS-N-14 submarine-launched ballistic missiles (SLBMs), which have a range of 7,000 kms, adequate for targeting all of India even if they are fired from near Hainan Island, where the Jin-class submarines are deployed. But there are questions about whether the SSBNs are advanced enough and engage on deterrent patrols. Recent reports suggest that China has equipped these submarines with a longer-range JL-3 SLBM of 12,000 km, with the ability to carry multiple warheads on each mobile (17). Even though there were questions about the Jin-class SSBNs, when armed with JL-3 SLBMs, they are considered more potent from a nuclear deterrent capability perspective for India. In addition, China is planning to launch newer SSBNs, Type 096 SSBNs, which are considered to be possibly a lot quieter and more capable than the Type 094 SSBNs (18).

China’s air-based nuclear capabilities are considered to be the weakest leg of its nuclear forces. It currently has only one bomber for nuclear missions: the H-6 twin-engine subsonic long-range bomber. It has gone through several modifications and is thought to be able to carry a 1,500 km range CJ-10 cruise missile that can be equipped with a nuclear warhead. This will essentially mean that H-6 can release its payload from inside the Chinese territory, making it difficult for Indian air defence systems to intercept. Reports in recent years suggest that the H-6 is being tested with an air-launched ballistic missile called CH-AS-X-13, a version of the DF-21 ballistic missile. Therefore, for now, it appears that China will continue to keep the H-6 as the primary air-based deterrent force (19). However, China is reportedly developing new long-range bomber, the H-20, which is considered to be similar to the American B-2 stealth bomber and will have a range of 8,000 kms with a payload capacity of more than ten tons. The new bomber capability could be a more serious threat to India. However, given that it is still in the testing phase, its deployment is unlikely to happen for a decade.

Along with the changes in the traditional nuclear forces, China has also undertaken other measures to bring critical and emerging technologies into the mix. Integration of space, cyber and electronic warfare in a unified manner under the PLA Strategic Support Force (PLASSF) is a case in point. The PLASSF is a clear demonstration of how China plans to use cyber, counterspace and electronic warfare means to target an adversary’s command and control as well as logistics networks. The PLASSF brings together cyber, space, and electronic warfare scattered across different services and departments under one umbrella, making it a much more efficient system. Besides, PLA analysts argue that the establishment of the PLASSF was to bring about “new synergies between disparate capabilities that enable specific types of strategic information operations (IO) missions expected to be decisive in future wars.” Additionally, these analysts argue that “the SSF’s strategic IO role involves the coordinated employment of space, cyber, and electronic warfare to ‘paralyze the enemy’s operational system-of-systems’ and “sabotage the enemy’s war command system-of-systems’ in the initial stages of conflict” (20). That the PLASSF is directly under the Central Military Commission evidences the importance of the Force in strategic operations.

Rationale for the Changes

China for several decades maintained a minimal nuclear deterrent force level and posture, but it appears that Beijing has decided to break out and seek parity with the US and Russia. The parity that China is seeking could be in terms of both the size of its arsenal and the strategy that guides the use of nuclear weapons. Many analysts of China nuclear issues claim that Beijing is primarily focused on augmenting the survivability of its nuclear forces, enhancing the mobility of its nuclear forces, making targeting complex for adversaries, improving the nuclear-conventional flexibility, and the precision and range of its delivery systems. While it is logical for every nuclear weapon state to focus on many of these aspects, China's particular focus on developing dual-use missiles for hot swapping (21) is destabilising. This creates a discrimination challenge for those targeted, resulting in escalation possibilities in a conflict. China has also developed multiple independent re-entry vehicle capabilities for many of the newer versions of its ballistic missiles.

But there is very little known from the Chinese side about the purpose of its nuclear expansion. Kristensen and Matt Korda from the FAS point to a combination of factors that might be driving the Chinese efforts. And it is not all US-focused but also what Russia and India are possibly doing. Some of the drivers for China include its goal to maximise targeting and strike options while removing or minimising the vulnerabilities of its ICBMs to a first strike, mitigating effects of the US and partner missile defences in the Indo-Pacific, logical transition from liquid to solid-fuelled missiles, and prestige (22).

There are also a few possible internal drivers pushing China's nuclear expansion. There is a sense that it could be part of Chinese President Xi Jinping's articulation at the 20th Party Congress in October 2022 of the need to "establish a strong system of strategic deterrence, increase the proportion of new-domain forces with new combat capabilities, speed up the development of unmanned, intelligent combat capabilities, and promote coordinated development and application of the network information system" (23). Xi also paid some attention to this in his 14th Five-Year Plan for 2021-25, when he highlighted the importance of "building high-calibre strategic deterrence and joint operation systems" (24).

A critical question associated with China's nuclear expansion is about its NFU policy. With an expanded arsenal and more advanced delivery systems, there are doubts whether China will continue to adhere to the NFU policy, announced back in 1964 when it conducted its first nuclear weapon test. In the past decade, there have been some sporadic calls among Chinese strategists for revisiting its NFU policy. A Japanese media report, quoting former senior Chinese government official, said that in 2021, there was an articulation that the NFU policy "should not apply to the United States." The same media report said that in 2022, the Central Military Commission (CMC) of the Chinese Communist Party had used that report for discussions around China's nuclear expansion and modernisation. The CMC reportedly commented that "significantly increasing the number of nuclear warheads was unnecessary if the no first use policy remained unchanged" (25). These debates have gained some weight in the context of the Russian invasion of Ukraine. Reportedly, there was a report from China's National Defense University in 2022 that called for a change to the NFU policy, saying that it "would be necessary to amend" with the objective of essentially "preventing" the US and its partner countries "from intervening in the event of a Taiwan emergency" (26). This suggests that there might be some pressure internally from various quarters within China, but as yet, it does not appear that Xi is on board with those who are making a case for giving up on the NFU policy.

Implications for India and the Indo-Pacific

China has possibly undertaken the nuclear expansion and modernisation with the US in mind, but irrespective of the logic, it has created ripples among its neighbours in the Indo-Pacific neighbourhood. India has so far adopted a rather cool approach to China's nuclear expansion, without letting it trigger any debates on whether New Delhi should make an effort at catch up with China. But China's massive nuclear expansion will also likely create a strategic imbalance between China and India. While India so far has not responded to China's nuclear expansion, if the Chinese expansion continues, and the imbalance between the two grows, it will likely put much greater pressure on India too to increase its own nuclear arsenal and potentially even alter its nuclear doctrine.

While it is possible that China is responding to perceived vulnerabilities, an equally likely reason is that China is seeking parity with the US. If this is the case, then we should expect that China's nuclear expansion will be both more rapid and extensive than hitherto assumed. In other words, China may not stop at one thousand warheads but seek to build several thousands to achieve parity with the US and Russia. If China achieves such parity, this will severely constrain any American response not only at the nuclear level but also at the conventional level. China's nuclear expansion is particularly problematic because, except for India and the US, none of the other Indo-Pacific powers have a nuclear deterrent capability. China may therefore have an incentive to use its nuclear forces for compellance (refers to the use of nuclear weapons for political gains by way of coercion and/or blackmail, thus compelling an opponent to do what you want to do) rather than purely for deterrence. This will increase the insecurities of China's neighbours and could lead to renewed incentives for nuclear proliferation in the region.

In terms of other implications for the region, as the Pentagon Press Secretary Air Force Brig. Gen. Pat Ryder said at a press briefing in November 2022, "The challenge here is, the more proliferation there is, the more concerning it is, the more destabilizing to the region it is" (27). Beyond India-China dynamics, this could trigger responses from South Korea and Japan who are also concerned about developments in North Korea. There is considerable wariness and scepticism in Seoul about the US willingness to deploy nuclear weapons or come to South Korea's aid if deterrence fails vis-a-vis North Korea. This thinking leads to arguments that South Korea may need to invest in its own nuclear weapons as a reliable countermeasure against Pyongyang, although the Yoon administration is exploring other proposals as well to strengthen its deterrence, including through bringing back US tactical nuclear weapons to South Korea and exercising joint control over US nuclear weapons. Increasingly, many South Koreans see a problem with these proposals because the "ultimate authority" for use of American nuclear weapons still rests with the US president (28). Therefore, there is an incentive for South Korea to develop its own nuclear weapons, at least as far as the broader domestic sentiment is concerned. Meanwhile, Seoul plans to pursue the development of ballistic and cruise missiles, especially now that the US has removed restrictions on the payload of South Korean missiles.

There is a similar internal debate brewing in Japan (29). For Japan, both North Korea's growing nuclear and missile capabilities as well as China's strengthened military posture in the region are concerning. The regional security scenario has pushed Japan to debate the prospects of how developing a nuclear weapons programme could give it an enhanced and more credible nuclear deterrent against North Korea. Japan also believes that such capability development would also have the effect of Japan being better placed to tackle China's aggression, coercive behaviour and compellance especially as it relates to territorial disputes in the East China Sea.

All these changing deterrent dynamics could increase the pressure on the US's extended deterrence commitments in the region, though one solution might be for India to supplement the US deterrence commitments. It is extremely unlikely that India will consider such options even if it acquired such capabilities. On the other hand, India, the US, and other regional powers can consider scenarios and contingencies under which the US extended deterrence becomes more viable. Other non-regional partners such as the UK and France could also be involved in such discussions. Expanding US (and others, possibly) extended deterrence commitments to the region could provide security and greater confidence to smaller regional powers to counter any Chinese efforts at nuclear compellance.

Similarly, India, the US, and other regional partners need to explore cooperation in other military technologies that could strengthen deterrence dynamics and strengthen the Indo-Pacific peace and stability. There is also a need for India, the US, and other partners to have periodic dialogue to develop a shared understanding of red lines and escalatory thresholds, which must be publicly conveyed through joint documents/statements. These could be helpful messaging tactics that can bring about a certain amount of predictability and stability, which will have the overall effect of strengthening deterrence and escalation dynamics especially involving China. Being able to bring some element of predictability and stability are critical pieces in the context of possible future crises.

Conclusion

China's nuclear expansion and modernisation has several consequences, all of which strengthen the likelihood of instability in the Indo-Pacific. China could be undertaking the expansion and upgradation to remove perceived vulnerabilities in the US-China context, but Beijing's aggressive behaviour across the region, its embrace of critical and emerging technologies, and its disruptive uses have created enormous insecurities among its neighbours in addition to worsening the great power rivalry. China's nuclear upgradation has also the potential to push for a new wave of proliferation in the Indo-Pacific, all of which will only further weaken the global nuclear non-proliferation order.

Rajeswari (Raji) Pillai Rajagopalan *is the Director of ORF's Centre for Security, Strategy and Technology.*

Endnotes

(1) John Wilson Lewis and Xue Litai, *China's Strategic Seapower* (Palo Alto, CA: Stanford University Press, 1994), 232.

(2) "Statement of Anthony J. Cotton, Commander, United States Strategic Command Before the Senate Committee on Armed Services," March 9, 2023, https://www.armed-services.senate.gov/imo/media/doc/2023%20USSTRATCOM%20Congressional%20Posture%20Statement%20-%20SASC.pdf.

(3) "Statement of Anthony J. Cotton, Commander, United States Strategic Command"

(4) Matt Korda and Hans Kristensen, "A Closer Look at China's Missile Silo Construction," Federation of American Scientists, November 2, 2021, https://fas.org/publication/a-closer-look-at-chinas-missile-silo-construction/.

(5) "The Arms Control Landscape: Featuring DIA Lt. Gen. Robert P. Ashley, Jr. on Russian and Chinese Nuclear Weapons," Hudson Institute, May 29, 2019, https://s3.amazonaws.com/media.hudson.org/Hudson%20Transcript%20-%20The%20Arms%20Control%20Landscape.pdf.

(6) Hans M. Kristensen and Matt Korda, "China's Nuclear Missile Silo Expansion: From Minimum Deterrence to Medium Deterrence," *Bulletin of Atomic Scientists*, September 1, 2021, https://thebulletin.org/2021/09/chinas-nuclear-missile-silo-expansion-from-minimum-deterrence-to-medium-deterrence/.

(7) Hans M. Kristensen and Matt Korda, "Chinese Nuclear Forces, 2019," *Bulletin of the Atomic Scientists* 75, no. 4, 171–78 (2019), https://www.tandfonline.com/doi/full/10.1080/00963402.2019.1628511.

(8) "The Arms Control Landscape: Featuring DIA Lt. Gen. Robert P. Ashley, Jr. on Russian and Chinese Nuclear Weapons"

(9) Hans M. Kristensen and Matt Korda, "Chinese Nuclear Forces, 2020," *Bulletin of the Atomic Scientists* 76, no. 6, 443–57 (2020), https://www.tandfonline.com/doi/full/10.1080/00963402.2020.1846432.

(10) Hans M. Kristensen, Matt Korda, and Eliana Reynolds, "Chinese Nuclear Weapons, 2023," *Bulletin of the Atomic Scientists*, March 12, 2023, https://www.tandfonline.com/doi/full/10.1080/00963402.2023.2178713#:~:text=The%20Nuclear%20Notebook%20column%20has,warheads%20with%20more%20in%20production.

(11) Caitlin Talmadge, "The U.S.-China Nuclear Relationship: Growing Escalation Risks and Implications for the Future," USCC, June 7, 2021, https://www.uscc.gov/sites/default/files/2021-06/Caitlin_Talmadge_Testimony.pdf; Eric Heginbotham et al., "China's Evolving Nuclear Deterrent: Major Drivers and Issues for the United States," RAND Corporation, 2017, https://www.rand.org/pubs/research_reports/RR1628.html.

(12) China's sea-based capabilities in particular are considered "rudimentary and still evolving" because of the advanced nature of US anti-submarine warfare capabilities. See Talmadge, "The U.S.-China Nuclear Relationship: Growing Escalation Risks and Implications for the Future".

(13) "Statement Of Anthony J. Cotton, Commander, United States Strategic Command"

(14) Federation of American Scientists, "Strategic Posture Commission Report Calls for Broad Nuclear Buildup," Federation of American Scientists, https://fas.org/publication-term/china/; Kristensen, Korda, and Reynolds, "Chinese Nuclear Weapons, 2023".

(15) Stockholm International Peace Research Institute, "States Invest in Nuclear Arsenals as Geopolitical Relations Deteriorate—New SIPRI Yearbook Out Now," Stockholm International Peace Research Institute, June 12, 2023, https://sipri.org/media/press-release/2023/states-invest-nuclear-arsenals-geopolitical-relations-deteriorate-new-sipri-yearbook-out-now.

(16) With dual-use missiles or missiles that can carry both conventional and nuclear warheads, the defending side will not be able to distinguish whether the incoming missile is conventionally-armed or nuclear-armed. This could potentially lead to a nuclear response if the defending side assumed that the incoming missile is nuclear-tipped.

(17) Aadil Brar, "China's JL-3 Missile Can't Cover the US Mainland. But it Has Implications for India," *The Print*, November 21, 2022, https://theprint.in/opinion/chinas-jl-3-missile-cant-cover-the-us-mainland-but-it-has-implications-for-india/1227323/.

(18) Greg Torode and Eduardo Baptista, "Analysis: China's Intensifying Nuclear-Armed Submarine Patrols Add Complexity for U.S., Allies," *Reuters*, April 4, 2023, https://www.reuters.com/world/chinas-intensifying-nuclear-armed-submarine-patrols-add-complexity-us-allies-2023-04-04/.

(19) Greg Waldron, "H-6 Evolves from Cold War Relic to Beijing's Hammer," *FlightGlobal*, September 4, 2020, https://www.flightglobal.com/fixed-wing/h-6-evolves-from-cold-war-relic-to-beijings-hammer/140043.article.

(20) John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for A New Era," *China Strategic Perspectives* 13, Institute for National Strategic Studies, National Defense University, Washington DC, 2018, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

(21) Hot swapping refers to the capacity to change between nuclear and conventional warheads rapidly on a missile that is ready to launch. See Sky Lo, "Could China's "Hot-Swappable" Missile System Start an Accidental Nuclear War?" *Bulletin of Atomic Scientists*, April 8, 2022, https://thebulletin.org/2022/04/could-chinas-hot-swappable-missile-system-start-an-accidental-nuclear-war/#:~:text=The%20DF%2D26%2C%20which%20has,swapped%20on%20launch%2Dready%20missiles; "SECTION 2: China's Nuclear Forces: Moving Beyond A Minimal Deterrent," in *US-China Economic and Security Review Commission Annual Report 2021*, https://www.uscc.gov/sites/default/files/2021-11/2021_Annual_Report_to_Congress.pdf.

(22) Kristensen and Korda, "China's Nuclear Missile Silo Expansion: From Minimum Deterrence to Medium Deterrence," *Bulletin of Atomic Scientists*, September 1, 2021, https://thebulletin.org/2021/09/chinas-nuclear-missile-silo-expansion-from-minimum-deterrence-to-medium-deterrence/.

(23) "Transcript: President Xi Jinping's Report to China's 2022 Party Congress," October 18, 2022, https://asia.nikkei.com/Politics/China-s-party-congress/Transcript-President-Xi-Jinping-s-report-to-China-s-2022-party-congress.

(24) The National Committee of the Chinese People's Political Consultative Conference, "Xi's Two Sessions Messages Point Way for China at Historic Development Juncture," Xinhua, March 10, 2021, http://en.cppcc.gov.cn/2021-03/10/c_600432.htm.

(25) Seima Oki and Hiroshi Tajima, "Xi Facing Calls in China to Rethink "No First Use" N-Policy," *The Japan News*, March 31, 2023, https://japannews.yomiuri.co.jp/world/asia-pacific/20230331-100592/.

(26) Oki and Tajima, "Xi Facing Calls in China to Rethink "No First Use" N-Policy"

(27) "Pentagon Press Secretary Air Force Brig. Gen. Pat Ryder Holds an On-Camera Press Briefing," https://www.defense.gov/News/Transcripts/Transcript/Article/3231190/pentagon-press-secretary-air-force-brig-gen-pat-ryder-holds-an-on-camera-press/.

(28) Brad Roberts, ed., "Deterring A Nuclear-Armed North Korea," Center for Global Security Research Lawrence Livermore National Laboratory, May 2023, https://cgsr.llnl.gov/content/assets/docs/230427_CGSR_Deterring_Nuclear_Armed_North_Korea.pdf.

(29) John T. Deacon and Etel Solingen, "Japan's Nuclear Dilemmas in a Challenging New Era," East Asia Forum, June 1, 2023, https://www.eastasiaforum.org/2023/06/01/japans-nuclear-dilemmas-in-a-challenging-new-era/.

The Role of Nuclear Deterrence

Tanvi Kulkarni

MAKING PREDICTIONS ABOUT THE FUTURE OF WARFARE is a serious affair. Not because it is impossible to make true predictions about how warfare will evolve over the near to distance future, but because poor predictions can have catastrophic consequences. The twentieth and twenty-first centuries are strewn with examples of military debacles rooted in poor forecasts, including those by some of the most advanced military leaderships in the world (1). Lessons from the past can, however, inform how we approach predicting future warfare. This essay discusses two broad factors—nuclear norms and emerging technologies—in the context of the future of nuclear deterrence. It emphasises that the strength of nuclear norms and the applications of modern and emerging technologies will play a decisive role in determining how and to what extent nuclear weapons will play a role in future conflicts. Other variables—including the nuclear stockpiles, policies and postures, alliances, arms races, and prospective arms controls or risk reduction efforts—will likely affect future warfare through one or both of these broad factors. The essay also briefly discusses uncertainty as an overarching element that requires careful consideration in forecasting the future of nuclear deterrence.

The Role of Nuclear Deterrence in Warfare

Deterrence is, foremost, an 'idea.' Carl Builder wrote in 1991 that nuclear deterrence is a "...creature of the reflections and thinking of the society in which it was conceived. We are less likely to find the future of nuclear deterrence in the future of weapons technologies than in the future of our society and its thinking" (2). As an idea, therefore, the future of nuclear deterrence also lies in the future of ideas. Builder suggested that in order "to speculate on the future of nuclear deterrence, we need to look at its origins and evolution, as well as the history of the society that shaped the concept (historical progression of the idea in the society which conceived it and nurtured it" (3).

As a strategic doctrine, deterrence espouses that peace and security can be achieved by threatening potential enemies with unacceptable 'retaliatory' damage. In the golden period of European peace (1815-1914), deterrence, through rivalries and military strength, successfully avoided wars between the great powers. As a formal security concept, however, the idea of deterrence took root in Anglo-American thinking during the First World War, manifesting through Britain's strategic aerial bombardment capabilities (4). The introduction of nuclear weapons in the 1940s dramatically altered perceptions about threats and consequences in the act of conventional deterrence. A new discourse on power and security consequently emerged in international politics, framed around nuclear weapons. After the Second World War, many Western scholars predicted that future wars would be predicated on nuclear weapon prowess, and that these would be large-scale confrontations between the US and the Soviet Union, with Europe as the main theatre of conflict. Nuclear deterrence really came into play when the Soviet Union built their nuclear weapon in 1949 (5) and the US was drawn into a mutual nuclear deterrence relationship with the Soviet Union, helping spark the Cold War.

The question of mutual vulnerability spelt out the basic axioms of warfare in the nuclear age—the impossibility of defence, the vulnerability of the world's major cities and populations, the possibility of a sudden attack, and the necessity of a retaliatory capability. The introduction of the thermonuclear weapon in 1952 forced a change from nuclear war-fighting strategies to nuclear war-preventing strategies (6). With nuclear weapons, the concept of deterrence was broadened to include preventing conventional military attacks on the homeland and preventing attacks on allies (extended deterrence). Formulations like minimum nuclear deterrence, mutually assured destruction, and the flexible response became part of the strategic military doctrines of nuclear powers. These concepts altered not only the conduct of warfare but also the conduct of politics, in that decision-makers were forced to achieve political and strategic objectives during war without escalating to a nuclear war. Warfare in the nuclear age became a 'bargaining process' managed through threats rather than 'victory.'

Phases of arms races and arms controls also impacted the ability to conduct warfare in the Euro-Atlantic theatre. After the US and Soviet Union were nearly drawn into a nuclear war during the 1962 Cuban Missile Crisis, the two superpowers avoided getting into direct conventional military confrontations with each other, instead getting drawn into several crises outside Europe, particularly in Africa and Asia: most notably Vietnam (1964), Jordan (1970), the Arab-Israel War (1973), and Angola (1975). On at least two occasions during this period, there was potential for the outbreak of a nuclear crisis (7). In Vietnam, the US found itself embroiled in a protracted, draining, and humiliating war. At the turn of the century, the US launched itself into another expeditionary war in Asia, this time in Afghanistan—the longest war in US history (8) and a terrific drain on American resources and the economy (9). Although the Afghan model of unconventional warfare, featuring special operation forces and precision strikes, became arguably popular in the first decade of the twenty-first century, the war ended in a disaster for both the US and Afghanistan, with nearly 2,400 US troops and more than 46,300 Afghan civilians killed over two decades of fighting (10), and the Taliban eventually surging back to power in 2021.

Even as the threat of superpower nuclear war waned in the post-Cold War period, the number of nuclear-armed states grew. India and Pakistan's nuclear tests in 1998 added a 'nuclear dimension' to their protracted territorial conflict. In 2006, North Korea demonstrated its nuclear weapons capability, adding to the security complexities of Northeast Asia, particularly the Korean Peninsula.

Notwithstanding a historical record of the non-use of nuclear weapons since 1945, modern warfare is being imagined and conducted in the shadow of nuclear weapons and involves the risk of deliberate or inadvertent nuclear exchange. The space for conducting warfare under the nuclear level, however, depends on the actors involved and the kind of risk that is to be exploited. The situation in South Asia, for instance, is often characterised using Glenn Snyder's phrase 'the stability-instability paradox,' in which the impossibility of fighting and winning a full-scale war, given the fear of nuclear escalation, incentivises one or both states to initiate conflict in the form of limited conventional fighting, kinetic operations, or proxy and sub-conventional attacks using non-state actors. Nuclear-armed states like China and Russia are increasingly exploiting the coercive power of hybrid warfare and grey-zone tactics to their advantage in the unconventional battlefield (11). On the Korean Peninsula, too, the nuclear shadow looms large with North Korea's growing nuclear threats, demonstrated, largely since 2022, in an unprecedented increase of nuclear-capable missile tests. In the latest iteration of 'conventional warfare under the nuclear shadow,' Russia played up the nuclear threat, successfully deterring a direct NATO intervention in the Ukraine war (12).

The Strength of Nuclear Norms

The strength of nuclear norms has political and strategic import for policymaking. They affect public opinion and affect the choices that decision-makers can make, including the extent to which these weapons can be exploited in the pursuit of national interests. Over the last decade, norms that restrain the military value of nuclear weapons have been gradually and consistently weakening. Efforts toward nuclear disarmament have practically stalled, and since 2010, the nuclear non-proliferation treaty (NPT) regime has struggled to achieve consensus among states on implementing its provisions. Older frameworks of nuclear arms control between the US and Russia have broken down. Nuclear-armed states are pressing forward with the expansion and modernisation of their nuclear arsenals, revealing a new era of arms races and nuclear dangers. The war in Ukraine, for instance, is seeing a renewal of East-West conflict with ominous indicators of potential nuclear weapons use.

Five nuclear norms are likely to affect the role that nuclear weapons will play in the future of military warfare: the nuclear myth, the nuclear taboo, the norm of non-proliferation, the norm of responsible nuclear ownership, and the nuclear ban.

The nuclear myth characterises nuclear weapons as extraordinary and 'ultimate'. It strengthens nuclear deterrence, and it is, in turn, internalised through the strategies of nuclear deterrence and formalised through nuclear doctrines and postures (13). The stronger the myth grows, the more valuable nuclear deterrence becomes in the military and strategic thinking of nuclear-armed states (14). Nationalism defined in terms of nuclear power also fortifies the nuclear myth in national security discourse. The North Korean regime, for instance, defines its national power in terms of the country's nuclear capabilities, and nuclear weapons figure highly in its foreign policy discourse and domestic narratives (15). The Russian nuclear sabre rattling in Ukraine, irrespective of the plausibility of those threats, has renewed the nuclear dimension of big power competition in Europe.

The nuclear taboo, that emerged from the negative normative context in the aftermath of the atomic bombings of Hiroshima and Nagasaki (16), is arguably the strongest normative force proscribing the use of nuclear weapons in actual combat. The taboo operates in three forms: an unconditional nuclear non-use policy, the no first use (NFU) policy; and negative security assurances (non-use against non-nuclear weapons states). It has been codified through regimes like the NPT, nuclear-weapon-free zones, arms control agreements, and political declarations made by states from time-to-time in adherence to the taboo. The success of these regimes, however, largely depends on the allegiance of nuclear armed states and their commitments to uphold them. Rising military tensions, especially between the US and China in Southeast Asia and the Western Pacific and between Russia and NATO in Europe, pose serious challenges for the stability of these regimes and their normative foundations.

The NFU norm has been the weakest of the nuclear taboo. There is widespread resistance to universalising the NFU (17). China and India are the only two nuclear armed countries with a stated NFU policy. Technological acquisitions by both these states, however, has cast a considerable degree of scepticism about the validity of their NFU claims. For instance, China's advanced theatre-range nuclear weapons, the DF-26 intermediate-range ballistic missile (18), and the PLA Rocket Force's higher readiness level (19) demonstrate China's ability, if not its willingness, to threaten a first nuclear attack to deter a major conventional attack (20). Recent developments in India's nuclear weapons programme have also opened the debate about India's targeting doctrine and thereby its commitment to the NFU policy (21). There is broad agreement among experts that the NFU significantly brings down the chances of nuclear use especially if backed by legally binding commitments and supporting strategies (22). On 27 May 2021, civil society groups and policy practitioners worldwide launched a global NFU campaign, beginning with a call for the US to adopt the NFU policy. If such a campaign succeeds, nuclear deterrence could be deprioritised in future military warfare.

The Treaty on the Prohibition of Nuclear Weapons (TPNW; the nuclear ban treaty) is a step forward on legalising the nuclear taboo. Supporters of the treaty hope that it could establish a new legal norm against nuclear weapons (23). The TPNW finds its jurisprudential foundation in the 1996 International Court of Justice's Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, which envisaged a prohibition treaty to conclusively establish the illegality of nuclear weapons (24). A successful push to put nuclear weapons on the list of peremptory laws (alongside genocide, slavery, torture) would reduce the salience of nuclear deterrence in military warfare. Despite its tremendous success (25), its opposition by key NPT states limits the treaty's ability to accomplish its stated aims. The divide between the treaty's supporters and opposers has also resulted in a standoff between the NPT and the TPNW (26).

Responsibility norms or norms of responsible nuclear behaviour have not been fully settled and, therefore, what constitutes a 'responsible nuclear power' remains contested. Generally these norms lay down the expected standards for legitimate behaviour for the nuclear weapons powers (27). Nuclear powers are expected to ensure safety and security of their arsenals, minimise any nuclear arms race, promote transparency and clarity of command and control, and build cooperative frameworks to promote greater security outcomes. Worsening big power competition is, however, making it difficult to frame new nuclear arms controls and risk reduction mechanisms to replace outmoded ones. The Russian military operations around the Chernobyl reactor and Zaporizhzhia nuclear power plant, in early 2022, shows that big powers are no longer stewards of responsible behaviour. In the absence of international consensus on nuclear responsibilities and institutional frameworks (28) that enumerate this norm, nuclear threats will continue to find space in the military strategies of states.

The Applications of Technology

Technologies can, therefore, play a decisive role in defining or redefining the character of warfare. The invention of the nuclear weapon and the means to deliver it, for instance, have 'revolutionised' warfare in the last century. Every new military invention or application of technology, irrespective of its destructive potential, however, may not revolutionise warfare, even though they may modify methods or the optics of war. A technology, its application, can be deemed consequential if they alter the existing status of strategic stability (which is a combination of deterrence stability, arms race stability, and crisis stability). In the nuclear realm, emergent technologies can affect the options that states have to conduct nuclear operations, to structure their command-and-control systems, to approach crisis management and escalation control, and to engage in risk reduction, arms controls and confidence building measures. Technologies like hypersonic systems, supersonic glided vehicles, anti-satellite weapons, directed energy weapons, offensive cyber capabilities, artificial intelligence (AI) for information warfare, lethal autonomous weapon systems, and dual-use weapons systems are challenging traditional ways of thinking about escalation and stability (29) and will be most consequential for nuclear deterrence stability in future crises.

Technological applications that abet the manipulation of risks, tamper with nuclear weapons systems and their command-and-control structures, build escalatory pressures, raise risks of inadvertence and accidents, and increase the vulnerability of nuclear forces, have a destabilising effect on nuclear deterrence stability. These applications of technologies in crises and war can therefore prompt deterrence breakdown. Hypersonic weapon systems and directed energy weapons (30) significantly shrink decision-making time during crises and provoke escalation. Their 'use-it-or-lose-it' character incentivises first-mover advantage, making them very high-impact weapons. Cyber and AI applications, and intrusive digital information technologies, can be used offensively to interfere with nuclear weapons systems to constrain, confuse, or malfunction them, increasing the vulnerability of nuclear forces to preemptive, inadvertent, and accidental launches. AI-related threats are especially difficult to predict, and the fallouts of cyber operations can be very difficult to control (31).

Rapid advancements in military technologies are also a challenge to existing nuclear regimes. For instance, the NPT has struggled to keep up with the speed and spread of technological innovations in recent decades. Many non-nuclear weapon states within the NPT have now acquired relevant dual-use technologies or conventional weapons systems powered by fissile material, like the nuclear-propelled submarines (32). Traditional arms controls also risk becoming obsolete due to highly decentralised dual-use capabilities, including AI and cyber systems (33).

The stabilising effects of technological applications are, unfortunately, easily overlooked over their disruptive effects. Military technologies can have varying, sometimes even contradictory, effects on strategic stability and nuclear deterrence (34). Technological applications that are able to increase transparency and predictability, enhance escalatory firebreaks, increase survivability of nuclear forces, collect accurate information, and effectively process battlefield conditions, will have a more stabilising effect on nuclear deterrence. For instance, AI applications related to intelligence, surveillance, and reconnaissance, situational awareness, early warning, command and control, human-machine coordination, and network empowerment can help to increase the survivability of nuclear forces, collect accurate information, effectively process battlefield conditions, and enhance transparency, all of which have a relatively positive impact on strategic stability (35).

How certain military applications of technologies affect nuclear decision-making and deterrence dynamics are also determined by social and institutional contexts in which these technologies are embedded (36), the levels of technological readiness (37), increased geopolitical competition (38), attitudes of leaders (39), and the social, cultural, economic, and geopolitical contexts in which norms, policies, and regulations around applications of technologies are designed (40). Policymaking with regards to technologies is challenged by the sheer pace of innovations and advancements taking place in the private and commercial sectors, outside the direct jurisdiction of governments (41). Managing the societal, political, and normative effects of these technologies is an even bigger challenge.

Conclusion: Tackling Growing Uncertainties in Forecasting the Role of Nuclear Deterrence in Warfare

Uncertainty is an overarching element that cuts across the factors that affect the role of nuclear deterrence in the future of political and military warfare. In classical deterrence strategy, an ‘adequate’ measure of uncertainty is understood to strengthen deterrence. This premise is, however, increasingly being questioned in the face of a myriad of uncertainties in the realm of nuclear weapons. For instance, the uncertainty and ambiguity about the risks involved in certain military applications of emerging technologies makes it hard to predict their role in the nuclear sphere. These uncertainties and ambiguities add to the complexity of threat perceptions in ways that were unknown before the advent of such technologies (42). Uncertainty over the health and survival of existing nuclear regimes reduces confidence in their ability to maintain a stable global order. Uncertainty also operates at the systemic level of the global order. Uncertainty and volatility have resulted in international politics with the rapidly evolving nature of existential threats to human life and the environment. Human societies are now confronted with a matrix of anthropogenic and technological risks, including global war, nuclear holocaust, climate crisis, and infectious diseasesto name a few. Traditional notions of power, interests, and organisation in the international system are shifting with rapid changes in global geopolitics. Against the background of these uncertainties, nuclear decision-making is beset with tremendous complexities. These make it difficult to predict the future of warfare with any certainty.

More systematic approaches to international relations forecasting have to be applied to each of these factors—norms, technologies and uncertainties—to map the precise nature of their effects. More importantly, urgent action is called for to address and alter the catastrophic scenarios that such studies might forecast.

Tanvi Kulkarni *is a Policy Fellow at the Asia-Pacific Leadership Network for Nuclear Non-Proliferation and Disarmament (APLN), Seoul.*

Endnotes

(1) Cohen et al., “The Failures of Forecasting the Future,” in *The Future of Warfare in 2030: Project Overview and Conclusions*, Santa Monica, RAND Corporation, 2020, 5–10, https://www.rand.org/pubs/research_reports/RR2849z1.html

(2) Carl H. Builder, “The Future of Nuclear Deterrence,” RAND Corporation, 1991, 2, https://www.rand.org/content/dam/rand/pubs/papers/2008/P7702.pdf

(3) Builder “The Future of Nuclear Deterrence,” 1

(4) Builder “The Future of Nuclear Deterrence,” 2

(5) The use of the atomic bomb on the Japanese cities of Hiroshima and Nagasaki is typically described as an act of nuclear coercion and not an act of nuclear deterrence. From 1945 to 1949, the United States enjoyed a monopoly as the sole nuclear weapons power in the world.

(6) According to Lawrence Freedman, the United States’s imperative behind the development of the thermonuclear weapon was to keep the lead with the Soviet Union and keep the US nuclear primacy. See Lawrence Freedman, “The First Two Generations of Nuclear Strategists,” in *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, ed. Peter Parett, Gordon A. Craig, and Felix Gilbert (Princeton: Princeton University Press, 1986).

(7) In October 1969, President Nixon ordered the US Strategic Air Command nuclear forces on alert for almost two weeks during the Vietnam War. The US nuclear forces went on high alert to Defcon III level of readiness a in October 1973 in the middle of the Arab-Israel Yom Kippur War.

(8) “Remarks by President Biden on the End of the War in Afghanistan,” The White House, August 31, 2021, https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/31/remarks-by-president-biden-on-the-end-of-the-war-in-afghanistan/

(9) Anna Shortridge, “The United States Spent More Than $2.3 Trillion Dollars Trying to “Save” Afghanistan,” Council on Foreign Relations, 2021, https://www.cfr.org/blog/us-war-afghanistan-twenty-years-public-opinion-then-and-now

(10) Shortridge, “The United States Spent More Than $2.3 Trillion Dollars Trying to “Save” Afghanistan”

(11) Rebecca Hersman, “Wormhole Escalation in the New Nuclear Age,” *Texas National Security Review* (Summer 2020), 90–109, https://tnsr.org/2020/07/wormhole-escalation-in-the-new-nuclear-age/

(12) “Russia’s Lavrov Warns of ‘Real’ Danger of World War III,” *The Moscow Times,* April 25, 2022, https://www.themoscowtimes.com/2022/04/25/russias-lavrov-warns-of-real-danger-of-world-war-iii-a77486

(13) The United States and the Soviet Union played a fundamental role in the emergence, evolution and institutionalisation of this normative discourse around nuclear weapons.

(14) The discursive practice of narrating the Cold War history as a success story of nuclear deterrence only enhanced the positive normative value of nuclear weapons, and by implication also the nuclear myth.

(15) San-hoon Kim, "The Dangers of Nuclear Nationalism in DPRK," Asia-Pacific Leadership Network, 2020, https://www.apln.network/analysis/commentaries/apln-and-korea-times-essay-contest_the-dangers-of-nuclear-nationalism-in-north-korea; "The Nuclear Power of Korea is an Absolute Symbol of Peace Protection and National Revival," Rodong Sinmun, June 3, 2017, quoted in Ezra Kim, Sokchun Chang, and Hyunchul Yeo, "What Does North Korea Pursue Using Peace?—Focusing on Rodong Sinmun During the Kim Jong Un Era Of 2012–2022," *The Korean Journal of Defense Analysis* 35, no.3, (2023): 410.

(16) Richard Price and Nina Tannenwald, "Norms and Deterrence: The Nuclear and Chemical Weapons Taboo," in *The Culture of National Security*, ed. P. J. Katzenstein (Ithaca, NY and London: Cornell University Press, 1996), 114–52.

(17) Uta Zapf, "Turn Back the Doomsday Clock: Achieve No-First-Use," No First Use Global, January 16, 2022, https://nofirstuse.global/2022/01/16/turn-back-the-doomsday-clock-achieve-no-first-use/

(18) Fiona S. Cunningham, "The Unknowns About China's Nuclear Modernization Program," Arms Control Association, 2023, https://www.armscontrol.org/act/2023-06/features/unknowns-about-chinas-nuclear-modernization-program

(19) The 2021 Pentagon report to the congress on Military and Security Developments Involving the People's Republic of China notes that "nuclear and conventional PLARF brigades conduct "combat readiness duty" and "high alert duty," which apparently includes assigning a missile battalion to be ready to launch, and rotating to standby positions as much as a monthly basis for unspecified periods of time." See US Office of Secretary of Defense, "Military and Security Developments Involving the People's Republic of China," US Office of Secretary of Defense, 2021, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF

(20) Tanya Ogilvie-White, "Lessons From Asian Leadership on No-First Use," Asia-Pacific Leadership Network, January 21, 2022, https://www.apln.network/analysis/commentaries/lessons-from-asian-leadership-on-no-first-use

(21) Rajesh Rajagopalan, "India and Counterforce: A Question of Evidence," Observer Research Foundation, May 14, 2020, https://www.orfonline.org/research/india-and-counterforce-a-question-of-evidence-66126/

(22) Ogilvie-White, "Lessons from Asian Leadership on No-First Use"

(23) Nobuyasu Abe, "NPT-TPNW Standoff: Who Can Break This Gridlock?" Asia-Pacific Leadership Network, 2022, https://www.apln.network/projects/wmd-project/npt-tpnw-standoff-who-can-break-this-gridlock

(24) Kennedy Graham, "The Nuclear Weapons Prohibition Treaty: Future Prospects," Asia-Pacific Leadership Network, February 16, 2022, https://www.apln.network/analysis/commentaries/the-nuclear-weapons-prohibition-treaty-future-prospects

(25) A total of 122 states, more than three-fifths of the world's total, voted in favour of the Treaty's adoption. A total of 139 states (more than 70 percent of the global total of 197 states) are supportive of the TPNW. See Nuclear Weapons Ban Monitor, "TPNW," Nuclear Weapons Ban Monitor, https://banmonitor.org/the-tpnw

(26) John Carlson, "The Nuclear Weapon Ban Treaty is Significant but Flawed," The Lowy Institute, July 11, 2017, https://www.lowyinstitute.org/the-interpreter/nuclear-weapon-ban-treaty-significant-flawed

(27) Kate Sullivan, "Is India a Responsible Nuclear Power," Rajaratnam School of International Studies, 2014, https://www.rsis.edu.sg/rsis-publication/idss/is-india-a-responsible-nuclear/

(28) One framework that supports this norm is the non-attack agreement signed between India and Pakistan in 1988, which prohibits both states from targeting each other's nuclear power plants and other such infrastructure.

(29) Hersman, "Wormhole Escalation in the New Nuclear Age"

(30) Directed Energy Weapons can absorb a nuclear attack and degrade an adversary's command-and-control systems. They challenge the adversary's second-strike capability.

(31) Michael Onderco and Madeline Zutt, "Emerging Technology and Nuclear Security: What Does the Wisdom of the Crowd Tell Us?" *Contemporary Security Policy* 42, no. 3, 286–311, https://www.tandfonline.com/doi/pdf/10.1080/13523260.2021.1928963

(32) AUKUS, for instance.

(33) Brigitte Dekker and Maaike Okano-Heijmans, "The US–China Trade–Tech Stand-Off and the Need for EU Action On Export Control," Netherlands Institute of International Relations 'Clingendael' The Hague, 2019, https://www.clingendael.org/sites/default/files/2019-08/Report__US-China__stand-off.pdf

(34) Marina Favaro, "Emerging Technologies and Nuclear Stability," Asia-Pacific Leadership Network, July 19, 2021, https://www.apln.network/analysis/commentaries/emerging-technologies-and-nuclear-stability

(35) Cai Cuihong, "The Shaping of Strategic Stability by Artificial Intelligence" in *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Volume II East Asian Perspectives*, ed. Lora Saalman (2019), 54–77, https://www.jstor.org/stable/resrep24532.16

(36) Melvin Kranzberg, "Technology and History: "Kranzberg's Laws"," *Technology and Culture* 27, no.3 (1986): 544–60.

(37) Technology readiness level is the method for determining the maturity of a technology during the production, acquisition, deployment, and employments phases. Maturity levels are affected by technical, legal, regulatory, ethical, normative, and state-specific barriers to technology development.

(38) Paul van Hooft et al., "Shifting Sands of Strategic Stability: Towards A New Arms Control Agenda," The Hague Centre for Strategic Studies, 2022, https://hcss.nl/wp-content/uploads/2022/02/Arms-Control-Shifting-sands-of-strategic-stability-2022-HCSS.pdf

(39) Onderco and Zutt, "Emerging Technology and Nuclear Security: What Does the Wisdom of the Crowd Tell Us?"

(40) Marina Favaro et al., “Negative Multiplicity: Forecasting the Future Impact of Emerging Technologies on International Stability and Human Security,” The Institute for Peace Research and Security Policy, 2022, https://ifsh.de/file/publication/Research_Report/010/Research_Report_010.pdf

(41) Camino Kavanagh, “New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?” Carnegie Endowment for International Peace, 2019, https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736

(42) Beyza Unal et al., “Uncertainty and Complexity in Nuclear Decision-Making,” Chatham House, 2022, https://www.chathamhouse.org/sites/default/files/2022-03/2022-03-07-nuclear-decision-making-unal-et-al_1.pdf

No Domain an Island: Ground Forces Need AI in Other Domains to Succeed

Michael Depp

THE USE OF ARTIFICIAL INTELLIGENCE (AI) in warfare has gone from being a thing of the distant future to an emergent trend, thanks to recent announcements and uses on the battlefield. The increasing use of uncrewed or autonomous drones, both in the air and at sea in Ukraine, is a principal cause of this. As is the announcement by the US Department of Defense on its new Replicator initiative that hopes to quickly scale up its drone production and produce large numbers of uncrewed systems (1). Whether these efforts prove to be successes or failures, it is clear that autonomous systems will become more prevalent and more effective as time goes on. Because of this, the quality of these systems and how they are used on the battlefield will have a very significant impact on the capabilities of future military forces.

Even though there have been significant advancements in AI technology in military systems, automating ground warfare has proven particularly difficult. Most of the research progress and functional use cases have come from air and naval systems; progress that has not been matched by ground systems. What progress there is in ground applications has, so far, been more focused on the augmentation of existing processes rather than adding new capabilities. This is because autonomy in the air and sea has proven to be easier to design and more robust in tests. This state of affairs will likely remain true for some time. The ground domain has a more chaotic environment, with smaller and variable targets, and entails much more variability.

Research in air and sea systems could radically change how humans carry out their missions, or potentially even replace them completely. Tests are underway for fully autonomous aircraft, drone swarms that provide support for traditional aircraft, suicide drones in both air and sea, infantry-launched surveillance systems, and entirely uncrewed warships. Many of these are still nascent, but they are being actively considered, tested, and even used during both peacetime and wartime activities. These advances will leave an indelible mark on future ground operations. Moreover, despite these advancements occurring in entirely other domains, they will be the key to effectively using AI for success in ground operations.

The effective use of AI advancements in other domains to support ground operations will be the hallmark of victory in the future. The militaries that take advantage of the tools that air and sea platforms create to improve their position on the ground will be the ones that win. To build a force that does this well, militaries will need to apply close coordination and deeper thinking. Beginning in the conception stage, these will carry on through the procurement processes, and then find final success in the human-machine teams and the institutions that enable joint action. Due to the challenges of ground operations for AI systems, the most impactful applications of AI for those operations will come from air and naval systems. Militaries should build their autonomous systems with this in mind.

Hurdles for Effective AI on the Ground

The ground domain creates several persistent challenges for AI development. Thus far, it has proven impossible to develop an AI system that can deliver kinetic force on the ground in a way that materially improves what human soldiers can do. Much of the innovation in the ground domain is focused on smaller-scale innovation, such as optics that provide information synthesised by AI (2). But without more robust systems, AI focused solely on the ground domain will be the support, not the star of the show.

The difficulty and variability of military operations on the ground are responsible for much of this. From the mountains of Afghanistan to the Plains of Abraham, from the steppes of Mongolia to the deserts of Arabia, humans have proven that they can live and consequently fight in various environments, each with its own challenges. These different environments are also frequently visited by the same units in the same campaign. History is replete with generals like Hannibal and Bolivar who led their troops through windswept mountains, only to descend on the farmland and swamp below and fight just as effectively. Autonomous forces that accompany or constitute this force will have to be able to thrive in all potential environments as well.

To be of any serious use for militaries, autonomous ground systems will have to function in variable terrains, weather patterns, and visual environments. This will require locomotion equipped for soil, mud, snow, sand, and rock, any one of which presents a serious challenge for current forms of robotic movement, as well as sensors that can work in a range of different conditions. While there has been some good progress in this field, to replace or augment humans in a meaningful way (3), machines will not only be able to handle variable terrain but will also need to excel in it.

Setting aside the variable nature of ground operating environments, the targets in these theatres are nonetheless very different from those in the air and sea domains. In those domains, the targets that AI would be seeking out or defending are large metal objects that are not naturally found: all ships in the ocean and aircraft in the sky are man-made, not at all similar to naturally occurring features, and roughly analogous in composition. The key issue is the determination as to whether it is a legitimate and correct target. This is not the case when fighting on land.

Object detection will also be a perennial issue for these systems. Rather than identifying a single anomaly against a uniform background, these systems will have to distinguish humans from their background. This will require multiple sensor inputs on the system. Infrared sensors will be needed to distinguish humans from visually similar objects, such as rocks or plants in the dark, but visual identification through image classification will also be required because infrared alone will not be able to necessarily distinguish people from animals.

Despite these challenges, this is the area where computers have made the most progress in the past decade. What was once considered a virtually unsolvable problem has now seen great advancements that make target identification on the ground possible in many cases (4). The complicating factor for this will be whether these systems can reliably validate their targets as correct and legal in a timely fashion in a domain filled with non-combatants. As it now stands, this challenge may be difficult for humans to successfully accomplish (5). An autonomous system will not only need to identify targets, but it will also first have to confirm that these targets are legal to engage.

Humans are also much more adept at hiding and changing their appearance than machines are. For example, Paul Scharre notes the difficulty that computer vision has in detecting soldiers in a practical setting (6). In a recent test, people were asked to sneak past a system designed to find them, and no human failed to fool the AI. They quickly determined that dressing up as trees, hiding in boxes, or somersaulting past the camera would all be able to avoid machine detection. This sort of subterfuge is not as easily available to planes and ships, which present fairly uniform physical appearances. Humans, especially when their lives depend on it, are very adept at learning to exploit holes in a machine's logic, which does not bode well for our ability to rely on machines for major combat operations.

In addition to sneaking past computerised eyes, humans have other methods of avoiding detection in combat, such as deliberately disguising themselves as civilians to avoid opponents. Counterinsurgency operations frequently take place in urban environments where guerilla fighters can dress and act like civilians or allies until the moment of attack (7). Training machines to make the split-second decision between attacking a possible civilian or allowing a potential attack will be difficult and presents numerous ethical dilemmas that will only grow as militaries allow machines to make more and more decisions. These considerations alone may prevent the use of autonomous systems in many active operations (8).

As difficult as it is to find and identify lawful human targets in ground warfare, the chaotic nature of the domain may stymie machines in other ways. Unlike air and sea operations, where combat can take place when combatants are tens or even hundreds of kilometres away using missiles, in ground combat, battle often occurs at a visual distance and possibly within the physical reach of an enemy. Smoke from small arms, debris kicked up from battle, and rapid movements together make a physical fog of war that limits combatants' abilities to function effectively as a team and requires excessive training and experience to overcome. These conditions will be difficult or impossible to reliably recreate in training data. The question, therefore, is: Will militaries deploy untested technology in mission-critical areas when it may be impossible to prove a system is adequately trained first?

Progress Anywhere Means Progress Everywhere

Despite the difficulty of replacing humans on the battlefield, this does not mean that AI will be negligible in conflicts that take place on the ground. As the main theatre of all operations, AI developments in the other domains of conflict will be significant components of any ground operation, even if they are not in the domain itself. Moreover, in the air and sea, there is no shortage of near-term advances. Autonomous systems that pilot fighter jets or accompanying drones, or ones that defend capital ships from missile threats, have been tested or are already in use. These advancements will likely be boons to the air forces and navies that deploy them by making their forces more lethal and survivable, but they will also create forces that can support their comrades on the ground better than the AI systems developed for that domain alone.

Some of the greatest technological gains in autonomy have been found in the air. Uncrewed aerial vehicles have been in service in the US for decades, and by now have reached an almost global ubiquity, with Türkiye, Israel, and China producing and exporting their own systems of drones (9). With the numerous examples of success in the conflict in Ukraine, this trend is likely to accelerate further (10). For many years, the most famous of these systems were uncrewed but not autonomous, requiring an operator to remotely pilot them.

Greater autonomy is coming, however, and there have been both tests and demonstrations of systems that easily pass that bar. The concept of the loyal wingman is one such example (11). Here, each crewed aircraft would be paired with drones, either individually or, more likely, in a swarm, which would augment their existing abilities. These drones could independently target enemies, jam enemy signals, scout ahead, or provide cover. These expendable aircraft could increase a crewed fighter's lethality, survivability, and time on target. Even more advanced are tests of fully autonomous fighter aircraft, either in the form of entirely uncrewed vehicles or as a way to take some of the strain of flying from a pilot who stays in the aircraft (12).

Autonomous systems like these would dramatically improve the capabilities of aerial support for ground forces. Fully autonomous aircraft would allow militaries to support their ground forces with the most powerful aerial systems, without putting pilots who take years to train in harm's way. At the same time, because there would not be a limit to the number of these systems based on available pilots, more flights could be scheduled than ever before. Concepts such as loyal wingmen would also dramatically improve air support as pilots would have to worry less about protecting themselves, outsourcing that mission to an autonomous aide, and focusing on their primary mission. Likewise, these drones could also carry their own payloads so air support missions can stay out longer and strike more targets.

Large systems launched from operating bases several miles away from the frontline are useful, but AI will also create the ability for infantry forces to deploy smaller systems for information gathering. Systems such as Nova 2 will autonomously map a building for infantry units and give a readout of potential threats before the building is entered (13). Drones like these would allow urban forces to reduce casualties and carry out operations more quickly, acting as a force multiplier. There may come a time when units may not have to clear a building because they will know for sure if it contains enemy units and where they are.

Similarly, while they may carry smaller payloads, infantry-launched autonomous systems could play a vital role in providing cover for ground operations. Ukraine has proven a good example of the types of systems we may see in the future (14), and the US military has proposed a version specifically designed to kill tanks based on their success (15). In that conflict, we see forward-operating units deploy systems such as suicide drones that can help eliminate massed enemy forces, hard points, or vehicles, creating opportunities for those units to exploit. In Ukraine, these systems are primitive and even remotely piloted by those soldiers, but it will not be long before we see more advanced forms of automation in these systems.

Navies have long since been a tool for rich and advanced militaries to support their ground operations, but this is quickly changing. By deploying mobile air cover or bombarding the shore, warships can exert power far inland in many cases, but the trade-off is that these platforms are expensive and require sailors with years of training to work effectively. This has meant that only the richest and most advanced militaries can reap the full rewards of deploying them. Critically, defending against them has, until recently, required a navy of one's own as well.

AI may allow coastal defence forces to credibly attack navies and deny their opponents control of the sea even without their own blue-water navy to match. Ukraine, again, serves as an illustrative example, using autonomous shore-launched drone boats to attack Russian warships (16). Presently, it is unclear just how autonomous these systems are, but like those in the air domain, it seems inevitable that they will require less and less human oversight over time.

These advancements have significant value in their own domains, but many of these examples illustrate their ability to support efforts in the ground domain. Air and naval forces that are more survivable have larger and more accurate payloads and spend more time on target, which can better support units on the ground. In the face of an opponent with these capabilities but without their own to match, any future ground force will likely face an uphill battle.

However, just as ground forces unsupported by other domains will falter, so too will these other domains if they are not working to support ground forces. As T.R. Fehrenbach notes about the American experience in Korea, where a successful air war was stymied by a lack of progress on the ground, "[Y]ou may fly over a land forever; you may bomb it, atomize it, pulverize it and wipe it clean of life—but if you desire to defend it, protect it, and keep it for civilization, you must do this on the ground" (17). Focusing only on success in the air and naval domains at the expense of on the ground is a recipe for paralysis in the broader war effort. It is only through a joint effort that AI-enabled forces will truly change the battlefield.

Unity of Purpose

The most critical aspect of success in deploying AI, like so many things in the military right now, is fostering this jointness. AI systems will transform the air and sea domains far more, but their biggest successes will have to be reaped on the ground. No domain is an island unto itself; it is only by integrating disparate capabilities that future militaries see the true value of AI.

This needs to start in concept development and procurement. To be most effective with their AI innovations, militaries must conceive how their systems can work jointly with their other forces. Ideally, these capabilities should be conceived in response to an existing requirement or operational problem. Shield AI's drones are a good example. Small, infantry-launched quadcopters used to map rooms in advance of clearing emerged from examining the trials and tribulations of coalition forces in the Global War on Terror (18).

Acquiring the right new systems is not enough; it must also be matched with the ability to actually get them to the necessary units and teach them to use them. This requires both bureaucratic/logistic changes (i.e., the correct units have access to the technology when necessary) and operational ones (i.e., commanders know how to effectively use it to achieve the desired result). Even the most exquisite tools have no value unless they are wielded by someone trained in their use. Both sides of this equation, bureaucratic integration into force structures and training combatants in their use, are equally important to ensure that machines become an effective part of teams. Fostering the creation of these human-machine teams has many components that must be done correctly: from fostering trust in the humans that will use the machines (19) and designing the machines to take their human operators into account (20), to creating proper institutions within militaries to promote the use of these tools (21). Properly implemented, these can help militaries harness the full might of AI to make their units more lethal, better protected, more knowledgeable, and faster than their opponents.

The new Replicator initiative in the US military is a good showcase of the dilemma of fostering jointness in a timely manner. The programme is a big bet on AI from the US Department of Defense. Announced in August of 2023, this initiative seeks to create new autonomous systems in different domains with a focus on attritable systems in the next 18-24 months (22). The main goal is to create new mass to support the American military's deterrence efforts and to do it as quickly as possible.

However, Replicator's success will not be a function of the technology working. It is safe to say that systems like these will be up and running soon. What will make or break the US Department of Defense's efforts will be the bureaucratic enabling and the effective use of these tools that the programme produces. Will the US be able to overcome the bureaucratic hurdles in the way of developing and implementing new technologies (23)? Is there enough defence-industrial capacity to produce the kinds of attritable systems that are proposed (24)? Will planners be able to obtain and understand these tools quickly enough to use them in the near term (25)? It is on questions like these that the effective use of AI will hinge, and militaries will have to answer them correctly to be effective.

Conclusion

Just as the autonomous systems of the future have to be developed around the world, so too must the methods for using those systems. Fostering the capabilities that will be required for AI-enabled warfare will look different in each country and each service. However, the need to think through priorities from the beginning, create strong institutions, and develop training programmes will be immutable. Militaries must work to take full advantage of the many innovations in the air and sea domains, innovations that have yet to be matched on the ground. To achieve an advantage on the battlefield on the ground, those forces will have to rely on the AI capabilities of platforms in the air and at sea. AI will truly force militaries to live up to the goal of a joint force to compete.

Michael Depp *is a research associate for the AI Safety and Stability project at the Center for a New American Security (CNAS).*

Endnotes

(1) Lauren Kahn, “Scaling the Future: How Replicator Aims to Fast-Track U.S. Defense Capabilities,” War on the Rocks, September 20, 2023, https://warontherocks.com/2023/09/scaling-the-future-how-replicator-aims-to-fast-track-u-s-defense-capabilities/.

(2) David Crane, “Vortex Optics XM-157 Next Generation Squad Weapon-Fire Control (NGSW-FC): Meet the US Army’s New Game-Changing Smart Scope,” *Defense Review*, October 26, 2022, https://defensereview.com/vortex-optics-xm-157-next-generation-squad-weapon-fire-control-ngsw-fc-meet-the-us-armys-new-game-changing-smart-scope/.

(3) Tuomas Haarnoja et al., “Learning Agile Soccer Skills for a Bipedal Robot with Deep Reinforcement Learning,” ArXiv, April 26, 2023, https://arxiv.org/abs/2304.13653.

(4) Qiangchang Wang and Yilong Yin, “Recent Advances of Local Mechanisms in Computer Vision: A Survey and Outlook of Recent Work,” Arxiv, June 2, 2023, https://arxiv.org/pdf/2306.01929.pdf.

(5) David Lloyd Roberts, “Teaching the Law of Armed Conflict to Armed Forces: Personal Reflections,” *International Law Studies* 82, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1229&context=ils.

(6) Paul Scharre, *Four Battlegrounds: Power in the Age of Artificial Intelligence* (New York, NY: W.W. Norton & Co., 2023), 231.

(7) Christina Farr, *Ethics and War: When Combatants Hide among Civilians*, Washington DC, Center for International Security and Cooperation, March 14, 2011, https://cisac.fsi.stanford.edu/news/ethics_and_war_when_combatants_hide_among_civilians_20110314.

(8) Zoe Stanley-Lockman, *Responsible and Ethical Military AI*, Washington DC, Center for Security and Emerging Technology, June 9, 2023, https://cset.georgetown.edu/publication/responsible-and-ethical-military-ai/.

(9) “Who Has What: Countries with Armed Drones,” New America, https://www.newamerica.org/future-security/reports/world-drones/who-has-what-countries-with-armed-drones/.

(10) Marcel Plichta, “Ukraine Strikes Back Against Russia as World’s First Drone War Escalates,” *Atlantic Council*, August 15, 2023, https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-strikes-back-against-russia-as-worlds-first-drone-war-escalates/.

(11) Stephen Losey, “How Autonomous Wingmen Will Help Fighter Pilots in the Next War,” *Defense News*, February 22, 2022, https://www.defensenews.com/air/2022/02/13/how-autonomous-wingmen-will-help-fighter-pilots-in-the-next-war/.

(12) Tom Ward, “The US Air Force is Moving Fast on AI-Piloted Fighter Jets,” *Wired*, March 8, 2023, https://www.wired.com/story/us-air-force-skyborg-vista-ai-fighter-jets/.

(13) "Shield AI Teams with EPE to Bring Nova 2 Indoor Drone to Australia, New Zealand," *Defense Brief*, August 10, 2022, https://defbrief.com/2022/08/10/shield-ai-teams-with-epe-to-bring-nova-2-indoor-drone-to-australia-new-zealand/.

(14) Dan Peleschuk, "Ukraine Sets Up Drone Assault Units," *Reuters*, January 27, 2023, https://www.reuters.com/world/europe/ukraine-sets-up-drone-assault-units-2023-01-27/.

(15) Colin Demarest, "US Army Developing LASSO Tank-Killing Drone for Infantry," C4ISRNET, July 31, 2023, https://www.c4isrnet.com/unmanned/uas/2023/07/31/us-army-developing-lasso-tank-killing-drone-for-infantry/.

(16) "Russian Warship Damaged in Ukrainian Drone Attack," *New York Times*, August 4, 2023, https://www.nytimes.com/live/2023/08/04/world/russia-ukraine-news.

(17) T.R. Fehrenbach, *This Kind of War: A Study in Unpreparedness* (New York, NY: Bamtam Books, 1991), 290.

(18) John Spencer, "The Eight Rules of Urban Warfare and Why We Must Work to Change Them," Modern War Institute at West Point, January 12, 2021, https://mwi.westpoint.edu/the-eight-rules-of-urban-warfare-and-why-we-must-work-to-change-them/.

(19) For more discussion on the need for trust in machines and how to foster it, see Margarita Konaev and Husanjot Chahal, *Building Trust in Human-Machine Teams*, Washington DC, Brookings Institution, February 18, 2021, https://www.brookings.edu/articles/building-trust-in-human-machine-teams/.

(20) For more discussion on how to create trust in operators, see Aaron Stein, "Miscalibration of Trust in Human Machine Teaming," War on the Rocks, March 7, 2023, https://warontherocks.com/2023/03/miscalibration-of-trust-in-human-machine-teaming/.

(21) For more discussion on how institutions matter in effective use of AI, see Scharre, *Four Battlegrounds: Power in the Age of Artificial Intelligence.*

(22) Kathleen Hicks, "The Urgency to Innovate" (speech, Washington DC, August 28, 2023), https://www.defense.gov/News/Speeches/Speech/Article/3507156/deputy-secretary-of-defense-kathleen-hicks-keynote-address-the-urgency-to-innov/.

(23) Noah Spataro et al., "Winged Luddites: Aviators are the Biggest Threat to Carrier Aviation," War on the Rocks, January 10, 2022, https://warontherocks.com/2022/01/winged-luddites-aviators-are-the-biggest-threat-to-carrier-aviation/.

(24) Andrew Metrick, "For Replicator to Work, the Pentagon Needs to Directly Help with Production," Breaking Defense, September 7, 2023, https://breakingdefense.com/2023/09/for-replicator-to-work-the-pentagon-needs-to-directly-help-with-production/.

(25) Meagan Metzger, "There Isn't Just One Valley of Death: Tackling the DOD Transition Problem," *DefenseScoop*, March 1, 2023, https://defensescoop.com/2023/03/01/there-isnt-just-one-valley-of-death-tackling-the-dod-transition-problem/.

’It was an Accident’: Implications of AI on the Ability to Distinguish Between ‘True’ Accidents and Violations of International Humanitarian Law

Laura Bruun

AS WORLD GOVERNMENTS’ INTEREST IN MILITARY artificial intelligence (AI) increases, the importance of clarifying how AI can—or cannot—be used lawfully in targeting decisions becomes more relevant than ever. Here, one important (but relatively overlooked issue) pertains to how international humanitarian law (IHL) regulates unintentional incidents involving the use of AI, because while the famous fog of war described by Carl von Clausewitz 200 years ago (1) does not seem to be lifting from the battleground any time soon, some argue that increased reliance on AI may add new layers to the fog.

Thus, flowing from concerns around increased unpredictability associated with AI, a deeper understanding of the risks—and how IHL regulates these—is critical to ensure legal compliance and human accountability in future and potentially more AI-reliant warfare. To promote such a better understanding, this essay outlines some of the challenges and potential solutions to ensure the ability to distinguish a tragic, but not unlawful, accident from a breach of IHL. The essay is largely informed by the research on autonomous weapon systems (AWS) and IHL conducted by the Stockholm International Peace Research Institute (SIPRI).

Was it an Accident or Violation? Existing Norms and Challenges

One of the only constants in warfare, today and throughout history, is perhaps that few things go exactly as planned. Regardless of how well-intended militaries may be or how advanced their technology is, unexpected changes in the environment, miscommunication, or technical glitches are among the many factors that can lead to unintended, potentially harmful, incidents. While such incidents are regrettable, they are not considered unlawful per se. The US drone strike in July 2021 in Kabul that accidentally killed 10 civilians is an example of such. Whilst debated, the incident was, according to the Pentagon, not a violation but rather a ‘tragic mistake’ due to different factors, including “a breakdown in process” (2). Therefore, before diving into the specific challenges related to AI, it is important to first clarify the delicate (and oft-debated) relationship between ‘true’ accidents and IHL violations.

The starting point for both ‘true’ accidents and IHL violations is likely to be the occurrence of an unintended, possibly harmful incident. Unintended harmful incidents are the overarching term we can use to describe situations where harm inadvertently is inflicted against combatants, civilians, and/or civilian objects during an armed conflict. Then, if the harmful incident could not have been reasonably foreseen or prevented, it would likely be labelled as a ‘true’ accident, which does not automatically constitute a violation of IHL. On the other hand, if the harmful incident resulted from a foreseeable or known risk that was not prevented, mitigated, or proportionate with the concrete and direct military advantage anticipated, it could amount to a violation of IHL.

However, distinguishing between ‘true’ accidents and IHL violations is easier said than done. Because here, the violation we are looking for will likely not manifest in certain conduct (such as a commander intentionally directing an attack against civilians) but rather in the absence of certain conduct or care (such as a failure to take all feasible precautions) (3). Thus, we are dealing with the establishment of a positive obligation under IHL. Positive obligations under IHL are especially relevant in relation to states who, unlike individuals, are not only responsible for respecting IHL but also for ensuring respect and thus account for the collective and systemic nature of IHL implementation (4). The difficulty in distinguishing 'true' accidents from violations of positive IHL obligations stems from the fact that many of these obligations feature open-textured language (5). Take, for example, the principle of precautions in attack, which requires parties to a conflict to take 'constant care' to spare civilians in military operations and to take all feasible precautions in attacks (6). While this obligation is considered critical to ensure compliance with IHL, establishing whether it has been breached can be difficult because the assessment is largely based on non-explicit international standards of behaviour (7).

Existing challenges around distinguishing accidents from IHL breaches arguably become more evident than ever in light of the recent developments in, and the implementation of, AI in the military. Why that is so and how to address this challenge will be explored in the following sections.

Military AI and the Increased Risk of Unintended Harm

Throughout history, technological developments have driven how wars have been fought. The steamship enabled naval warfare, railroads facilitated faster deployment of troops and equipment, and the telegraph completely transformed communication between field commanders and national authorities. Now, in light of the recent and rapid developments in the field of AI, it is expected that this technology will revolutionise the way warring parties make targeting decisions in future warfare.

Military applications of AI can be (and already is) implemented for several different purposes, such as intelligence, mobility, interoperability, and targeting (8). The most debated type of application is perhaps AI for targeting, i.e. when AI is used to inform the identification, selection, and even engagement of targets. A concrete example of the latter is the case of AWS, which is likely but not necessarily enabled by AI. Though there is no internationally agreed definition of AWS (yet), they generally refer to weapon systems that "once activated can select and engage targets without further human intervention" (9). AWS can come in many shapes and forms but share some distinctive socio-technical features. For example, AWS functions based on pre-programmed target profiles and technical indicators that AWS can recognise through their sensors and software. Also, since AWS is triggered to apply force partly by their environment of use (rather than a user's input), aspects of a decision to apply force can be made further in advance than with traditional weapons based on assumptions about the circumstances that will prevail at the time of the attack (10).

While AI has been used in different military functions for decades, recent developments (and significant investments) suggest that this technology will play a central role in modern warfare, not least when it comes to targeting decisions. Already now, we see a growing number of reports, including from Nagorno-Karabakh, Ukraine, and Gaza, about how AI is being used to identify, select and recommend targets (11). While the extent to which AI is also used to engage targets—i.e. amounting to an AWS—is more unclear, there are reports of such, including a UN report on Libya in 2021 (12). According to several big military nations, spanning from the US and Israel to Russia and Japan, the use of AI in the military contains the potential to provide better protection to civilians and combatants through faster and more accurate targeting than traditional types of weapons (13).

Besides potential benefits, the use of AI for targeting, however, also introduces new sources of risks that may inflict unintended harm or injury to protected individuals and objects. SIPRI's research indicates that harmful incidents involving AWS are increasingly likely to flow from unintended consequences caused by, for example, a technical failure or unexpected interaction with the environment rather than wilful decisions on the part of military decision-makers (14). This finding supports several scholars and experts who have argued that using military AI opens up new sources of risks, which may result in increased risk of unintended harm to civilians (15). These sources of risks, associated with the use of AI in targeting decisions that can cause unintended harm, can broadly speaking be divided into three categories:

- **Unintentional harm caused by the system** (Examples: data or software errors; malfunctions; technical glitches);
- **Unintentional harm caused by the users** (Examples: lack of care in planning and programming; user failure to operate the system with sufficient understanding and knowledge about the system behaviour and effects); and

- **Unintentional harm caused by external factors** (Examples: Adversarial interference and hacking; type of environment not accounted for in testing; unforeseen changes in the environment of use after activation)

Many of these risks are, of course, also present in the context of traditional weapons. However, the concern is that AI, due to increased technical complexity and unpredictability, is more vulnerable to these risks (16). A central rationale behind this argument flows from the fact that when activating, for example, an AWS, the user does not necessarily know the exact location, timing and/or circumstances around the application of force, and is thus likely to offer less foreseeability around the effects of the use of force (17). Besides general worries around the risk of inflicting unintended harm to civilians and civilian objects, additional concerns are also raised that the increased unpredictability will make it harder to establish when a harmful incident is no longer an accident but actually a violation, and thus to ensure accountability in case of a breach. To ensure compliance with IHL, notably positive obligations to ensure respect, a deeper understanding is needed of how much certainty about the effects of force IHL demands and how much risk-taking it permits.

A Gap in the Policy Debate

Despite its importance, the issue of unintended harm involving AI has not been addressed in depth in the international policy debate. A good example is within the Convention on Certain Conventional Weapons (CCW) where states for more than ten years have discussed how to ensure the lawful use of AWS. Here, compared to the attention given to, for example, the risk of intentional misuse or individual responsibility for war crimes, the risk of unintended harm and its legal consequences has received little in-depth attention. While states generally seem to agree that unintended incidents involving AWS are not IHL violations if they are the consequence of 'unwilful' and 'unforeseeable' errors or external interference, is unclear what situations this term covers and whether they are a violation of IHL or not (18). To support a deeper and more structured discussion on this issue, the following section will present and discuss some of the challenges and potential solutions.

Discerning Accidents from Violations Involving AI: Challenges and Ways Forward

To minimise the risk of unintended harm involving the use of AI—and to ensure the ability to assign responsibility in case of a breach—both legal and practical aspects must be tackled. Specifically, a critical starting point is to get a deeper understanding of the types of unintentional incidents involving AI that amount (or should amount) to a violation of IHL (legal clarification) and how to practically discern accidents from violations involving AWS (practical clarification).

Identifying types of unintentional incidents involving AI that amount to violations of IHL

To strengthen the ability to distinguish IHL violations from accidents involving AI, a critical first step is to systematically map and describe the different types of incidents that may occur and assess which of these should be considered a violation. This is important because when states, notably in the CCW, have described the types of incidents involving AWS that should not be considered IHL violations, they have referred to several distinct terms, such as 'unintended engagements', 'accidents', 'malfunctions', 'failures', 'mistakes', and 'technical errors'. However, these terms have not been addressed systematically and it is unclear whether these terms—and the kinds of incidents to which they refer—are congruent (19). To support structured discussions on this topic, the following outlines and discusses state views considering the three types of harm described above.

Harmful incidents caused by the system : An examination of views expressed in the CCW indicates initial agreement that harmful incidents flowing from technical errors should generally not be considered a violation. For example, the US expressed in 2021 that "unintended harm to civilians and other persons protected by IHL from accidents or equipment malfunctions, including those involving emerging technologies in the area of LAWS, is not a violation of IHL as such" (20). However, according to a statement from Switzerland tracing back to 2017, it is argued that "States remain legally responsible for unlawful acts and resulting harm caused by autonomous weapon systems they employ, including due to malfunction or other undesired or unexpected outcomes" (21). While these two statements suggest disagreement around responsibility for malfunctions, their dating also indicates that states have not addressed this question in recent years. Going forward, it would, therefore, be helpful for states to articulate their views on this specific aspect. Here, it would be particularly relevant to address the extent to which—and in what circumstances—unintended (but perhaps foreseeable) incidents caused by glitches, malfunctions, and bugs of increasingly complex systems can continue to be considered 'true accidents'.

Harmful incidents caused by the users: An examination of views expressed in the CCW indicates that whether harmful incidents caused by users amount to an IHL violation or not is perhaps the most contested. To get a better understanding of this question, it is first important to distinguish between individual criminal responsibility for a harmful incident caused by the users and state responsibility for harmful incidents caused by the users. This is because there are different legal standards, and obligations, applying to individuals and states.

First, under IHL, individuals can only be held criminally responsible for grave breaches of IHL, such as violations of the principles of distinction and proportionality (22). However, to assign individual criminal responsibility for a grave breach, it is not enough to establish the unlawful act (i.e. proving that the person either committed, contributed to, ordered or failed to prevent an unlawful attack), but also that the individual did so 'wilfully' (23). According to the International Committee of the Red Cross, this mental element means that the perpetrator 'must have acted consciously and with intent' (24). However, the degree of intent needed to establish individual criminal responsibility for a grave breach is debated and, for example, concerns whether recklessness or negligence about the effects of an attack amounts to a war crime or not (25). While this debate predates AI, the existing unclarity regarding the criminalisation of risk-taking behaviours and types of carelessness has become increasingly relevant in the context of AI. For example, in the case of AWS, where users, upon activation, do not necessarily know the exact timing or location of the application of force, it becomes ever more important to clarify what individuals are required to know and foresee to comply with the principles of distinction and proportionality (26). Thus, to establish whether an unintended incident caused by a user amounts to an IHL violation, a deeper understanding is needed of what such users are required to know and foresee to exercise their obligations under IHL.

In contrast to individual criminal responsibility, state responsibility is broader in its scope and application. In short, states are responsible for complying with the entire body of IHL (not just grave breaches) and establishing state responsibility does not require proving the same degree of intentionality. Thus, to assess whether an unintended incident caused by the users could trigger state responsibility, it becomes relevant to consider the content of states' obligations to ensure respect for IHL and whether these have been fulfilled or not. For example, to ensure respect for IHL, states are required to disseminate IHL 'as widely as possible' to its armed forces, which includes integrating it into military instruction (27). If it can be established that an unintended incident caused by the users can be traced back to insufficient training, the incident may trigger the state's responsibility. However, with that, we reopen existing debates of what requirements flow from such relatively open-textured obligations. While IHL, for example, does not appear to require specific military training for specific weapons, this is argued to be an implicit requirement flowing from obligations to 'ensure respect' and 'take all feasible precautions' (28). Therefore, whether an unintended incident resulted from the users' lack of sufficient training or knowledge amounts to a breach of a state's positive obligations to ensure respect, remains an interpretative question. Though this is a challenge that also predates AI, it would be helpful if states could deepen their (common) understanding of what compliance with positive obligations entails in the specific context of AI, for example, in terms of standards of training and levels of technical knowledge that are required of those planning or deciding upon attacks (29).

Harmful incidents caused by external factors: Harmful incidents caused by external factors, such as hacking or adversarial interference, do not appear to be considered IHL violations per se among state representatives consulted by SIPRI. This is, however, on the condition that the party to the conflict in question satisfied their obligations to take constant care in the military operation to comply with IHL (30). With that said, an additional element must be considered in states' deliberations. In the specific context of AWS, for example, several experts have warned that AWS are more prone to hacking, enemy behavioural manipulation, and other unexpected interactions with the environment—i.e., external factors that may result in harmful incidents (31). If that should be the case, states should specifically address to what extent that would impact compliance with their obligation to take all feasible precautions in the choice of means and methods of warfare. Finally, it should be mentioned that some legal experts have argued that the inherently unpredictable nature of AWS—and the corresponding risks associated with their use—demand that states should be subject to a strict liability regime (32). This means that a state would be responsible for all types of incidents involving an AWS, no matter the underlying cause or intent. However, as of now, this remains a suggestion mainly articulated by legal scholars and in the specific context of AWS.

Discerning accidents from IHL violations involving AI

Once states have agreed on the types of harmful incidents that constitute an IHL violation, it becomes equally important to ensure the practical ability to trace back and recognise such (33). While this is also true for incidents not involving AI, this task may become more important (and tricky) in the context of AI (34). To this end, SIPRI's research has identified at least two aspects that would constitute useful starting points to ensure the ability to separate IHL violations from accidents involving AI:

Deepen the technical understanding of the characteristics of respectively accidents and IHL violations involving AI

To discern accidents from violations involving AI, it is important to understand what the characteristics of respectively a 'true' accident and a violation are. What is, for example, from a technical perspective, the difference between a mistake, a malfunction, a system error, or a user error and how would they manifest in the specific context of AI? Efforts to deepen the technical understanding of the characteristics of respectively accidents and IHL violations involving AI can be implemented both during the development, use and post-use phases.

First, in the development phase, developers could, through rigorous testing, evaluation and verification, map and describe the potential failures that the use of the system could lead to. In that way, it would be easier to assess later whether the risk was foreseen or not, and thereby the extent to which it was a 'true accident' or not.

Second, during development and use, the establishment of reporting mechanisms and transparency requirements around the technical behaviour and performance of the systems would be useful. Here, states could take inspiration from the AI Act (35). The AI Act, which is the European Union's forthcoming (and first-of-its-kind) regulation on civilian and dual-use AI systems, is expected to impose reporting and transparency requirements around malfunctions, system behaviour, and so on, when developing and using 'high-risk' AI systems. Thus, if applied to military AI, this would promote a deeper common understanding among developers of how a certain malfunction, technical error, and the like, may materialise in a specific system. This type of documentation would be valuable when potentially assessing whether an unintended incident was foreseeable or not.

Finally, in case of a harmful incident, states could implement (or strengthen if already in place) technical investigations to inquire into unintended incidents. Such investigations, for example, known as safety investigations in the US military, could provide a useful avenue to increase the technical understanding of how different accidents, mistakes, technical errors etc. materialise in the use of AI as well as what their respective characteristics would be (36).

Strengthen the ability to investigate systemic violations of IHL

Finally, to distinguish a 'true accident' from an IHL violation in the context of AI, it is important to have strong mechanisms in place to investigate and identify potential underlying structures causing harm, potentially indicating a state's failure to ensure respect for IHL (imagine situations of poor training of armed forces, insufficient testing or overreliance on certain data). To this end, so-called administrative investigations become particularly relevant. Unlike criminal investigations that mainly inquire into potential grave breaches amounting to war crimes, administrative investigations serve to establish the facts around an incident and inquire into a broader set of potential breaches. This broader scope allows investigators to inquire into underlying systemic issues that may not amount to a serious violation of IHL but still inflict harm that may be attributable to the state.

The Need to Clarify States' Obligations to 'Ensure Respect' for IHL in the Context of AI

One of the biggest challenges associated with the use of military AI pertains to an increased risk of unintended incidents. Besides the harmful consequences these may have, additional concerns are raised because of the lack of clarity around how IHL regulates such unintended incidents. Indeed, the unpredictability associated with the use of AI brings back to life debates about how much risk parties to a conflict may lawfully assume while still satisfying core obligations to 'ensure respect' for IHL and take constant care in military operations. Therefore, to distinguish so-called 'true' accidents from violations of IHL involving AI, a critical first step is to clarify the content of states' positive obligations to 'ensure respect' for IHL in the context of AI. Such a deeper understanding will make it easier to spot when an absence of certain conduct or care may amount to systemic (albeit unintentional) violation of IHL attributable to the state.

Laura Bruun *is a Researcher within the Governance of AI programme at the Stockholm International Peace Research Institute.*

Endnotes

(1) Carl von Clausewitz, *On War* (Princeton: University of Princeton Press, 1830).

(2) Eric Schmitt, "No U.S. Troops Will Be Punished for Deadly Kabul Strike, Pentagon Chief Decides," *The New York Times,* December 13, 2021, https://www.nytimes.com/2021/12/13/us/politics/afghanistan-drone-strike.html.

(3) Prohibited as a negative obligation under IHL as the principle of distinction: Additional Protocol to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 (hereafter 'AP I'), Arts 48, 51(2), 51(4), and 51(5); International Committee of the Red Cross (ICRC), Customary IHL Database (hereafter 'CIHL Database'), rules 1, 7 and 13; The obligation to take feasible precautions: AP I, Art. 57(1); CIHL Database, Rules 15, 16, 17, 18 and 19.

(4) "Geneva Convention (I) on Wounded and Sick in Armed Forces in the Field," August 12, 1949, https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-1.

(5) Marta Bo, Laura Bruun, and Vincent Boulanin, "Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems: On Accountability for Violations of International Humanitarian Law Involving AWS," Stockholm International Peace Research Institute, 2022, https://www.sipri.org/sites/default/files/2022-10/2210_aws_human_responsibility.pdf.

(6) AP I, Art. 57(1); CIHL Database, Rules 15, 16, 17, 18 and 19.

(7) Marco Longobardo, "The Relevance of the Concept of Due Diligence for International Humanitarian Law," *Wisconsin International Law Journal* 37, no. 1 (2019): 183–84, https://wilj.law.wisc.edu/wp-content/uploads/sites/1270/2020/07/37.1_44-87_Longobardo.pdf.

(8) Vincent Boulanin and Maaike Verbruggen, "Mapping the Development of Autonomy in Weapon Systems," Stockholm International Peace Research Institute, November 2017, https://www.sipri.org/sites/default/files/2017-11/siprireport_mapping_the_development_of_autonomy_in_weapon_systems_1117_1.pdf; Vincent Boulanin et al., "Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control," Stockholm International Peace Research Institute and International Committee of the Red Cross, June 2020, https://www.sipri.org/sites/default/files/2020-06/2006_limits_of_autonomy.pdf.

(9) Boulanin and Verbruggen, "Mapping the Development of Autonomy in Weapon Systems"; Boulanin et al., "Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control"

(10) Laura Bruun, Marta Bo, and Netta Goussac, "Compliance with International Humanitarian Law in the Development and Use of Autonomous Weapon Systems: What Does IHL Permit, Prohibit and Require?" Stockholm International Peace Research Institute, March 2023, https://www.sipri.org/sites/default/files/2023-03/ihl_and_aws.pdf.

(11) Robert Marks, "The First War Using Modern AI-Based Weapon is Here," Mind Matters, October 15, 2020, https://mindmatters.ai/2020/10/the-first-war-using-modern-ai-

based-weapons-is-here/; Samuel Bendett, "Role and Implications of AI in the Russian-Ukraine Conflict," Center for a New American Study, July 20, 2023, https://www.cnas.org/publications/commentary/roles-and-implications-of-ai-in-the-russian-ukrainian-conflict; Israeli Defense Forces, "A Glimpse of the IDF's Target Factory that Operates Around the Clock," *IDF*, November 2, 2023, https://www.idf.il/אתרי-יחידות/יומן-
סיה-ליח-ריוואה-ליח-ןיעידומה-ףגא-ל-הצ-תוחוב-ופקתוהש-תורטמ-המחלמ/תוצפה/תובתכה-לכ/המחלמה/.

(12) The 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, https://www.npr.org/2021/06/01/1002196245/a-u-n-report-suggests-libya-saw-the-first-battlefield-killing-by-an-autonomous-d.

(13) United States Mission to the United Nations, "U.S. Commentaries on the Guiding Principles," September 2020, https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2020/gge/documents/US_2020.pdf; Permanent Mission of Israel to the United Nations, "Israel Considerations on the Operationalization of the Eleven Guiding Principles Adopted by the Group of Governmental Experts," August 31, 2020, https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2020/gge/documents/Israel_2020.pdf; Permanent Mission of Russia to the United Nations, "Application of International Humanitarian Law to Lethal Autonomous Weapon Systems (LAWS)," 2022, https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2022/gge/documents/Russia_July2022.pdf; Permanent Mission of Japan to the United Nations, "Draft Elements on Possible Consensus Recommendations in Relation to the Clarification, Consideration and Development of Aspects of the Normative and Operational Framework on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems," 2021, https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2021/gge/documents/Japan_sept.pdf.

(14) Bo, Bruun, and Boulanin, "Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems"

(15) Paul Scharre, "Autonomous Weapons and Operational Risk," Center for a New American Security, 2016, https://www.cnas.org/publications/reports/autonomous-weapons-and-operational-risk; Rebecca Crootof, "War Torts," *New York University Law Review* 97 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4040075; Robin Geiss, "State Control Over the Use of Autonomous Weapon Systems: Risk Management and State Responsibility," in *Military Operations and the Notion of Control Under International Law*, ed. Rogier Bartels et al. (The Hague: T.M.C. Asser Press, 2021), https://www.springerprofessional.de/en/state-control-over-the-use-of-autonomous-weapon-systems-risk-man/18258332; Kelsey Atherton, "Understanding the Errors Introduced by Military AI Applications," Brookings, May 6, 2022, https://www.brookings.edu/articles/understanding-the-errors-introduced-by-military-ai-applications/; Afonso Seixas-Nunes, "Autonomous Weapons Systems and the Procedural Accountability Gap," *Brooklyn Journal of International Law* 46, no. 2 (2021), https://brooklynworks.brooklaw.edu/bjil/vol46/iss2/3/; International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (Geneva, 2019), 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.

(16) Crootof, “War Torts”; Scharre, “Autonomous Weapons and Operational Risk”; Tsvetelina Benthem, “Exploring Changing Battlefields: Autonomous Weapons, Unintended Engagements and the Law of Armed Conflict,” in *14th International Conference on Cyber Conflict: Keep Moving*, ed. Taťána Jančárková and Gábor Visky (2022), https://ccdcoe.org/uploads/2022/06/CyCon_2022_book.pdf.

(17) Bruun, Bo, and Goussac, “Compliance with International Humanitarian Law in the Development and Use of Autonomous Weapon Systems”

(18) Bruun, Bo, and Goussac, “Compliance with International Humanitarian Law in the Development and Use of Autonomous Weapon Systems”

(19) Bruun, Bo, and Goussac, “Compliance with International Humanitarian Law in the Development and Use of Autonomous Weapon Systems”

(20) United States Mission to the United Nations, “US Proposals on Aspects of the Normative and Operational Framework,” CCW/GGE.1/2021/WP.3, September 27, 2021, https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2021/gge/documents/US-1.pdf.

(21) Permanent Mission of Switzerland to the United Nations, “A ‘Compliance-Based’ Approach to Autonomous Weapon Systems,” CCW/GGE.1/2017/WP.9, 10 Nov. 2017, p. 6, https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2017/gge/documents/WP9.pdf.

(22) The definition of a grave breach is found in the four Geneva Conventions (GC) and Additional Protocols: GC I, Art. 50; GC II, Art. 51; GC III, Art. 130; GC IV, Art. 147; and AP I, Art. 11.

(23) AP I Art 85(3).

(24) International Committee of the Red Cross, “Commentary to the Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I),” June 8, 1977, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-85/commentary/1987?activeTab=undefined.

(25) Bo, Bruun, and Boulanin, “Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems”

(26) Bo, Bruun, and Boulanin, “Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems”

(27) GC I, Art. 47; GC II II, Art. 48; GC III, Art. 127; GC IV, Art. 44; AP I, Art. 83; CIHL Database, Rule 142.

(28) Elizabeth Stubbins Bates, “Towards Effective Military Training in International Humanitarian Law,” *International Review of the Red Cross* (2014), https://international-review.icrc.org/sites/default/files/irrc-895_896-bates.pdf; Bo, Bruun, and Boulanin, “Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems”

(29) Bo, Bruun, and Boulanin, “Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems”

(30) Bo, Bruun, and Boulanin, “Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems”

(31) Crootof, "War Torts"; Scharre, "Autonomous Weapons and Operational Risk"

(32) Rebecca Crootof, "War Torts: Accountability for Autonomous Weapons," *University of Pennsylvania Law Review* 164, no. 6 (May 2016), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9528&context=penn__law__review&httpsredir=1&referer=; Elizabeth Fuzaylova, "War Torts, Autonomous Weapon Systems, and Liability: Why a Limited Strict Liability Tort Regime Should Be Implemented," *Cardozo Law Review* 40, no. 3 (2019), http://cardozolawreview.com/wp-content/uploads/2019/03/40.3.9.Fuzaylova..pdf.

(33) Bo, Bruun, and Boulanin, "Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems"; Arthur Holland Michel, "Known Unknowns: Data Issues and Military Autonomous Systems," United Nations Institute for Disarmament Research, 2021, https://unidir.org/sites/default/files/2021-05/Holland__KnownUnknowns__20210517__0.pdf.

(34) Benthem, "Exploring Changing Battlefields"; Bo, Bruun, and Boulanin, "Retaining Human Responsibility in the Development and Use of Autonomous Weapon Systems"

(35) European Commission, *Regulation Of The European Parliament And Of The Council: Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, Brussels, 2021, https://artificialintelligenceact.eu/the-act/.

(36) US Air Combat Command, "Air Force Safety and Accident Board investigations," January 25, 2019, https://www.acc.af.mil/Portals/92/Docs/Fact%20Sheets%20-%202020%20Update/SafetyAccidentBoardInvestigation_Formatted.pdf?ver=2020-06-23-093803-637.