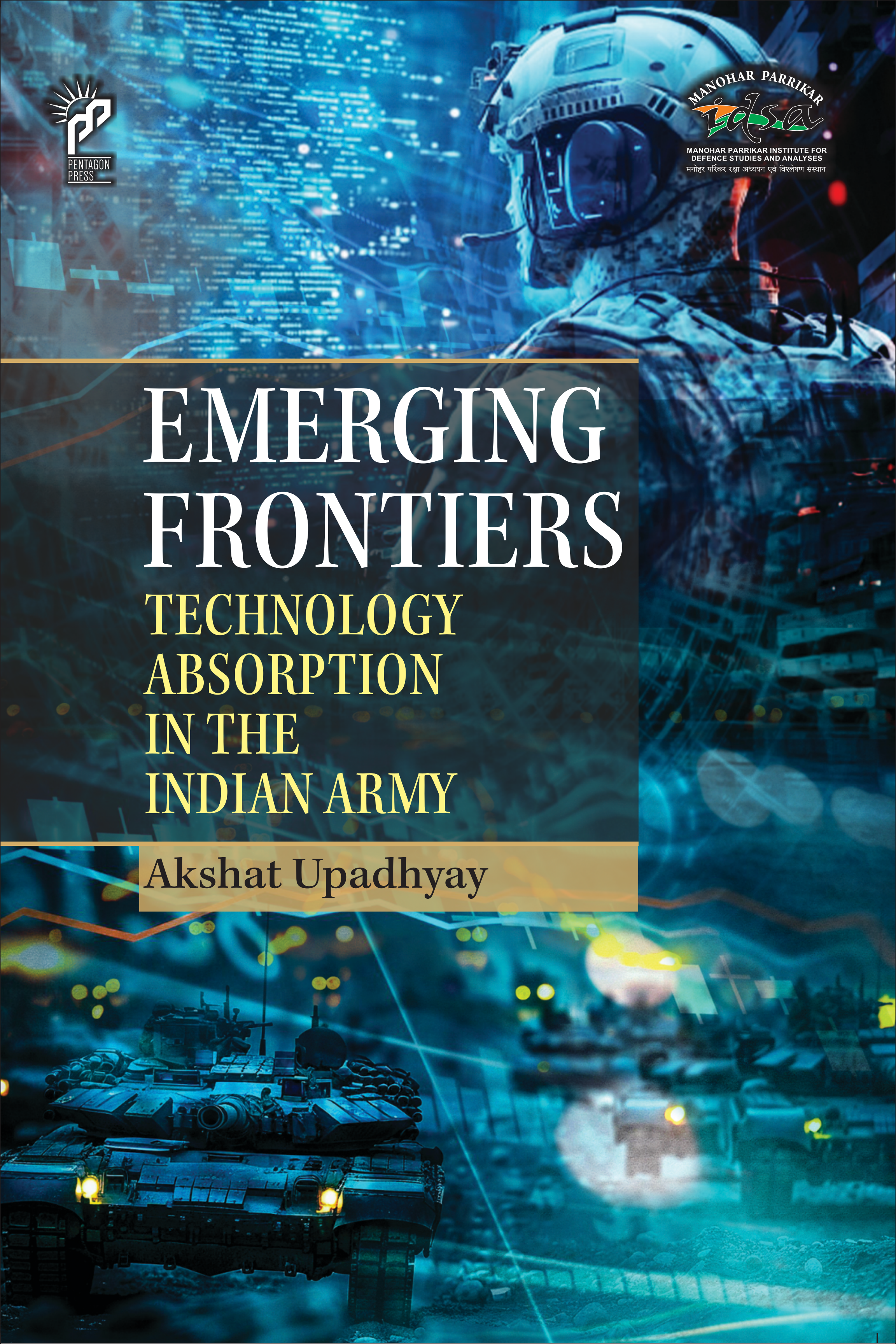


PENTAGON PRESS

MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

EMERGING FRONTIERS

TECHNOLOGY ABSORPTION IN THE INDIAN ARMY

Akshat Upadhyay

EMERGING FRONTIERS

Technology Absorption in the Military

EMERGING FRONTIERS

Technology Absorption in the Military

Akshat Upadhyay

MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
[illegible]

PENTAGON PRESS LLP

First published in 2025 by

PENTAGON PRESS LLP
206, Peacock Lane, Shahpur Jat
New Delhi-110049, India
Contact: 011-26490600

Typeset in AGaramond, 11.5 Point
Printed at Aegean Offset Printers, Greater Noida

ISBN 978-81-984458-8-9 (HB)

Disclaimer: The views expressed in this book are those of the authors and do not necessarily reflect those of the Manohar Parrikar Institute for Defence Studies and Analyses, or the Government of India.

www.pentagonpress.in

Contents

Acknowledgements

The successful completion of this book would not have been possible without the unwavering support and blessings of many people. This is a labour of love and writing this has been as cathartic for me as I hope it is informative for the readers.

A heartfelt gratitude to my father, Maj. Gen. Ashok Kumar (Retd.) for believing in me, and cajoling me (to the extent of coercion) into writing many such works in the future. His enthusiasm for my written work and attempts at proliferating it through broadcasts, remains a constant source of motivation.

My mother, for her constant inspiration and love.

My wife, Ishita, for her rock solid support and belief in my work, despite the fact that I have tried multiple times to force her into reading at least a page of my writings and have failed every single time. Secretly, I know she has read at least one.

My younger brother, Sqn. Ldr. Anubhav Upadhyay, medical wizkid and Aviation Medicine Specialist. His ideas on certain sections of the book have been very insightful. Many thanks to Ankita, my sister-in-law for her constant support. A lot of what you see on the book cover and hopefully will judge me for it, is a result of her designing expertise.

The very fact that I have been able to write a second book and have it published speaks volumes about the inspiration and constant motivation that I have received from my seniors, peers and juniors during my time in this wonderful organisation and the broader armed forces community (serving and retired). It is very hard to point to every one who has, in a persistent manner, prodded me on this path, and if I forget to acknowledge them here,

the fault is entirely mine. I have learned a lot and have been given freedom to express my views and perspectives on a number of subjects, honing my skills in the process. My heartfelt gratitude and thanks to Lt. Gen. D.P. Pandey (Retd.), Lt. Gen. Mohit Malhotra, Maj. Gen. R.R. Patil (Retd.), Maj. Gen. Voodev Parida, Maj. Gen. Abhijit Mitra, AVM Arjun Subramaniam (Retd.), Brig. Somnath Banerjee (Retd.), Brig. K. Arun, Col. P.K. Sharma, Col. Manas Kundu, Col. Ankur Pandey, Col. Praveen Kumar, Col. Sachin Ujjwal, Col. Ankur Srivastava, Lt. Col. Saket Mishra, Lt. Col. Rachit Ahluwalia, Lt. Col. Peeyush Nath, Lt. Col. D. Satapathy, Lt. Col. Shaleen Kaushik and Maj. Keshav Sharma.

My time spent at Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA) has been a revelation. This organisation is a treasure trove of knowledge and insights on all things national security. The assistance and support received has been nothing short of wonderful. My first and foremost thanks to the Director General Ambassador Sujan Chinoy. I have rarely met such a splendid mix of a personality with an elephantine memory and splendid oratory skills. Ambassador Chinoy has been extremely supportive in my endeavours in the two years of my Research Fellowship at MP-IDSA. My other colleagues at MP-IDSA: Col. Vivek Chadha (Retd.), Gp. Capt. R.K. Narang (Retd.), Cmde. Abhay Kumar Singh (Retd.), Shantanu Sinha IPS and Shruti Pandalai have always been a source of motivation and their insights on the topic of this book have been illuminating, to say the least. Dr. Swasti Rao, ex-MP-IDSA and now at the O.P. Jindal University has always been forthcoming with her views on the geo-strategic implications of emerging technologies and supply chains. Finally, Mr. Vivek Kaushik, Associate Editor at MP-IDSA and the tireless and ever-smiling workhorse of the organisation has gone through the endless drafts and revisions for the book to take its present shape. His contribution to the project is immense.

Finally, a special vote of thanks to Nuthan Prasanna, CEO Dvizira, an inspired and inspiring young defence technology entrepreneur and a true patriot whose insights on my writings have contributed to my own knowledge bank.

For everyone who has cheered me on and encouraged me, I will forever be grateful.

Akshat Upadhyay

Introduction

War and technology are inextricably linked in an endless cycle of destruction and creation. War creates conditions for innovation at a grand strategic, strategic and operational level due to the nature of this societal interaction: crises, urgent requirements, increasing pressure on constrained resources and need for inter-se prioritisation are hallmarks of wartime economies. Several problems and challenges arising out of war and warfighting are subjective and contextual to that particular period and interaction, necessitating a turn to science and technology for solutions. As a result, most innovations are products of conflict. Once wars end or are deemed to be paused for a longer duration (due to, say, an armistice, ceasefire or stalemate), the rigors of peacetime tend to temper or extinguish the flames of the innovation engine. A longer, comparatively peaceful ecosystem usually leads to private companies innovating on proven military technology – the so-called "spin-off" phenomenon. However, the end of the Second World War removed the existential Damocles' Sword hanging over the collective West, to be replaced by the Cold War which, barring a few episodes of nuclear grandstanding, remained 'peaceful', especially for the West. As a result, there has been a steady intellectual and scale transfer from the government to the private sector, the latter now light years ahead of the former.

The advancements in technologies generally tend to slow down. This shift, initially gradual, has picked up in the last decade. The question then arises: how do militaries leverage this unfolding revolution for their benefit? How do militaries leverage "spin-in"? In other words: how do militaries absorb technology?

In terms of categorisation, one needs to understand the basic concept of industrial warfare or the form of warfighting and related concepts that most militaries are familiar with and have been practising since the Second World War. Industrial era warfare was characterised by technologies designed specifically for the military and the broader security ecosystem, with multiple cycles of experimentation, testing and customisation. The typical time lag between military testing and use and civilian commercialisation, during the honeymoon era of state and science ie from the 1940s to the 1970s, was usually 20-25 years. For example, the transition from ARPANET to the Internet took close to three decades. This transition was not a sudden flip of the switch but a gradual and piecemeal giving away of precious intellectual property (IP). Similarly, the cases of GPS and microelectronics also display the same trend. Once innovation in the private sector picked up pace, due to the advent of semiconductors and their multiple applications, national security requirements were slowly but steadily replaced by commercial ones. Within the United States (US), the so-called peace dividend at the end of the Cold War reduced the relevance of the military as a large-scale customer for the private sector. The consolidation of the 'defence primes' after the 'Last Supper' in 1993 concentrated military innovation within those handful of companies. The private defence sector, as a major supplier of military technologies and platforms, already underinvested by the military, was reduced to a handful of ancillary companies providing spare parts and specific technologies to the bigger defence primes. However, the major technological innovations were still happening within the private sector, which had taken off from the initial funding and organisational support of the US Department of Defence (DoD). This time, the shoe was on the other foot and the issue of technology absorption became critical for the military since it became the site for secondary technological absorption, if any. In other words, technologies that had already matured commercially had to be adapted and adopted by the military, creating a conflict between how militaries view technology and how commercial technologies behave. This is the situation that militaries across the world, including India, face today.

Through this book, an attempt is being made to define and clarify the nature of emerging and disruptive technologies by explaining basic terms and concepts, followed by a discussion on how contemporary philosophers and practitioners of technology think about them. The main theme of the book hinges on the absorption of technology within the Indian Armed Forces, with the focus particularly on the Indian Army. Though this will be covered in detail later, a short introduction is provided to contextualise this new thinking.

There are usually three elements involved in the procurement process of any technology/platform within the military: the developers, the production agencies and the users. The developers are generally the academia, research and development (R&D) organisations and the private sector. This group prognosticates, forecasts and works on basic technologies in order to develop applications or prototypes for use in the military. The production agencies provide the means to refine, tweak, modify and then scale the product so that it can be made available to the user in deployable and deterrent quality and quantity respectively. The users are the most dynamic actors in this whole process since the agency of the user in designing and modifying technologies and platforms differs significantly from country to country. In fact, within the same uniformed force, the role of the user in technology acquisition differs widely. For a long time it has been assumed that the role of the user is solely to define and lay down certain broad attributes of a platform based on the threat scenario, which in itself is derived from a broader security and defence strategy. Once a prototype is created, the user will vet the platform in different settings, followed by a financial process in which the lowest bidder will receive the contract to manufacture the platform at scale. After this, drills and procedures are employed for training and deploying the platform. This was the situation in the previous eras of industrial age warfare where specific platforms performed specific tasks and improvements were evolutionary in nature. Tanks are upgraded to better tanks, and similarly, artillery guns, fighter jets, destroyers, submarines, missiles and helicopters to their more modern and hopefully, better selves. These tasks could be stitched together using communications and basic networking but could not be switched. Tanks could not fly nor could helicopters go underwater.

The current fourth industrial era is different. Instead of platforms alone, the focus is on capabilities and systems. The hardware forms the foundational layer for a greater level of military and technological abstraction supplemented by advancements in computing, electronics, miniaturisation and power consumption. This means that the various industrial and modern era platforms are connected through intelligent networks, powered by autonomy and function as a singular whole to achieve effects. A single hardware platform such as an aerial drone becomes a vessel for the integration of advanced technologies and capabilities such as cameras, sensors, bombs, electronic warfare (EW) and even cyber warfare. The role of the user has also expanded. Apart from the functions mentioned in the previous paragraph, the user now is required to absorb commercial technologies at the speed of innovation. Many militaries have created innovation organisations to harness the engineering and technological expertise of their service members in concert with academia and industry for leveraging these emerging and disruptive technologies. Instead of a tank or an artillery gun, the talk is about firepower, intelligence analysis, manoeuvrability and autonomy. Similar to a graphical user interface (GUI), only the abstraction is visible to the user while the inner components (in this case individual platforms) are required to work noiselessly. The user, therefore, needs to absorb technologies in the following fields: organisational, operational, intellectual and functional. This is a major departure from the conventional thinking about the relation between the soldier and technology. Instead of solely being a user, the soldier now also needs to be a creator, thinker, designer and regulator. This is the central theme and premise of the book. The book also posits that there is a deep interconnection between innovation and absorption. Through analysing case study of defence innovation ecosystems of three countries – the US, Israel and Ukraine – different levels and conditions under which absorption takes place will be studied. Observations from contemporary conflicts will be used to judge and derive lessons that may be suitably adapted to the Indian Armed Forces.

The absorption of technologies is not merely a matter of acquisition but a complex interplay of organisational ambidexterity and technology absorptive capacity (TAC).[1] Organisational ambidexterity – balancing innovation and market exploitation in management theory terms – becomes crucial. This concept aligns with the need for the armed forces to maintain robust current operations while dynamically adapting to technological innovations. Furthermore, the book rewires TAC – the ability of a military organisation to recognise the value of new technologies, assimilate it and apply it for strategic ends. For the Indian Armed Forces, this involves not only the integration of cutting-edge technologies but also the development of an ecosystem that fosters innovation, learning and adaptation. It is here that a new concept, that of an Adaptive Integrative Framework for Technology Absorption in the Armed Forces (AIF-TAF), coined by the author, is introduced. The AIF-TAF attempts to take a broader look at the absorption of emerging technologies into the armed forces by combining concepts from complexity science, military and defence innovation and management science.

Through analysis of primary and secondary literature on the subject – certain important observations are eked out with respect to the absorption process of emerging and disruptive technologies within the Indian Armed Forces. The final section of the book recommends methods and means to enable the Indian military to absorb technologies better, as per AIF-TAF, and in the process start seeing modern warfare from a renewed perspective.

NOTES

[1] Tarique Mahmood and Muhammad Shujaat Mubarik, "Balancing Innovation and Exploitation in the Fourth Industrial Revolution: Role of Intellectual Capital and Technology Absorptive Capacity", *Technological Forecasting and Social Change,* 120, November 2020, pp. 1–9.

Chapter One

Understanding Technology: Foundations and Definitions

The focus of this book is on absorption of disruptive technologies by the Indian Armed Forces, especially the Indian Army. It is therefore necessary to understand in detail what technology is, how it relates to emerging or disruptive technologies and finally, what are the means and processes through which armed forces absorb any technology. The process of absorption is complex and nuanced and is an interplay of three factors, that is, absorption, innovation and the technological absorptive capacity (TAC) of an organisation. Assuming a cyclical periodicity, within the military, absorption will refer to an end state where successful military and defence innovation combine to create lasting changes in tactics, techniques and procedures (TTPs), eventually culminating in military effectiveness. As a new model of absorption will show, the interplay of TAC, absorption and innovation is a three-layered model where TAC informs the level of innovation, which mediates between TAC and absorption. However, successful innovation and absorption also act as positive feedback that loop back to increase and improve TAC in an ideal virtuous cycle. Successful absorption creates an elevated base for TAC and raises the technological threshold for further innovation. The next section will focus on the various aspects of innovation in the national security realm and see the factors influencing its development and finally define the contours of this new framework of absorption, aptly named Adaptive Integrative Framework for Technology Absorption in the Armed Forces (AIF-TAF).

Defining Technology

There are multiple approaches to defining and contextualising technology. It is therefore, pertinent to define emerging technologies, and how they relate to the broader concept of technology. This section will focus on the works of prominent thinkers, scientists and practitioners and look at the multiple ways in which technology has been conceptualised by them. Once we home in on a proper understanding of technology, we can then focus on its main attributes, the various terms that will help us understand its nature and how emerging technologies figure under the gamut of technologies.

What is Technology?

Technology can be understood as the application of 'conceptual knowledge for achieving practical goals, especially in a reproducible way'. Technology includes both the products (tools and platforms) and abstractions (software). Technology can be 'viewed' from multiple lens: it can be seen as an enhancement of humans' mental and physical faculties; an oppressive tool; a liberating force – all based on what it represents to a particular class and time period. There are two opposing views regarding how technology is viewed in terms of its genesis: technological determinism and social constructivism. The former theorises that the growth trajectory of technologies follows a natural progression while the latter surmises that there is no inevitability to the growth of technologies and that they are shaped by culture, laws and politics. A slightly different conception of technology is that of David Deutsch, who considers technology as a form of knowledge on how to manipulate the physical world to achieve human purposes. Science and technology co-evolve with each other with advances in one spurring progress in the other. For example, advances in optics or the study of light (science) lead to advanced microscopes (technology) that help to study the world of microbes, let's say, in greater detail (science). Science solves problems of understanding, while technology solves practical problems.

What is Emerging Technology?

The term 'emerging technologies' refers to a set or group of technologies that are innovative, in the early stages of adoption or development and have the potential to significantly impact various fields in the future. They are characterised by radical novelty, coherence (over time), relatively fast growth, prominent impact and uncertainty and ambiguity. Emerging technologies are generally interdisciplinary, that is, they combine multiple seemingly disparate fields. The advent of digitisation and computation has rendered all fields amenable to mixing and made the emergence of technologies faster and relatively easier. In terms of the military, these are technologies that are in the research and development (R&D) phase, have a relatively high chance of affecting radical change in the future of warfare, may face ethical, legal or moral challenges in deployment and have uncertain long-term strategic implications.

What is Disruptive Technology?

Disruption is the overthrow of established conventions and that is what disruptive technologies set out to do. In a more general setting, disruptive technologies significantly alter the way consumers, industries or businesses operate, often displacing established technologies and shaking up the market. Within the military domain, these are innovations that fundamentally alter military doctrine, strategies or the balance of power, often rendering existing military systems or tactics obsolete. These generally start off in niche areas and then branch off to more practical fields and disrupt existing conventions of warfighting. For example, use of drones as individualised firepower and intelligence, surveillance and reconnaissance (ISR) asset, hyperspectral cameras for detailed target detection and identification, enhanced night vision and improved situational awareness. Drones have disrupted the conventional reliance on manned fighter jets and bombers for air superiority and strike missions. They have altered air defence (AD) strategies, making it necessary to defend against smaller, more numerous and generally expendable air threats. Hyperspectral cameras have disrupted conventional methods of battlefield reconnaissance and reduced reliance on human scouts and traditional optical/infrared (IR) systems.

What is Niche Technology?

Niche technologies are specialised innovations designed to serve a specific, often limited market segment or solve a particular problem. These are generally stable within their niche domains, have a limited broader market appeal and are highly customised and customisable. In the military domain, they can be understood as specialised military innovations designed for specific operational needs, particular branches of service or unique combat scenarios.

Though one can go into further details of the differences between these terms, it is equally important to understand that in the military context, the distinctions between these categories are more fluid, as a technology that starts as niche or emerging can quickly become disruptive if it proves highly effective in combat or significantly alters the strategic landscape. It is for this reason that the focus of the book is on emerging and disruptive technologies.

Before delving into the details of emerging technologies and how they affect warfare and the military structure, the next section takes a look at how technology, especially digital technology, is seen and understood by the stalwarts of the field. A careful selection of academics, philosophers and practitioners has been taken to provide an all-round perspective on differing views on technology.

Conceptions of Technology: Leading Thinkers and Practitioners

W. Brian Arthur

An accomplished economist specialising in the application of complexity science to economic problems and credited with the invention of the "El Farol Bar" problem,[1] Arthur Smith's influential book, *The Nature of Technology: What it is and How it Evolves*, provides a new form of reference on thinking about technologies. His approach to technology is deeply rooted in an evolutionary framework, drawing parallels with Darwinian concepts. He touches upon how technologies evolve, not through a linear progression but through a complex and adaptive process, similar to the Darwinian concept of natural selection.[2] He argues that technology isn't just a collection of gadgets or tools but a complex system of interconnected parts, practices and methods that work together, much like an ecosystem. He uses the term 'phenomena'[3] to describe the natural processes or principles that technologies leverage, such as a solar panel capturing sunlight to generate electricity through the photovoltaic effect. Central to his theory is the idea of 'combinatorial evolution',[4] where new technologies emerge from combining existing ones, mirroring how biological evolution works through the mixing of genetic traits.

Arthur also talks about 'structural deepening', meaning that technologies grow more complex over time as new functionalities are added, making the system increasingly intricate.[5] He emphasises the importance of 'modularity', the way technologies are made up of separate parts that can be swapped or reconfigured, allowing for flexible evolution.[6] Another key concept is 'path dependence', which suggests that a technology's development is heavily influenced by its historical use, shaping its future direction.[7] Closely related is 'lock-in', where a technology dominates not necessarily because it is the best but due to historical reasons or compatibility with existing systems, influencing future technological paths.[8] Arthur's work suggests that technological evolution, much like biological evolution, is not deterministic or predictable. It is contingent on a series of historical accidents, complex interactions and the constant remixing and repurposing of existing technologies. Understanding these concepts is crucial for comprehending how technologies develop and spread with profound implications for defence. When talking about technology, including emerging technologies in the rest of the book, this definition and conception of technology will be taken as the baseline.

There are a number of academics and practitioners of technology whose work features and defines the way technology is understood throughout this book. It is therefore important that their main thoughts and concepts are spelled out in brief before attempting an interlinking and distillation of their ideas. Individuals featured in this book include Carlotta Perez, Clayton M Christensen, Manuel Castells, Tim O'Reilly, Don Tapscott, Luciano Floridi, Yochai Benkler, Andrew McAfee, Balaji Srinivasan and Azeem Azhar. We will also look at some specific technological 'movements' that have influenced the development of these technologies and shape the encounter between technologies and societies.

The AIF-TAF framework focuses on the process of absorption and looks at the environmental and structural factors that contribute to technology absorption within the armed forces. The AIF-TAF also collates lessons learnt from the recent wars and conflicts in Armenia–Azerbaijan, Russia–Ukraine and Israel–Hamas. In the succeeding sections, we will have a look at the various concepts enunciated by these thinkers and see how they are relevant to the military. Later, after the respective thinkers and the movements have been analysed, the beginnings of AIF-TAF will be discussed and debated in detail.

Carlota Perez

Carlota Perez is a Venezuelan researcher renowned for her contributions to the understanding of technological revolutions, economic development and social change. Her seminal work, *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages*, provides a comprehensive framework for interpreting the interplay between technology, economics and societal structures. She does not define technology in isolation but rather sees it as a core element of 'techno-economic paradigms', which are broad configurations of technologies, industries, infrastructures and markets that drive economic growth and transformation.[9] These paradigms shift when radical innovations or what she calls 'technological revolutions',[10] disrupt the status quo and reconfigure economic and social landscapes.

She argues that technological revolutions occur in predictable cycles: an irruption phase marked by the advent of breakthrough technologies, followed by immense financial speculation (frenzy phase) and investment leading to a crash. After the crash, a synergy phase emerges, where technology diffuses broadly and leads to a 'golden age' of productivity and prosperity, finally ending with a maturity phase where growth slows and new tensions arise, setting the stage for the next revolution.[11] Perez's framework is rooted in Joseph Schumpeter's theory of 'creative destruction'[12] but extends it to explain how technology and financial dynamics can lead to structural changes in the economy and society. Before delving into how this conception of technological cycles affects military technologies and their absorption, it is important to understand capital cycles in brief, and how capital cycles impact innovation cycles.

Perez's conception of a boom-bust-plateau cycle is a much-nuanced approach that shadows theories by three classical economists, namely, Joseph Schumpeter, David Ricardo and Thomas Malthus. As per Schumpeter, and as argued above, there are industries that create new as they destroy the old, attempt to produce more with less and in the process unlock a new resource for the world.[13] Ricardo contended that due to trade, expansion and competition, this new resource gets distributed to new markets and made accessible to all.[14] Finally, it gets Malthus's conviction that the increased accessibility creates fear of corresponding need and hence a fear that there won't be enough for everyone, resetting the cycle that went back to extractive or the Schumpeterian phase.[15]

A post on the social media network Medium by Hemant Mohapatra, an ex-partner in a16z, a venture capital (VC) firm based in the Silicon Valley, California, explains this in the context of software as a service (SaaS) product, capital expenditure (CAPEX) and operational expenditure (OPEX) cycles in a succinct manner. He describes how technological innovations undergo initial CAPEX-heavy cycles of R&D, followed by OPEX-heavy cycles where the focus shifts from fundamental innovation to differentiation based on efficiency, marketing and branding.[16] One of the examples cited involves the semiconductor industry. The semiconductor industry went through a substantial CAPEX cycle as companies such as Intel and AMD innovated in Central Processing Unit (CPU) technology. Over time, as CPUs became ubiquitous, the semiconductor industry transitioned into an OPEX-heavy cycle characterised by marketing strategies such as Intel's 'Intel Inside'.[17] One of the biggest effects of the omnipresence of CPUs is that modern technology in the form of compute heavy platforms is available to ordinary individuals, initially the preserve of universities and the military – organisations with significant amounts of resources.

This transition set the stage for the software and internet cycles, starting with significant innovations that unlocked new behaviours, such as Dropbox's revolutionising of file sharing. As these sectors matured, differentiation became less about groundbreaking innovation and more about incremental improvements and service aspects, leading to saturated markets and intense competition – a Malthusian scenario. The author suggests that we are now entering a new era where the cost of 'intelligence' or 'insight' driven by artificial intelligence (AI) is becoming the focal point. Instead of the current model of compute-SaaS-insight, the future trend may be compute-insight. The future of SaaS lies in AI-driven insights rather than compute-driven processes, which will create a more intuitive and efficient user experience.[18] This insight-driven approach is posited as the next major frontier in technological innovation, following the pattern of historical shifts from CAPEX to OPEX cycles in various industries. Let's take this frame to the military and have a look at two emerging technologies or platforms: drones or unmanned aerial systems (UAS) and AI.

CAPEX and OPEX in AI: Concept and Analysis

Initial investments in AI for military applications are substantial and involve both financial resources and human capital. This is the phase where foundational AI technologies are developed and adapted for unique military requirements. For example, developing an AI system capable of processing vast amounts of intelligence data for real-time decision-making requires significant R&D resources to create algorithms that can learn from and act upon complex and noisy data environments. Once the AI systems are operational, the focus shifts to maintaining and upgrading these systems, involving better methods of utilsing compute such as test-time compute, data management and system integration across various military platforms. This is visible in AI systems that are used for predictive maintenance of military equipment and where the initial development of the system is CAPEX intensive, but ongoing integration with equipment, analysis of data and continuous improvement falls into OPEX. The difference here is not in creating a new predictive maintenance system but in how well it can predict failures and streamline operations compared to others.

AI in the military is still largely in an extractive (CAPEX) cycle. This is characterised by significant R&D efforts to harness AI for various military applications such as autonomous vehicles, cyber defence, intelligence analysis and logistics management. Military AI is a rapidly advancing field, and the focus is on developing and refining technologies to ensure that they can operate reliably and effectively in volatile and complex environments where the military operates. For AI, continued investment in the extractive industries – involved in creating and refining AI capabilities – should be the dominant strategy. This investment is essential to maintaining a competitive edge, given the rapid pace of technological change and the strategic advantage conferred by advanced AI systems. There is a strong emphasis on developing AI that can process and analyse large datasets for decision-making, conduct autonomous operations and enhance the capabilities of human operators (human machine teaming or HMT).

CAPEX and OPEX can also be further understood under further subcategories of cost-benefit analysis, lifecycle management and finally procurement strategy. Military planners must consider the trade-offs between investing in new technologies (CAPEX) versus upgrading and maintaining existing systems (OPEX). With AI, the cost of initial development might be justified if the technology offers a significant strategic advantage such as enhanced cybersecurity defences or an exponential shortening of maintenance timings and material improvements within formations. However, one has to keep in mind that intangible issues such as improvement in quality of command and control through the use of AI-enabled systems may have to be quantified through other means such as interlinkage with military effectiveness or foregone in the overall analysis. Induction of AI into the military requires a lifecycle approach to investment. For AI, this involves planning for the continued training of machine learning (ML) models as new data becomes available on a regular periodicity or better ways of using post-training methods for inference tasks. Military procurement must adapt to the innovation cycle of these technologies. During the CAPEX phase, contracts might include extensive R&D components while in the OPEX phase, contracts could focus on service-level agreements, maintenance and iterative improvements. This also requires a different approach not only to procurement but also recruitment policies for personnel in the procurement verticals.

CAPEX and OPEX in Drones: Concept and Analysis

The early development of military drones is marked by high CAPEX due to the costs associated with designing, testing and manufacturing advanced materials, propulsion systems, energy storage and management systems, rotors and integrated sensor suites, among others. Investing in cutting-edge drones that can operate autonomously in contested environments, for instance, requires extensive upfront costs in technology and system development. As drone technology matures, the emphasis shifts from development to deployment, sustainment and incremental improvements. The OPEX cycle involves costs such as training operators, routine maintenance and software upgrades to enhance capabilities such as surveillance and delivery of payloads. During this cycle, militaries can focus on scaling operations by increasing the number of drones in use or improving the operational efficiency of existing fleets, rather than developing entirely new drone models.

Drones may be transitioning from an extractive to a distributive (OPEX) cycle. Drones have been used by the military for intelligence, surveillance and reconnaissance (ISR); certain militaries have effectively used them for combat operations for several years. This indicates that the foundational technologies have matured. The focus is now shifting towards enhancing the operational efficiency of drone fleets, improving maintenance and support systems, adding more performance and sensor assets to the drones and developing interoperability with other military systems. Investing in distributive industries related to drones could involve focusing on systems that enable broader deployment and better integration of drone technologies into the existing military infrastructure. It could also mean investing in training programs, user interfaces that allow for easier control of drone swarms and maintenance systems that allow for rapid repair and redeployment.

In terms of cost-benefit analysis, lifecycle management and procurement strategy, for drones, the decision to invest in a new design would depend on whether the performance gains align with strategic objectives. Lifecycle management will include planning for technology refreshes (in terms of slots, software compatibility, performance upgrades etc) to ensure that unmanned systems remain at the cutting edge of capabilities. A great example of this is how new Chinese electric vehicle (EV) makers are leaving their Western counterparts behind. They leave additional chips inside their newer models in the anticipation that may need to add performance-enabling features or totally new ones in the existing models.[19] Since cars are now being viewed from the perspective of 'as-a-service' models such as Mobility-as-a-service[20] and micromobility,[21] most of the additional features are digital and software based. The same model may be used in drones, such as facilitating swarm or autonomous operations. Finally, from the view of procurement strategies, military leaders must make informed decisions about where to allocate resources to maximise operational effectiveness and maintain technological superiority.

Clayton M Christensen

Clayton M Christensen was the Kim B Clark Professor of Business at the Harvard Business School where he coined the concept of 'disruptive innovation', introduced first in his book *The Innovator's Dilemma*.[22]

Christensen defines technology broadly as the processes by which an organisation transforms labour, capital, materials and information into products and services of greater value.[23] He emphasises that technology may not necessarily be innovative in itself, rather innovation occurs when technology is applied in a way that disruptively impacts markets or creates new ones. Disruptive technologies typically start out as cheaper, simpler, smaller and often more convenient solutions that initially target less-demanding customers. This notion contrasts starkly with sustaining innovations, which are incremental advances that help firms improve within existing markets. The 'Jobs to Be Done' framework proposes that customers 'hire' products to fulfil specific needs or jobs and that true innovation addresses these often unspoken jobs more effectively.[24] The key insight is that customers are less concerned with product attributes per se and more with the utility and outcomes that these products enable. In the military context, a 'job to be done' might be 'detect and neutralise threats' – drones might be 'hired' to complete this job more efficiently than manned aircraft in certain contexts, not necessarily because they are more advanced, but because they fit the job requirements better, such as being cheaper to operate and posing no risk to pilots.

Another term conceptualised by Christensen, 'value networks' define the operational and competitive context of firms, setting the stage for potential disruption by those not traditionally playing within these established networks.[25] They are the broader context within which a business operates, including supply chains to customer relationships. These networks influence and constrain the types of innovations a company can successfully introduce. In military terms, a value network might comprise defence firms, procurement processes and traditional weapon platforms, all of which prioritise certain types of technological innovation while potentially being resistant to others that don't fit an existing framework but might be more effective or cost efficient.

Christensen also introduces the RPV Framework – Resources, Processes and Values – as a three-way model that forms the sum total of a firm's capabilities. While resources are tangible and tradeable, processes and values embody often the inflexible and intangible methodologies and priorities of a company, which can hinder its ability to adapt to disruptive innovations.[26]

In the military context, resources would include weapons systems, intelligence capabilities, human capital (soldiers and staff), bases and technology infrastructure. Processes in the military encompass strategies for training, deployment, intelligence gathering, maintenance, logistics and decision-making protocols, among others. The military's values could be its mission, strategic priorities, rules of engagement, or the emphasis it places on certain types of capabilities (e.g. prioritising cyber warfare over traditional ground forces, or preferring continuous attrition over selected decisive engagements).

Finally, the law of conservation of attractive profits states that as commoditisation occurs through sustaining innovations, profit opportunities migrate to another part of the value chain, often to those who facilitate the commoditisation or to entirely new products or services.[27] In the military, as certain technologies or capabilities become standard (commoditised), the focus and potential for gaining strategic advantages (attractive profits) shift elsewhere. In military terms, this is the search for offsetting capabilities. For example, when advanced fighter jets become commonplace, competitive edge may shift to stealth technology, advanced radar systems or even to the domain of cyber warfare – areas that may have been less emphasised before but now offer a significant advantage (attractive profits). Similarly, as basic drones become more affordable and widely used, the differentiation and strategic advantage may shift to autonomous capabilities or integration with broader intelligence systems. Understanding and applying the RPV framework and the law of conservation of attractive profits can help military leaders and defence planners ensure that resources are allocated effectively, processes are innovative and adaptable and values align with the changing character of warfare. It ensures that as some aspects of military capability become standard, attention and investment can shift to the next innovative leap that will provide a competitive advantage.

In the context of the military technology, Christensen's theories imply that disruptive innovation can fundamentally alter strategic and operational landscapes. Military institutions, like established companies, can be prone to overlooking disruptive technologies that do not initially meet the standards of existing value networks. However, these innovations, when scaled and improved upon, have the potential to redefine the theatre of conflict and challenge existing notions of conventional military superiority and deterrence.

Manuel Castells

Manuel Castells is a sociologist widely recognised for his extensive work on the information society, communication and globalisation. His most influential contribution is the concept of the 'Network Society', detailed in his trilogy *The Information Age: Economy, Society, and Culture*. He understands technology – especially information and communication technology (ICT) as central to the formation of the contemporary social structure, which he describes as the network society. As per him, network society is "where the key social structures and activities are organised around electronically processed information networks".[28] From the perspective of the military, this may signal a paradigm shift where technology is understood not merely as a tool for enhanced capability but the very infrastructure that underpins all aspects of military operations. The ability of forces to conduct operations across vast distances with precision and in real-time, or time-space compression, is a direct result of this ICT revolution. Network society has particular relevance for the military in the form of advanced operational frameworks. The very nature of modern military engagement is characterised by flexibility, responsiveness and a dependence on network-centric warfare (NCW). This networked approach harnesses the power of ICT to link personnel, equipment and information sources together, creating a formidable and cohesive combat capability that can adapt to changing situations dynamically.

Relevant terms that can be culled out of Castells' theory for the military are 'space of flows' – tangible and intangible components allowing for the global movement of capital, information and people.[29] When translated to the military, they are understood as diffusion of technology, civil-military integration or fusion and capital flows (from VC funding or government funds to startups to the military). Military operations take place in a domain where physical movement of forces is integrated with the virtual flow of information, creating a complex operational environment that demands a sophisticated understanding and mastery of both material and immaterial aspects of power projection. Castells' conception of the innovation and informational economy accords priority to knowledge and information (intelligence within the military) in the security domain. The capacity to generate, process and operationalise information quickly has become critical to maintaining a strategic and tactical advantage over adversaries.

Tim O'Reilly

Tim O'Reilly is an author and entrepreneur who popularised the terms 'Web 2.0'[30] and 'open source',[31] and introduced several unique concepts such as the 'Internet Operating System', 'algorithmic regulation' and 'inner source'. Very briefly, these terms respectively refer to the foundational services and protocols that underpin the web and enable applications to deliver rich user experiences ('Internet Operating System');[32] use of algorithms by governments and organisations to automate decision-making, policy implementation and regulatory compliance ('algorithmic regulation');[33] and the adoption of open-source software for developing practices in an organisation to enhance collaboration and innovation ('inner source').[34]

O'Reilly's concepts have important implications for militaries and their relationship to technology. The two-way communication and interaction engendered by the notion of Web 2.0 highlights the transition from a one-way communication of information (conventional military approach) to an interactive and integrated approach to intelligence, operations and communications. In practical terms, this means leveraging real-time data streams, social media analytics and crowd-sourced intelligence to plan and conduct operations. Platforms allowing two-way interactions can significantly enhance situational awareness and decision-making. For example, integrating social media intelligence or open-source intelligence (OSINT) into military operations can provide real-time insights into public sentiment, adversary movements and potential security threats. In more social terms, this also makes way for a more communication and managerial heavy leadership where 'orders' – understood as one way communication between higher and lower commanders in the military – are transformed into a two-way 'communication'. What this means in practical terms is to adjudicate between the two military imperatives of centralisation and decentralisation.

While centralisation is required for translating political objectives into military ones, decentralisation is required at the operational level and below. This is where the Web 2.0 terminology comes into play. The requirement is not only in terms of technology but also of a 'technological temperament'. The open source ethos that O'Reilly champions, can be translated into the military, through the practice and philosophy of shared software development allowing for a more trusted and collaborative approach not only across the hierarchy in the Army but also between the Army and civilian counterparts working in the same functional domain. By adopting open-source principles, a military organisation such as the Indian Army can tap into a spread-out community of indigenous developers to accelerate technological advancements and ensure the robustness of their digital infrastructure. Additionally, the use of open-source software can reduce costs and increase flexibility in the development of military systems, though one needs to be careful and deliberate while deploying them.

The concept of 'government as a platform'[35] can impact military operations by making government data and services more accessible and functional, promoting clusterisation of scarce resources and capabilities, such as GPUs. Applied to the military, this means disclosing and sharing non-sensitive data to encourage development of applications that can, for example, aid in disaster response or veterans' services. It can also mean using government platforms to crowdsource solutions to complex logistical or strategic challenges. The Next:Economy[36] and its focus on the impact of technology on work will have significant implications for the personnel employed in the military. With an increasing role of automation and AI, the military must consider how these technologies will reshape roles and responsibilities. There is a need to have a serious re-look within the military on its existing roles and responsibilities, ensuring that personnel are trained for the high-tech requirements of the future and that the human element of warfare is effectively integrated with emerging autonomous systems. As mentioned above, the next generation of systems are likely to be automatically AI-enabled, ditching the internet and networks as a mediating medium between the user and results. Inference engines will directly interact with the user and get them the required results. This will require an infusion of personnel who understand the relevant technologies including their specificities and idiosyncrasies, and are able to tailor solutions on the go.

Don Tapscott

Dan Tapscott is the Executive Chairman of the Blockchain Research Institute, which he co-founded with his son, Alex Tapscott.[37] The institute looks into 'blockchain strategy, use-cases, implementation challenges and organisational transformations'.[38] He is also an influential author of books on the information technology (IT) revolution and blockchain.

Tapscott's thoughts on digital natives and the changing workforce, innovation through collaboration and the digital economy are more or less reflected in other theorists' works and will be not be repeated here. His unique contribution towards technology is his emphasis on blockchain and trust.[39] The potential of blockchain technology to create a new architecture for trust has profound implications for the military, especially in areas such as logistics, secure communications and maintaining the integrity of supply chains. Blockchain can offer solutions for ensuring the authenticity of critical components, secure sharing of intelligence without the risk of tampering and transparent management of contracts and resources. These applications can lead to more secure, efficient and resilient military operations, enhancing trust within military organisations.

Further exploring the realm of blockchain for military applications, one needs to be a bit inventive to see that this technology could be used in creating a decentralised command and control (C2) system. This blockchain-enabled system will operate beyond the confines of centralised command centres. In this scenario, the attributes of functional commands such as intelligence, personnel management etc will be distributed across a blockchain network, enabling units in the field to make real-time decisions based on secure and immutable data. This will not only increase the resilience of military operations against cyberattacks but also enhance the speed and agility of decision-making processes. A totally autonomous logistics system can also be visualised using the same technology where smart contracts could automatically initiate resupply missions based on real-time data from the field, such as ammunition levels, equipment wear and tear and personnel needs. Drones and autonomous vehicles, guided by AI algorithms, could then fulfil these missions without human intervention, streamlining logistics and reducing vulnerability during resupply operations. Integrating blockchain with virtual reality (VR) and augmented reality (AR) technologies could lead to the development of highly immersive and secure training environments. These platforms could record training progress, competency achievements and operational scenarios on a blockchain, ensuring that skills and experiences are verifiably tracked, recognised, and transferred when moving to a new unit/formation facilitating a more personalised and adaptive training regimen. Blockchain can also act as the foundation for the creation of digital twins for military assets and operational theatres, offering a secure and dynamic platform for conflict simulation and strategy development. By simulating real-world assets and environments on the blockchain, military leaders can explore complex scenarios, test strategies and anticipate adversary moves with high fidelity and accuracy, all within a secure and controlled digital space.

Luciano Floridi

An Italian and British philosopher, Floridi's work focuses on the philosophy of information that includes information ethics, ontology, epistemology and the logic of information. He views technology as an integral component of the infosphere, shaping and being shaped by the flow and transformation of information.[40] For Floridi, technology is both a creator and a product of the informational environment, playing a crucial role in the development and evolution of the information society. Innovation, in Floridi's perspective, is a process deeply embedded in the informational structure of the society.

He argues that the digital revolution, driven by advancements in ICT, has ushered in a fourth revolution in human self-understanding, following the Copernican, Darwinian and Freudian revolutions.[41] The Copernican Revolution marked humanity's cognitive shift from a geocentric model of the universe to a heliocentric one. This revolution fundamentally changed human understanding of Earth's place in the cosmos, replacing the long-held belief that Earth was the centre of the universe. The impact was not just scientific but also philosophical and challenged human exceptionalism and humans' perceived significance in the grand scheme of existence.[42] The Darwinian Revolution, initiated by Charles Darwin's publication of *On the Origin of Species* in 1859, acted to further humanity from its sense of self-importance as a specially endowed species. Darwin's theory of evolution by natural selection introduced the idea that all species, including humans, descended from common ancestors. This positioned humans as part of the natural world, subject to the same evolutionary pressures as other organisms, and debunked the notion that human beings were divinely created and distinct from the animal kingdom.[43]

The Freudian Revolution emerged from the work of Sigmund Freud in the late 19th and early 20th centuries, which introduced a new depth to the understanding of the human psyche. Freud argued that much of human behaviour is influenced by unconscious processes and that our conscious minds are just the tip of the iceberg of a much more complex mental structure. This challenged the Enlightenment view of the rational, autonomous individual, suggesting instead that humans are often driven by desires and fears of which we are barely aware.[44] These three revolutions collectively demoted humanity from its self-assigned position at the centre of creation, part of a divine plan and as fully rational beings in control of our destinies. They recalibrated humankind's understanding of its place in the universe and its connections to the natural world alongside the workings of human minds.

Interestingly, in Floridi's work, the digital revolution like the three others before it challenges and redefines humanity's self-conception. This revolution, driven by the advent of digital information and communication technologies, reshapes how we interact with the world and each other. It blurs the lines between reality and virtuality, between human, machine and nature, questioning the very nature of knowledge, identity and reality.

Converting his ideas into insights for the military brings out a unique perspective on the military. Today, the military has to understand its role and position within the society rather than the traditional notion of being insulated from it. This has relevance for both operational (dependence on civilian firms for armaments, networks and new technologies) and administrative domains (increasing challenges of using open networks for communication, psychological issues emanating out of excessive use of smartphones). These have to be thought of as social and human behavioural issues rather than adverse syndromes afflicting the forces. Coming to certain specific terms coined by Floridi, the infosphere represents the whole informational environment constituted by all informational entities, their properties, interactions, processes and relations.[45] The military's integration into the infosphere represents a fundamental shift in how forces conceive of the battlefield, intelligence and even the notion of warfare itself. The infosphere comprises not only tangible assets and physical domains but also digital information and cyber operations. Recognising the infosphere as a critical domain of military engagement necessitates a re-evaluation of strategy where the digital battlefield is as important as the physical one.

In terms of information ethics (IE), Floridi enunciates four principles:

- **Entropy ought not to be caused in the infosphere**[46] – For the military, this principle emphasises the responsibility to avoid actions that introduce disorder or harm to the informational environment. Cyber operations, for example, should be conducted with an awareness of their potential to cause widespread disruption beyond the intended target, affecting civilian infrastructure or compromising personal data.
- **Entropy ought to be prevented in the infosphere** – This principle calls for proactive measures to safeguard the infosphere from potential threats and disruptions. For the military, this translates into robust cyber defence mechanisms, intelligence gathering to anticipate and counter cyberattacks and collaboration with civilian agencies and international partners to strengthen global information security. By preventing entropy, the military not only protects its own strategic interests but also contributes to the stability and integrity of the global infosphere.
- **Entropy ought to be removed from the infosphere** – Beyond defence, this principle suggests an active role for the military in repairing and restoring the infosphere where harm has occurred. This could involve efforts to mitigate the effects of cyberattacks, such as restoring services and securing compromised data, as well as participating in international efforts to address broader challenges in the digital realm, such as misinformation campaigns. The military could also leverage its resources and expertise in technology to support initiatives aimed at enhancing digital literacy and resilience among civilian populations.
- **Flourishing of informational entities as well as the whole infosphere ought to be promoted by preserving, cultivating and enriching their well-being**[47] – It involves not only protecting and repairing the digital environment but also contributing to its positive development. This could take the form of advancing cybersecurity research, supporting open standards and interoperability and engaging in public–private partnerships to foster innovation in ICTs. Moreover, the military can lead by example, demonstrating ethical use of digital technologies and advocating for policies that promote the well-being of all participants in the infosphere.

Other concepts introduced by Floridi include 'onlife', which is a condition where the distinction between online and offline experiences becomes blurred.[48] The concept of onlife underscores the integration of digital technologies into the lives of military personnel, affecting everything from training and operations to welfare and social interactions. The diminishing distinction between online and offline experiences reflects a broader cultural shift within the military, impacting cohesion, command structures and the nature of service. As digital natives become prevalent within the ranks, the military's internal culture, its approach to leadership and collaboration and its adaptation to digital life become central to maintaining effectiveness and morale. Another term, reontologisation, refers to the process by which the foundational structure of reality is transformed by the pervasive dissemination and integration of digital technologies.[49] This suggests a future where, for the modern military, training, planning and even conflict may take place in environments that merge physical and virtual elements, demanding a new understanding of preparedness, resilience and combat effectiveness. The forces may have to deal with a threat or challenge that has its roots and manifestations in the digital and physical world simultaneously. The advent of cyber-physical systems is just a basic example of threats of this nature.

Yochai Benkler

Yochai Benkler is an author and Berkman Professor of Entrepreneurial Legal Studies at Harvard Law School. He is known for his book *The Wealth of Networks* and coined the term 'commons-based peer production'. He examines the role of the internet and digital technologies as catalysts for new forms of social and economic interactions. He also expounds a collaborative approach where the production of information, knowledge and culture is decentralised and largely built on volunteer participation and sharing.[50] As per him, the nature of the internet and digital technologies encourage a horizontal non-hierarchical structure of interaction amongst peers. 'Commons-based peer production', as coined by him, is an alternative to the 'traditional economic incentives of the private sector' where 'key technology standards are not owned by any one individual or organisation, and a vast majority of contributors to open-source projects do not receive direct compensation for their work'.[51] The military can benefit from commons-based peer production by engaging in open-source software development and hardware projects. This model can accelerate technological innovation, reduce costs and enhance interoperability within the military. Similar to the model espoused by Benkler, the military being a non-profit seeking organisation, can spur on the development of new technologies and platforms through collaboration with startups, individual experts and not only gain access to cutting-edge tools and systems but also contribute to a broader ecosystem of innovation that supports global security and stability.

Embracing decentralisation, the military can adapt to modern warfare's dynamic and distributed nature more effectively. Decentralised command structures and decision-making processes, underpinned by robust communication networks, can enhance operational flexibility and responsiveness. By distributing authority and empowering lower echelons with greater autonomy, the military can execute more fluid and adaptable operations, tailoring responses to specific situations. Adopting social production mechanisms can transform the military's approach to innovation and training. Platforms that facilitate the collaborative efforts of service members across ranks and specialisations could lead to the development of new tactics, technologies and problem-solving methodologies. Initiatives such as internal wikis for knowledge sharing, crowd-sourced solution platforms for tactical challenges and open forums for strategic discussions can empower individuals at all levels, fostering a culture of continuous learning and innovation. This harnesses Benkler's formulation of 'social production', which are collaborative efforts of individuals working together, generally through the internet.[52]

Andrew McAfee

Andrew McAfee is a principal research scientist at the Massachusetts Institute of Technology (MIT) and co-director of the MIT Initiative on the Digital Economy. McAfee views technology broadly as a set of digital tools and platforms that augment human capabilities, allowing humans to achieve more with less. He focuses particularly on the exponential improvements in computing, AI and network technologies, emphasising their transformative potential for productivity, innovation and economic growth.[53]

McAfee's pioneering contribution is the etymology of the Second Machine

Age, our current era, characterised by the rapid advancement and widespread adoption of digital technologies. In simple terms, it's the period we're living in now, where computers, the internet, AI and other digital tools are fundamentally changing how we work, communicate and live our lives.[54] This age is different from the First Machine Age, which took place during the Industrial Revolution. The First Machine Age was about machines that helped overcome the limitations of human muscle power. It was an era that focused on harnessing physical power to perform tasks more efficiently than human or animal muscle could ever allow.[55]

In contrast, the Second Machine Age is about augmenting and enhancing our brain power. It is about intelligence, processing information and making connections at speeds and scales that the human brain alone can not achieve. This age is powered by digital technologies allowing for the creation, manipulation and sharing of information in entirely new ways. Software, data, networks and how these technologies create bounty – wealth, better products and services and increased efficiency – and spread, which implies a growing gap between those who have access to and can leverage these technologies and those who do not.[56]

The transition into the Second Machine Age presents the military with unparalleled opportunities to augment human brain power with digital innovations. Integration of AI, ML and advanced analytics into military operations leads to enhanced decision making, intelligence analysis and surveillance capabilities. The ability to process vast amounts of data at unprecedented speeds allows for more accurate threat assessments, strategic planning and operational agility. This technological leap mirrors the shift from physical to cognitive enhancement, with digital innovation as a critical force multiplier in modern warfare. The terms 'bounty' and 'spread' reflect, respectively, increased operational efficiency, improved capabilities and enhanced situational awareness due to digital technologies and the challenges posed by these technologies, including likely obsolescence of traditional skill sets and ethical dilemmas presented by autonomous weapons systems.

The shift towards digital goods, platform-based ecosystems and crowd-sourced intelligence redefines how the military approaches innovation, logistics and engagement. Digital platforms can facilitate more efficient communication and collaboration across different branches, optimising resource allocation and strategic coordination. Crowdsourcing can be leveraged for a variety of purposes from OSINT gathering to problem-solving challenges, tapping into the collective expertise of military personnel and civilians. As AI and robotics increasingly take on roles traditionally filled by humans – logistics support, direct combat roles – the military must navigate implications for employment, training and retaining the human element in decision-making processes.

Azeem Azhar

Azeem Azhar is a writer, entrepreneur and creator of the Exponential View newsletter and podcast. He is known for his insights on how emerging technologies – such as AI, robotics, biotechnology, novel energy storage solutions and digital platforms – shape the world for the future. His concepts such as the Exponential Gap, network effects, platform economies, sustainability, agile governance and the spiky nature of global innovation and economic activity provide a new lens through which to view the evolving landscape of military strategy, operations and innovation. The Exponential Gap – the discrepancy between rapid technological growth and society's slower adaptation[57] – presents a critical challenge for military organisations. This gap necessitates that military institutions not only invest in new technologies but also evolve doctrinal, organisational and operational frameworks at a comparable pace. Azhar's advocacy for a holistic view of technology's impact underscores the importance of considering ethical, societal and environmental implications as the military integrates advanced technologies.

By fostering innovation ecosystems around military needs – using a combination of government support, academic research and private sector initiatives – the armed forces can tap into a wider array of technological solutions. The trends towards clusterisation[58] contributes to a vibrant OPEX and CAPEX cycle, where investments in cutting-edge technologies (CAPEX) are complemented by operational expenditures (OPEX) on innovation, maintenance and continuous improvement.

The intersection of sustainability and technology offers the military avenues to enhance operational efficiency and reduce environmental impact. Investing in renewable energy sources, sustainable materials and green technologies not only aligns with broader environmental goals but also supports long-term strategic resilience and operational self-sufficiency. Azhar's concept of 'spiky',[59] with innovation and economic productivity concentrated in specific urban centres needs to be emulated in the military innovation ecosystem, with focus on developing Centres of Excellence in military stations or hi-tech civilian centres. Recognising and leveraging innovation spikes through partnerships and collaborations can accelerate the absorption of new technologies into the armed forces. Aligning the military's R&D efforts with these innovation clusters enables the military to tap into cutting-edge R&D in the civilian sector, fostering a symbiotic relationship between the military and the private sector.

Balaji Srinivasan

Balaji Srinivasan is a prominent entrepreneur, investor and thinker in the technology space. He is known for his insights on the future of technology, economics and society. He has introduced concepts such as the network state[60] and favours exit over voice,[61] in Albert O Hirschmann's concepts of 'exit' and 'voice' as responses to dissatisfaction with organisations or states.[62] He is also a strong proponent of blockchain and decentralisation. Exploring some of his concepts in detail, 'network states' envisions a new form of socio-political organisations that are built on and operate through digital networks.[63] Unlike traditional nation-states bound by geographic borders, network states are decentralised, digitally native communities that form around shared interests, values or goals. These entities leverage technology to govern, provide services and interact with traditional states and each other.

Srinivasan emphasises the strategy of 'exit' – the idea of leaving or opting out of systems that do not serve one's interests in favour of creating or joining new ones. In a digital and increasingly decentralised world, the feasibility of 'exit' as a strategy is enhanced, offering individuals and communities more autonomy in shaping their environments and governance structures.[64] He also highlights the role of 'sovereign individuals' – people who leverage technology to become economically and politically independent from traditional state systems.[65] Enabled by digital currencies, remote work and global communication networks, these individuals derive their incomes from global sources, choose their locations based on personal preference rather than necessity and influence or create digital communities and marketplaces.

Translating these concepts into the military realm creates new avenues for thinking about problems. The concept of sovereign individuals has two parallel approaches within the military. The first is the strategic advantage of empowering individuals within the armed forces to act as autonomous agents in technological innovation, akin to sovereign entities operating within a larger networked ecosystem. The second is to collaborate with the brightest minds on the internet and the wider scientific and startup ecosystem to create new technologies and platforms. Here the forces must act as enablers for the development of open-source standards, software and platforms. This could involve forming specialised units or task forces (TFs) composed of highly skilled individuals who operate semi-independently, using digital platforms to coordinate and execute missions. Adopting the principle of 'exit over voice' within military R&D can lead to the establishment of parallel development tracks where traditional and unconventional projects advance simultaneously. This allows for a more diverse array of technological solutions to emerge, ensuring that the military does not become overly reliant on a singular approach or technology.

Now we will take a brief look at the principles illuminating certain movements related to modern technologies. Specifically, we will look at five, namely, techno-optimism, techno-skepticism, effective accelerationism (e/acc), atoms-not-bits and techno-realism. The totality of these movements reflects the wide schism amongst the developers regarding the potential of technology to accelerate human development and progress or contribute towards a centralisation of power and dehumanisation of society. In this divide, it is important that this book also take a stand, which is the belief that technology, especially modern digital technology, will play an outsized role in furthering the development of the human society and as an allegory, in the modernisation of armed forces. However, one will have to be very careful in delineating principles, ensuring trustworthiness of systems and finally ensuring that the design and operations of the technologies and platforms reflect an ethical way of fighting wars. With respect to the technology movements, two principles, that is, techno-optimism and effective accelerationism (e/acc), highlight the optimism towards technologies, the principle of techno-realism calls for a balanced approach while the balance two are critical in their evaluation of technologies, focusing on the 'atoms' or physical rather than the 'bits' or the digital part.

Techno-Optimism

Techno-optimism is the belief that technology can drive positive change, improve human conditions and solve complex problems. It's grounded in the idea that techno-solutionism, with its emphasis on using engineering and technology can be used to solve any social problem.[66] The idea entrenched in this movement is that technological advancements since the 18th century and starting with the Industrial Revolution have been responsible for the growth of humankind as a whole and that the use of technology is the only way forward to advance the growth of our species.[67] The main principles of this movement are: innovation for improvement, adaptability and resilience, access and democratisation, border-less collaboration and sustainability and ethical responsibility.[68] The military can take a leaf out of this movement's book. Innovation needs to be applied within the military for improvement in military effectiveness, which is defined by success on the battlefield.[69] The principle of adaptability underscores the importance of developing military forces that are flexible and resilient in the face of technological change. By investing in training programs that emphasise digital literacy and adaptability, militaries can ensure that their personnel are prepared to leverage new technologies effectively. Democratising access to cutting-edge technologies within the military can spur innovation at all levels. By fostering a culture that encourages experimentation and the sharing of ideas, the military can harness the collective creativity and expertise of its personnel.

Effective Accelerationism

This is a 21st century movement that advocates for an explicitly pro-technology stance and can be regarded as an offshoot of the techno-optimist movement. Guilllaume Verdon[70] and an anonymous X (previously Twitter) handle called Bayeslord[71] are said to be the originators of this movement, which believes in unrestricted technological progress, driven by AI, as the universal solution to problems such as poverty and war. The core aim of this movement is to climb the 'Kardashev gradient', which is a measure of technological progress by a civilisation based on its energy usage.[72] The broad tenets of this movement are: every problem must be solved online, technology and market forces are accelerating in their power and abilities, rapidly induced societal changes impacting the individual and the creation of next-generation based life forms and silicon-based awareness. In terms of principles, this movement believes in embracing technological advancement, directed progress and adaptability and resilience.[73] Applying these principles to the military leads to more focus on harnessing the potential of AI-enabled and autonomous systems, rapid prototyping and innovation and finally training and preparedness. For example, accelerating the integration of VR and AR into training programs allows for more immersive and effective preparation for real-world scenarios. Directed progress here focuses on enhancing soldier skills and readiness while ensuring that training methodologies are adaptable to future technological advancements.

Techno-Realism

Techno-realism is an approach that advocates for a balanced understanding of technology's role in society, recognising both its potential benefits and inherent limitations.[74] It emphasises that while technology can drive progress and solve problems, it also raises new challenges and ethical questions that must be carefully managed. This movement emerged as a middle ground between techno-utopianism and Luddism by critically assessing technologies as a whole so that humans had a better control over them.[75] Techno-realism suggests that a technology, however revolutionary it may seem, remains a continuation of similar revolutions throughout human history, a view very similar to the core thought of this book, which also views technology from a combinatorial and Darwinian lens. The main principles behind the movement are balanced perspective, socio-technical integration, ethical consideration, transparency and accountability and informed public engagement. When translated into the military domain, these principles translate into balancing technological capabilities with human judgment and ethics, ethical use of surveillance and intelligence technologies and a wider discourse on the role, benefits and challenges of using emerging technologies.

Techno-Skepticism

Techno-skepticism represents a cautious or critical stance towards the unbridled adoption and celebration of new technologies. It underscores the potential negative impacts, unintended consequences and ethical dilemmas that can arise from technological advancements. The core principles of this movement are critical assessment of technological impact, unintended consequences, technological dependency and vulnerability and ethical and social responsibility.[76] In terms of military applications, this refers to a critical evaluation of dual-use technologies, rigorous testing and ethical oversight while deploying new technologies, maintenance of analog backups and adhering to principles of ethical responsibility while deploying these systems.

Atoms-Not-Bits

The 'atoms-not-bits' philosophy emphasises the importance of physical goods and manufacturing over digital products and services. In contrast to trends that highlight the digital and virtual as the primary drivers of modern innovation and economic growth, the atoms-not-bits viewpoint argues for the tangible, physical world's enduring significance. Based on a series of essays and posts by Greg Satell, this philosophy believes that the digital era is ending and that it has been one of the least productive eras in applying general purpose technologies. Satell points to the mushrooming of robotics, green energy, composite materials and biotechnology hubs within the United States (US) as an example of the overshadowing of the digital by the physical.[77] He, however, acknowledges that digital technologies will still remain in the background as a foundation. Key features of this movement include tangible value creation, focus on manufacturing and infrastructure, material innovation and sustainability of physical resources. The military can take specific lessons from this movement, keeping in mind that most of these innovations have been enabled due to hyper-connectivity, sharing of data and experiences and borderless collaboration engendered by digital technologies. Some lessons are the cross mix of digital and physical technologies, for example, use of sensors on a drone fused by AI algorithms, resilience of infrastructure through a combination of physical and cyber defences, material innovation for defence and use of sustainable materials.

Now that we have looked at the works of major thinkers and movements and the theoretical implications for military organisations, it is important that critical insights and foundations for further discussion on these issues be distilled from these writings.

- The foundation of technology is based on the adaptation and integration of existing technologies. Technology is a system of interconnected parts and needs to be understood as having evolved from a system of combinatorial evolution. This means that in the military, the basic building blocks of a technology have to be carefully analysed for future permutations and combinations. Various mixes and innovations on a foundational layer of technology can lead to new capabilities. Whether this is commercially available off the shelf (COTS) or part of an indigenous system, both need to be integrated for building disruptive capabilities.

- Technology also deepens structurally, that is, becomes complex over time as more parts, abstractions and layers are added and built over it. Once procured for the military, it becomes important to preserve the intellectual property, and also to encourage in-house innovation with adequate institutional memory. Additionally, technological evolution requires modularity, which is only possible by standardisation – of components and constituent technologies. For example, use of multiple categories of drones operated by the three armed Services of a country (traditionally the Army, Navy and the Air Force) need to be able to 'speak' to each other, therefore standardisation in communication protocols is the bare minimum requirement.
- Technological revolutions can be predicted with a fair degree of regularity due to the 'S' shaped nature of their growth and demise. As a result, CAPEX and OPEX cycles of major technologies need to be analysed in detail. One of the preconditions is to differentiate between technologies requiring CAPEX and OPEX, with the former for comparatively premature or on the horizon technologies and the latter for already proven and diffused ones and where add-ons and innovation layering is required.
- Mere technology in itself is not disruptive, but its use can be. Regular organisations indulge in sustaining innovations that are incremental in nature and are essentially an upgrade of an existing platform. The process of innovation in militaries is that of the sustaining one. However, what the literature on disruptive technologies argues for is the focus on utility and outcome (i.e., effects and ends in military terms) rather than the product attributes (or the means). A major

change required is to shift focus from platforms and technologies to capabilities. For example, one needs to define capabilities such as long-range firepower, precision effects, space-based C4ISR, cross-terrain mobility and individualised miniature aviation etc. This needs to be the foundation and will obviously be informed by the threat scenario and a national security and defence strategy, written or unwritten. Once the requirements are clear, one can start finding, inventing and absorbing new technologies.

- The process of digitisation and computation forms the backbone of major societal reorganisation and restructuring. This has impacted militaries, which cannot insulate themselves from the positive and negative effects of these technologies.There will be an inherent time-space compression in the application of military capabilities on the broader battlefield. The overarching digital nature of ICT also makes obsolete the conception of limited battlefields, which can now stretch directly into the heartland of the adversary.
- The inherent nature of digital technology is horizontal and non-hierarchical. This leads to the concepts of 'flattening' and 'spreading' in government organisations, which includes the military. As most digital technologies have been designed with the aim to create a horizontal distribution of specialised work and a collaborative mindset, government bureaucracies must either reorient and restructure themselves or adapt the technology to suit the organisation. This leads to one of two things: either technology itself is designed or used in a manner that mirrors/replicates the daily routines of administrative manners or the bureaucracy 'flattens' and 'spreads' over a period of time. Flattening and spreading in relation to the armed forces can be thought of as sequential processes. While 'flattening' is part of the cognitive realm and refers to the breaking of silos and acceptance of a more open and collaborative model of functioning, 'spreading' is the physical counterpart when the actual coordination between departments happens.
- Militaries must leverage decentralised digital networks for enhanced operational agility while ensuring investments in physical infrastructure and capabilities, blending the strengths of both digital

and tangible assets for operational advantage. They must foster open and collaborative innovation ecosystems, emphasising the importance of cross-sector partnerships and real-world applications of digital advancements, all the while ensuring that technology is used for practical and strategic military needs.

- Militaries should cultivate an environment of continuous learning and adaptability, recognising the fast pace of technological change and the importance of upskilling and resilience among military personnel.

The themes that emerge clearly from this detailed exposition on the absorption of emerging technologies in the armed forces is the focus on organisation, doctrine and leadership. This needs to be kept in mind since absorption of new technologies also implies importing certain inherent characteristics of the technology itself. This fact is generally ignored due to a misconception that technology in itself is neutral. Technology always reflects the milieu in which it was created, the predilections of its creator(s) and is never neutral. To understand and analyse technology, therefore, requires leadership of a different calibre, more so in an environment where the deployment and use of technologies is linked to physical casualties of individuals and the survival of nation states.

The last decade has witnessed an unprecedented explosion in digital technologies, propelled by three key forces: Moore's Law delivering exponential computing power at declining costs, global communication infrastructure including vast undersea cable networks and Silicon Valley's innovation-driven capitalism. This convergence has created an environment where virtually anything can be digitized – converted into binary code that can be manipulated, analyzed and transformed through computation.

Computation encompasses data processing, algorithm execution and pattern recognition, but its real power emerges when applied to human experiences. Consider modern digital reading platforms: these sophisticated systems don't merely track basic reading metrics but build comprehensive user models through multi-layered data analysis.

A state-of-the-art reading platform might incorporate sensors that detect environmental conditions, time-of-day patterns and even physiological responses like eye movement patterns and reading posture. It analyzes not just what one reads but how one engages – pauses, highlights, passages shared and abandoned books.

On the content side, advanced natural language processing examines linguistic patterns, narrative structures and emotional arcs within texts, going far beyond basic metadata like genre or length. These systems might identify that a reader appreciates complex character development in historical fiction but prefers fast-paced narratives in thrillers.

The platform integrates social signals, noting when recommendations from friends lead to engagement and identifies communities of readers with similar tastes. It adapts to changing preferences over time, recognizing when a reader's interests evolve from one subject to another.

Most importantly, this ecosystem operates across modalities – recognizing when a user might prefer an audiobook for their commute but an e-reader before bed – and builds a holistic understanding of reading habits that spans devices and formats. The result is a deeply personalised experience that not only recommends relevant content but delivers it in the right format, at the optimal time, in service of the reader's evolving relationship with literature.

As mentioned above, this has been made possible due to the confluence of three events and breakthroughs. The first one, that is, Moore's Law, which was an observation by Intel co-founder Gordon Moore in 1965, that the number of transistors in a computer chip doubles every two years or so. The 'law' further postulates that as the number of transistors increase, the cost per transistor falls.[79] As a result, electronic devices have become powerful, smaller and accessible to increasing number of ordinary people. Initially limited to government agencies such as the military and meteorology department and certain laboratories of academic institutions, much more powerful computing devices are in the hands of ordinary citizens today.[80] A brief survey of the computing history will bear this out.

As per acclaimed futurist Ray Kurzweil, there have been four computational paradigms before the current or the fifth one. The first generation, which roughly spanned 1940 to 1956, consisted of vacuum tubes. The best analogy will be to imagine huge machines with glass tubes, like light bulbs, used to process information. These were the first computers, using vacuum tubes for circuits. They were powerful for their time but very large, consumed a lot of electricity and generated a lot of heat. The second generation comprised transistors and roughly spanned the time period of 1958–83. These transistors were like tiny switches turning on and off for computations, making computers smaller, faster and more reliable. The third generation from 1974 to 1981 was of the Integrated Circuits or ICs, where many transistors were put onto a single chip. This significantly reduced the size of computers and increased their speed and capability like packing an entire electrical circuit into a small pill. After that, in the fourth generation (from 1982 to 2010) microprocessors dominated the scene, which are essentially entire computers on a single chip. This made computers even more powerful and compact, leading to the birth of personal computers (PCs). The current generation or the fifth computational paradigm that started in 2010 and continues till date, is of Graphics Processing Units (GPUs) and multi-core processors.[81] These are like having many microprocessors working together, allowing computers to perform complex tasks, such as AI and advanced graphics, much faster and more efficiently than before.

Innovation in ideas, processes, engineering and business models has led to two major trends which, though breakouts in their time, are now considered as routine. The first one is the creation of sensors that can capture any physical phenomenon and convert it into digital data, for example, digital cameras, pulse rate meters, capacitive screens, gyroscopes, infrared (IR) and hyper-spectral cameras, among others. Since computers do not have an internal understanding of physical phenomenon but possess a computing capacity exponentially higher than that of humans, the interjection of a sensor between the human and his physical environment, creates a 'understandable' or machine-readable copy of this interaction – that between the human and his surroundings, which includes action, impact and reaction by both actors, that is, the human and his physical surroundings. This computed interaction is processed at extremely high speeds; the common terminology is that of floating-point operations per second (FLOPS),[82] which is used to predict, extrapolate and after the advent of generative AI, create new structures and ideas. The generated output can assist in planning in granular details.

Take, for example, the smartwatch or health monitoring device worn on the wrist. The device is essentially a mix of sensors, advanced chips and accompanying software. It can measure your heart rate, pulse, oxygen content and even inform the nearest hospital if there is a likelihood of the individual having a cardiac event. All these are available as interactive graphs and figures to the individual at the touch of a finger. This provides him real-time instant feedback on all the possible health parameters in a non-invasive manner. The device also suggests actions such as breathing, drinking 'x' glasses of water per day or taking 'y' number of steps to ameliorate any particular symptom such as an elevated heart rate. The use of this device, obviously, does not obviate the need to refer to a doctor in case of discomfort but it does help provide a detailed feedback on certain health parameters that were out of reach of so-called non-specialist ordinary citizens a few years back. Using a computation device quantifies the self and creates manipulable parameters that can be analysed and optimised to generate prediction and extrapolation products. Taking this to an extreme, there is a category of 'bio-hackers' who use a mix of bio-markers and AI techniques to optimise their health and well-being.[83]

Similarly, sensors used in the agriculture sector include electrochemical ones for measuring soil and water parameters and detecting nutrient levels, temperature sensors for monitoring plant temperatures, livestock monitoring sensors, tensiometer for measuring soil moisture status, generating field maps and airflow sensors for spray only a selected portion of the field.[84] Here the various parameters of agriculture are quantified using sensors and the output presented to the users in such a manner to highlight even the most sensitive and in-depth readings and analysis of the soil and food production ecosystem. The second trend is the intermixing of physical domains mediated by sensors and computation to create products that span inter-phenomena boundaries. This has led to a situation where technologies in their disembodied form are looking at platforms to carry them into different physical environments. These two trends indicate that technological advancement is set to and is increasing exponentially. It is under these circumstances and the unprecedented rate of growth of technology that one needs to look at the concepts of innovation and technology absorption in military organisations.

Situating Technology Absorption and Innovation

A voluminous literature exists for defining and typifying technology absorption and innovation in general, and there is a significant overlap with military organisations. This book offers a new model of technology absorption by building on concepts of innovation in the national security arena given by Tai Ming Cheung, Andrew Ross and Tom Mahnken, overlaid with concepts of technology absorption by Paul Oling, Martin Lundmark, Michael Raska, Brian Jackson, Kogila Balakrishnan, Jodie Kaye Stevens and Yantsislav Yanakiev. This model categorises innovation into three parts, that is, strategic, military and defence innovation, and argues that though contemporary wars may show a preponderance of defence innovation in certain battles and encounters, without a long-term strategic and an intermediate-term military innovation policy in place, defence innovation in itself will never be disruptive or bring about a change in military effectiveness. For this to take place, not only are certain policy changes required, but also an appreciation of what it takes to create true innovation that is absorbed by the military of the particular country.

What is Military Innovation?

Military innovation has been defined in multiple ways. These include how militaries fight as compared to a pre-existent format;[85] combining and utilising existing technologies and procedures in novel ways;[86] broad[87] or piecemeal process[88] and successful application in affecting change.[89] Many variations on these themes do exist. For example, some contest whether innovation is horizontal,[90] top down[91] or bottom up.[92] However, for most in the field, there are three common attributes that establish whether a change is an innovation: change in the manner a military functions in the field; whether it is significant in scope and impact; and whether it leads to greater military effectiveness in whatever manner it is calculated.[93]

Military innovation is said to comprise four schools of thought, primarily civil-military relations, inter-service politics, intra-service politics and organisational culture. Apart from these schools, there are five views on military innovation. The first is technological determinism; it highlights the role of technology as a primary driver of military innovation. This has been stated by Michael Horowitz in his work on military diffusion where he argues that the adoption and integration of new technologies by military forces can significantly alter the balance of power between states.[94] His viewpoint is rooted in technological determinism, suggesting that only technological advancements lead to changes in military tactics, operational capabilities and strategies. He also delves into factors that facilitate or hinder the diffusion of military technologies across nations. The second view reflects an organisational theory aspect and has generally been associated with Stephen Rosen. Rosen contends that innovation is not just about technology but involves significant changes in military organisations, including doctrine, training and leadership. According to him, the most significant innovations occur when military organisations are willing to undergo profound internal changes, challenging traditional hierarchies and doctrines to adapt to new technological realities and strategic demands.[95]

Eliot Cohen propagates the third view, which prioritises civil-military relations for military innovation. In his influential book *Supreme Command: Soldiers, Statesmen and Leadership in Wartime*, Cohen highlights the critical role of civil-military relations in fostering or inhibiting military innovation. He argues that effective political leadership and a healthy dialogue between civilian policymakers and military leaders are crucial for successful innovation, and proposes that civilian leaders, who often bring a broader strategic perspective, play an essential role in pushing military organisations to innovate and adapt.[96] Encapsulating the fourth view, John Arquilla and David Ronfeldt, in their widely acclaimed paper *Cyberwar*, emphasised the importance of information and networked structures for military effectiveness. The future of military innovation, as per them, lies in leveraging information technology (IT) to create highly adaptable and decentralised networks of forces, enhancing situational awareness, speed of command and precision in operations.[97] This perspective suggests that innovation is increasingly found in how forces are organised and communicate, rather than solely in technological hardware.

Finally, Andrew Krepinevich formulated the theory of revolution in military affairs (RMA), based on the assumption that certain periods in history witnessed shifts in warfare based on the convergence between new technologies, military strategy and organisational changes. Krepinevich was of the view that these moments needed to be identified by military forces in order to learn from them and increase military effectiveness.[98] Apart from these thinkers, certain practitioners have stated their views on what military innovation is. Israeli Chief of General Staff Lieutenant General Aviv Kohavi in 2021 stated that innovation was not about ideas but the ability to perform, execute and deploy.[99] Only those ideas that could be deployed on the battlefield and perform successfully could be termed as military innovations. This suggests a practical side to the idea of military innovation. Ideas that are new yet proven practical either through repeated tests or through a spiral development process – battlefield and back in an iterative fashion – should be considered. Then there is the question of training, techniques and tactics and the diffusion of the technology as a whole across the organisation, in addition to the pricing. All these issues are practical parameters that need to be thought of in detail when considering the concept of military innovation.

Tai Ming Cheung has introduced multiple terms to conceptually define defence innovation and, in the process, differentiate it from strategic and military innovation. As per him, defence innovation is the 'transformation of ideas and knowledge into new or improved products, processes and services for military and dual-use applications'.[100] Defence innovation manifests in various organisations and activities associated with both defence as well as related civil institutions and industry that use their respective expertise for contribution to R&D in the defence sector. Military innovation, on the other hand, is a more expansive concept that focuses on warfighting innovation or increasing military effectiveness on the battlefield. It encompasses both 'product innovation and process innovation' as well as 'technological, operational and organisational innovation'.[101]

Paradoxically, in terms of the actors involved, the roles are reversed. While defence innovation involves both military and civil individuals and institutions, military innovation concerns itself only with the military. The third category is that of strategic innovation. While not defined explicitly by Cheung, in the field of national security it refers to a broad national orientation that views the use of science and technology (S&T) and innovations to either overturn or perpetuate a state of technological superiority over a near contender.[102] Strategic innovation can be interpreted through several means and can be either coercive or constructive or a combination of both. One of the best examples of strategic innovation is the use of sanctions and regulations by the US to stop China's technological advancements in certain fields (coercive),[103] promote on-shoring (also called friend-shoring) of components involved in according technological leverage to the US back to the mainland,[104] providing subsidies and incentives for startups and academia to keep innovating within the country such as the Inflation Reduction Act (IRA)[105] and an Executive Order by the US President on the responsible use of AI[106] (constructive).

Cheung enunciates seven categories of the factors involved in the defence innovation process: catalytic factors (e.g., highest level intervention by the political class); input factors (material, financial, technological etc); institutional factors (rules, norms, established practices etc); organisations and other factors (companies, academia, military units, formation HQ, Services HQ, bureaucracy etc); networks and subsystems (social, professional, virtual networks etc); contextual factors (factors shaping the defence environment); and finally, output factors (production process, commercialisation, market forces etc).[107] Types of technological regimes have been defined based on different combinations of the relationships between these factors. Of the four, namely, incremental catch-up regimes, rapidly catching up regimes, advanced developed regimes and emerging technological domains,[108] India has been categorised in the first group, that is, an incremental catch-up regime. This type of regime can lead to four different types of innovation, which are creative imitation, creative adaptation, crossover innovation and incremental innovation.

Very briefly, creative imitation results when there is low R&D within the domestic system, but even this low level of R&D can result in improvements in components and non-core areas. Creative adaptation occurs when platforms take inspiration from foreign ones but differ in their characteristics and performance parameters in significant areas. Crossover innovation starts with a joint venture between a foreign and direct firm and can result in the creation of an R&D base, which can start innovating but will still depend on foreign support in the technology and managerial realm. Finally, incremental innovation is a condition where there is a limited updation in existing indigenous systems and platforms.[109] Cheung's use of these categories is helpful for forming a part of the book's analytical structure, though his categorisation of India in the incremental catch-up regime does not take into account the exponential power of new and emerging technologies, where India has gained a step ahead of a number of other countries. Extrapolating Cheung's three categories of strategic, military and defence innovation and using examples from contemporary wars, it becomes clear that the three categories form a linked and layered model of innovation, details of which will be explained later.

Before starting with the 'how', it is necessary to justify the 'why'. Why does the Indian military need a new framework for technology absorption? If this need is justified, the process and framework duly follow. The process of technology absorption is a long and nuanced one and involves multiple stages. It starts with a felt need for a change – either in the organisational hierarchy, C2 processes or the technology. Once a felt need has been identified, a military organisation then needs to analyse the domains that will benefit from military innovation in order to improve military effectiveness on the field. Identification of the domain will lead to the initiation of the two parallel processes of defence and military innovation, which will seek to change the organisational, doctrinal and technological thresholds of the organisation. This is also known as change management,[110] which has to be done in a manner that must build on the TAC of an organisation, improving and increasing it in steps.

The TAC is a combination of organisational ambidexterity (OA) and intellectual capital (IC) – itself a combination of human, structural and relational capital. The ambit of TAC can be expanded by increasing the VRIN factor (valuable, rare, inimitable and non-substitutable resources) through improving IC.[111] An organisation's OA refers to its ability to balance between innovation or exploration and exploitation or market capitalisation. In military terms, the organisation has to balance between innovation and applying products of that innovation to enhance military effectiveness. The evolution of major military innovations often triggers a dilemma between the aspirations and apprehensions within military organisations, encapsulating the ongoing struggle between the attraction of decisive and cost-effective victories or catastrophic defeat. This dynamic underscores a fundamental shift towards OA in military contexts, where the capacity to exploit existing competencies while concurrently exploring novel domains becomes paramount. Such ambidexterity is critical as armed forces navigate the dichotomy between their visions of dominating new and existing battlefields – naval, aerial, space and cyberspace – and the pragmatic challenges of integrating these advancements into multi-domain strategies.

The introduction of new capabilities and foray into uncharted domains invariably introduce substantial wartime friction, reflecting a deeper need for an organisational structure that is both adaptable and resilient. This requirement aligns with the VRIN framework, emphasising the importance of cultivating military resources and capabilities that are valuable, rare, inimitable and non-substitutable. Innovations that promise comprehensive victory underscore the strategic imperative for resources that not only offer a competitive edge, but are also deeply embedded within the fabric of military doctrine and logistical support systems. Moreover, the emergence of new domains of warfare necessitates a recalibration of strategic postures – from a focus on territorial defence to asserting military dominance. This strategic pivot elevates the role of intellectual capital within military organisations, as the knowledge, skills and innovative capacities of personnel become critical in harnessing the potential of new technologies. The ambition to ensure freedom of movement within a given domain while denying the same to adversaries has historical antecedents in the construction of blue water navies and the development of strategic air forces, underscoring a consistent strategic logic despite the changing technological landscape.

Addressing the infrastructural and logistical underpinnings required to sustain advancements in new domains further highlights the interplay between VRIN resources and organisational effectiveness. The challenges of adapting to new operational imperatives reflect underlying organisational issues, where the complexity of unstructured problems demands a sophisticated blend of intellectual capital and strategic resource allocation. The path towards bureaucratic restructuring and the inevitable internal struggles for resources and authority it engenders point to a broader narrative of institutional adaptation and reform. This narrative is linked to the concept of organisational ambidexterity, where the balance between exploiting existing capabilities and exploring new opportunities is constantly negotiated against a backdrop of internal and external pressures.

In the realm of new warfare domains, the speculative nature of combat effectiveness and the resultant unpredictability of confrontations underscore the critical role of intellectual capital. The capacity to innovate, adapt and anticipate in the face of uncertainty becomes a pivotal element of military strategy, transforming intellectual capital into a cornerstone of organisational resilience and strategic foresight. At its core, military advancement is an endeavour to minimise uncertainty, aiming to refine strategic and operational foresight to the highest degree of precision. This endeavour goes beyond the mere acquisition of new hardware and consists of a systemic transformation where knowledge creation and the dissemination of technological insights become integral to enhancing combat effectiveness and operational agility.

Production of knowledge and the integration of emerging technologies are not linear processes but are characterised by continuous evolution and adaptation. This dynamic underscores the necessity for military organisations to not only generate new strategic doctrines and operational practices but also ensure that these innovations can be efficiently transmitted within and across units. The effectiveness of this transmission hinges on the establishment of robust communication channels and the presence of adept science communicators who can bridge the gap between complex technological concepts and their practical military applications. Also, the process of technology absorption in the military is significantly influenced by the organisation's culture and structure. A culture that fosters innovation and adaptability, supported by a structure that facilitates swift decision making and the flexible allocation of resources is crucial for the timely integration of new technologies. However, inherent biases toward existing operational paradigms and the challenges of managing change within hierarchical and tradition-bound institutions often pose significant hurdles to technological absorption and innovation.

Change management within the military, therefore, is not merely about introducing new technologies but involves a comprehensive overhaul of existing doctrines, training protocols and command structures. It requires a concerted effort to cultivate an environment where experimentation is encouraged, and failures are viewed as stepping stones to valuable learning experiences. Such an environment is essential for fostering a culture of continuous improvement and for maintaining strategic and operational superiority in an evolving technological landscape. In order to create such an environment, it is equally important to move on to the third leg of the absorption process, which is to look at the work of contemporary scholars of military studies on the concept of absorption within militaries.

Paul Oling, using a case study of the Netherlands's Armed Forces' experience in countering improvised explosive devices (IEDs) through the use of emerging technologies in Afghanistan and Mali, focuses on the cultural traits of military organisations and how a military's organisational culture shapes the way a particular military absorbs technologies. He singles out three factors: 'innovation drivers throughout the absorption process'; 'distinction between a hot situation during military operations and a cold situation in periods in-between conflicts'; and 'gradual shift of organisational identities'.[112] The Dutch Army used an 'isomorphic' approach where soldiers and non-commissioned officers searched for innovative solutions in both a horizontal and vertical manner near simultaneously, that is, not only did they reach out to fellow soldiers in the British Army facing similar challenges but also to peer NCOs in other Dutch units deployed in Afghanistan. They also petitioned their senior officers to institutionalise certain ad-hoc measures that were proving effective in countering IEDs in the theatre.[113] As this case study and its analysis show, innovation drivers differ from situation to situation, however there are certain commonalities such as external shocks in the form of a conflict or hot war, where bottom up innovations need to be institutionalised and leadership has to ensure that the ad-hoc procedures are sharpened and formalised in doctrines.

There is also a need for in-built flexibility within a military organisation that can morph its structure to counter novel challenges. Martin Lundmark, in his policy brief on acquiring and absorbing new military capabilities in the context of the Indo–Pacific calls for these countries to follow a 'realist' policy of being technology followers and 'not formulate unrealistic ambitions that are not matched by domestic qualities and size of their defence innovation system, and of accessible financial resources'.[114] Though this brief advances the policy aims of Sweden as a major military technology power and calls for increasing its export potential, the bent of this paper shows that India must improve its own defence innovation ecosystem by leveraging the comprehensive network of multiple innovation organisations in the S&T arena spread across the length and breadth of the country.

Kogila Balakrishnan, using a case study of defence automotives for enhancing land-based capabilities of the military, pens down the challenges involved in ensuring adequate absorption of automotive technologies. She identifies three parameters that will dictate the future of these technologies, namely, the changing nature of land-based warfare, increasing burden of energy security and finally mitigating environmental challenges. The broad categories of technologies required for military automotives are lightweight materials, energy storage and management, additive manufacturing and hybrid-energy technology. The implementation challenges are non-matching with military standards, lack of civil-military integration and affordability of products with emerging technologies.[115] The solutions offered are to adopt a dual-use technology strategy, encouraging open innovation ecosystem by the government and offsets.

Brian Jackson uses case studies of absorption of technologies by commercial organisations to predict how terrorist organisations may acquire and absorb technologies. Starting with the concepts of internal and external innovation, two routes are depicted for commercial organisations, which deal respectively with application and acquisition.[116] However, a more nuanced difference is that between explicit and tacit knowledge, with the former standing for transferrable and codified blueprints and the latter for the specific knowhow embodied in the processes, norms and the intellectual capital of a firm. Tacit knowledge is resistant to transfer. Jackson compares a hypothetical successful terror organisation to a small, hi-tech firm (startup in contemporary terminology) and lists down the conditions that make the acquisition for such an organisation likely: 'not formulate unrealistic ambitions that are not matched by domestic qualities and size of their defence innovation system, and of accessible financial resources'. This is reinforced with 'necessary human resources, collaborations with sources of technology that transmit both tacit and explicit knowledge, appropriate leadership and structural support, and an environment that provides both enough pressure to force the firm to try many technology experiments and enough leisure to learn from […] results.'[117]

Yantsislav Yanakiev and his team while analysing results using the European Union's (EU's) Predictive methodology for TecHnology Intelligence Analysis (PYTHIA) regarding technology absorption conclude that emerging technologies have different effects on different levels of strategy, with the most powerful one being at the grand strategy and strategy levels.[118] When it comes to the operational and tactical levels of warfare, these technologies lead to innovative approaches in planning and carrying out operations and the modernisation of TTPs. The authors further contend that the interaction between defence strategy and technology development and consequently absorption have a mutually reinforcing effect on each other.[119] Disruptive technologies influence the development of defence strategy, while a dynamic strategic environment needs disruptive technologies to achieve the goals of a particular country.

Michael Raska, on the other hand, is agnostic about the impact of breakthroughs in the domain of emerging technologies on military effectiveness, stating that their 'comparative advantage could be both significant and hard to predict at their nascent stages'. He conceptualises three axes along which the study of defence innovation and absorption needs to take place, that is, conceptual paths (emulation, adaptation and innovation); technological patterns (speculation, experimentation and implementation); and organisational change (exploration, modernisation and transformation).[120] He emphasises the role of strategic, organisational and operational adaptability in absorbing technologies, which for him are a combination of 'changing military posture quickly and easily in response to shifts in geo-strategic environment, military technology, resource allocation, organisational behaviour, and national priorities'. This is to respond to emerging situations that may not take the form of conventional warfare but grey zone operations and where the impact of disruptive technologies may be more pronounced.

Finally, Jodie Kaye Stevens uses a case study of the Australian Army's ability to use mobile apps for training and learning to explain the barriers and enablers for technology absorption in a military organisation. Tactical factors for the absorption of a particular technology are explored and discussed in detail. These are: 'Get in, get out, get what you need; Value add potential; Blurred boundaries; Digital assumptions; Technology, traditions, tensions'.[121] These are important issues from the point of view of a soldier or user when it comes to using or absorbing technological artefacts related to emerging technologies. If one amalgamates the observations from these academic studies, it is evident that military organisations across the world need to restructure their intellectual processes as well as horizontal integration linkages with the government, industry and academia. The need for institutionalisation of bottom-up innovation is dire and this can only be recognised and fulfilled when the senior leadership of the armed forces recognise the importance and criticality of emerging technologies.

Analysis of Studies

These important papers and studies offer multiple perspectives on how change management in the military, especially in the case of digital technologies, can be visualised. Certain takeaways are mentioned below.

Organisational Culture and Adaptability

The ability of military organisations to absorb new technologies is heavily influenced by their organisational culture. The capacity for strategic, organisational and operational adaptability is crucial in effectively integrating emerging technologies. The isomorphic approach of the Dutch Army was made possible due to its embedding within the larger North Atlantic Treaty Organization (NATO) framework. This model may not work for others. However, there is a case for a more open and open-source based innovation system that can leverage knowledge networks. This theme finds a lot of traction in the works of a majority of scholars quoted in the initial sections. The next point is regarding the institutionalisation of ad-hoc measures seen to be practicable on the battlefield. This is an important point and has a wider impact. Most militaries engaged in operations resort to the use of ad-hoc measures or battlefield innovation when faced with challenges not catered for in any contingency planning. These are generally context specific and are discarded in peacetime. However, in the case of absorbing emerging and disruptive technologies, it becomes important to institutionalise the thinking behind the deployment of these technologies on the battlefield. There are two advantages to this. Firstly, these procedures and deployment patterns are more likely to be absorbed once their utility has been proven in ground operations. Secondly, the very nature of these technologies and the kinds of future challenges faced will force militaries to apply new thought methodologies, especially based on an engineering and technological mindset, helmed by 'first principles'. The organisational culture will also need to change to facilitate this mindset. This is evident in Paul Oling's study of the Netherlands Armed Forces and Michael Raska's emphasis on adaptability.

Multi-level Impact of Emerging Technologies

Emerging technologies have varying effects at different strategic levels. As highlighted by Yantsislav Yanakiev's team, these technologies have the most significant impact at the grand strategic and strategic levels, while leading to innovative approaches in planning and execution at operational and tactical levels.

Realistic Approach to Technology Absorption

Martin Lundmark's policy brief suggests that countries, especially in the Indo–Pacific region, should adopt a realistic approach to acquiring and absorbing new military capabilities. This involves aligning ambitions with domestic innovation ecosystems and available resources, which is particularly relevant for countries like India. While he emphasises that most countries should be technology followers, his policy recommendations should be extrapolated and abstracted to get a bigger picture and implementation options for the Indian military. A limited defence capital budget will require inter-se prioritisation between multiple promising technologies and their uses. With so many options on the table, it is necessary, especially for the military, to see which technology can be explored for further development and deployment, and which can be developed with assistance and partnerships with civilian counterparts as a joint project, which may end up as a proof of concept.

Challenges in Technology Implementation

Kogila Balakrishnan's study on defence automotives identifies several challenges in technology absorption, including mismatches with military standards, lack of civil–military integration and affordability issues. These challenges underscore the complexity of implementing emerging technologies in military contexts.

User-Centric Considerations

Jodie Kaye Stevens' case study of the Australian Army's use of mobile apps for training highlights the importance of considering tactical factors and user perspectives in technology absorption. Factors such as ease of use, value addition and compatibility with existing traditions and tensions play a crucial role in successful technology integration at the user level.

These takeaways emphasise that change management in the military, particularly concerning emerging technologies, requires a comprehensive approach that considers organisational culture, strategic alignment, realistic capability assessment, implementation challenges and user-centric design. In the next section, we will study the defence innovation ecosystems of three countries – the US, Israel and Ukraine – in detail. But before discussing the case studies, it is important that the concept of technology readiness levels (TRLs) be discussed in some detail.

The TRL levels are:

- **TRL 1**: Basic principles observed and reported.
- **TRL 2**: Technology concept and/or application formulated. Funding Sources are self-funding, grants and fellowships from government bodies and non-profit organisations as well as early-stage research grants from the government. Focus is on exploration of basic principles and initial concept formulation.
- **TRL 3**: Analytical and experimental critical function and/or characteristic proof of concept. Funding sources are government research grants, university funds and early-stage incubators that offer seed funding. The focus is on the development of experimental proof of concept in a laboratory environment.
- **TRL 4**: Component and/or breadboard validation in a laboratory environment.
- **TRL 5**: Component and/or breadboard validation in a relevant environment. Funding sources are advanced government grants, angel investors and incubators with a focus on specific technologies or portfolios. Participation in challenges and competitions can also provide non-dilutive funding (refers to financing methods that allow companies to raise capital without giving up equity or ownership). The focus is on validation of technology in a lab and then in a simulated environment. This is a critical phase where incubators and specialised accelerators play a significant role in providing both funding and technical resources.
- **TRL 6**: System/subsystem model or prototype demonstration in a relevant environment. Funding sources are angel investors, early-stage venture capital and government programs designed to support scaling technologies. Some government-backed loans may also be available. The focus is on demonstrating the technology in a relevant environment, which is often outside the lab. This stage aims to prove the technology's feasibility in real-world conditions.
- **TRL 7**: System prototype demonstration in an operational environment.
- **TRL 8**: Actual system completed and qualified through test and demonstration. Funding sources are venture capital, strategic investors

and corporate partnerships. Advanced government grants aimed at commercialisation can also be pivotal. The focus is on the development and demonstration of prototype systems in an operational environment. At this stage, the product is nearly or fully functional and the startup is likely engaging with potential customers and partners.

- **TRL 9**: Actual system proven through successful mission operations. Funding sources are growth-stage venture capital, private equity and debt financing. Revenue from early adopters and strategic partnerships can also support scaling at this stage. The focus is on technology maturation and commercial viability. The company focuses on scaling up, market expansion and possibly exploring international markets.[122]

Going from a technical paper on a new concept to a product prototype can be divided into two parts. The first is basic R&D, which is when research is being done to see if a concept on paper can be converted into a working prototype with some application for a particular user category, and the second is product R&D, which is when the first stage has been completed and proof of concept demonstrations have taken place. Most startups receive funding to take their program from a tech-concept (TRL 2) to component or system validation in a lab or a controlled environment (TRLs 4 & 5), that is, completion of the first stage. However, this funding is not adequate to cater for moving higher up the TRL, that is, TRLs 6–9, which require commercial support for transitioning the technology from a concept to a product.

Startups are assumed to be at the cutting edge of technological development and there has been a pronounced effort to fund and support them across countries. It is therefore necessary for the reader to understand how exactly a startup is funded so that future descriptions and details can be easily grasped. The route from an idea to a product by a startup consists of multiple steps, starting with ideation and market research. Here one needs to define his/her innovation, outline the technology or product, its unique value proposition and the problem it solves. A concurrent part of this first step is to also conduct market research to understand target market, potential customers and competitors. This step is crucial for validating a business idea. Next is the prototype stage where one develops a working prototype. This demonstrates the feasibility of the product or technology and is critical for startups to attract initial interest and funding. After this comes the step of engaging with incubators and accelerators. These offer mentorship, resources and sometimes, seed funding. They can help refine business model, develop product and prepare the startup founders for investor interactions. The role of incubators and accelerators is to provide a nurturing ecosystem, including workspace, mentorship, access to a network of investors and exposure to industry partners.

One of the most important steps after this is to look at the seed funding and government grants. These grants are ideal for early-stage funding without diluting equity. This is supplemented by bootstrapping, where one uses personal savings or funds from friends and family (known colloquially as an F&F or friend and family fund) to get the startup off the ground. This stage is crucial for demonstrating commitment to potential investors. After this step comes the process where a startup looks for angel investors and VC funding. Angel investors typically come in after the development of a prototype and some validation of the startup's market potential. They can provide valuable capital, mentorship and networking opportunities to help scale the business. Once the startup has started showing significant growth potential and market traction, one can approach VC firms specialising in tech investments. VCs come into play for larger funding rounds and can provide significant resources and expertise to help scale up the startup's business. This is also the early-stage valley of death (VoD), which occurs typically after the seed stage and before achieving significant market traction. After this is the Series A funding rounds and beyond. After successfully utilising angel investment and seed funding to prove a business model, enter markets and begin scaling, the startup will be in a position to seek larger funding rounds (Series A and beyond) from VC firms to accelerate growth. The penultimate step is to undertake continuous innovation and look for a market fit. One must iterate based on feedback and continuously improve products based on user feedback and market needs. Staying agile and responsive to market demands is key to long-term success. This is also where the startup encounters the late-stage VoD, which occurs when a startup has achieved significant growth and market traction but requires additional funding to scale operations, expand into new markets or achieve profitability.

We now move to the next chapter of defence innovation ecosystems where three countries are studied in extensive detail. There is a reason why only these countries have been considered. The US has the most extensive defence innovation ecosystem in the world with in-depth interlinkages with the industry, bureaucracy and academia. It serves as a foundational ideal and as a case of 'what-if' there are relatively few limits on military spending. The second case study is that of Israel. This country is known as an innovation powerhouse under comparatively restrained financial conditions. Also, the state of constant war that the IDF finds itself in, is unique in that the country and its armed forces are constantly developing and innovating new technologies. Being a middle power, it has several lessons for countries such as India. Finally, the third country being discussed is Ukraine. This country's experience in innovation is unique in many aspects: it is currently fighting a war against a much bigger and technologically sophisticated adversary; innovation and absorption is being spearheaded by civilian entrepreneurs; it is a relatively low-income country; and finally, it is an interesting case of how quickly a country's armed forces shift systems (from ex-Soviet and Russian to the NATO). Taken together, these countries provide a wide spectrum of the kind of defence innovation and absorption taking place across the world. The Indian military can take multiple lessons from these militaries.

NOTES

[1] W Brian Arthur, "Inductive Reasoning and Bounded Rationality", *The American Economic Review*, 84(2), May 1994, pp. 406–11.

[2] W Brian Arthur, *The Nature of Technology: What it is and How it Evolves?*, Allen Lane, Penguin Books, London, 2009, p. 103.

[3] Ibid., p. 49.

[4] Ibid., p. 185.

[5] Ibid., p. 135.

[6] Ibid., p. 39.

[7] W Brian Arthur, *Increasing Returns and Path Dependence in the Economy*, University of Michigan Press, Ann Arbor, 1994, pp. 1–10.

[8] W Brian Arthur, no. 3, pp. 139–43.

[9] Carlota Perez, *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages*, Edward Elgar Publishing, Cheltenham, United Kingdom, 2002, pp. 5–7.

[10] Ibid., pp. 8–11.

[11] Ibid., pp. 47–7.

[12] Tom Nicholas, "Why Schumpeter Was Right: Innovation, Market Power, and Creative Destruction in 1920s America", *The Journal of Economic History*, 63(4), December 2003, pp. 1023–58.

[13] Ibid.

[14] Arnaud Costinot and Dave Donaldson, "Ricardo's Theory of Comparative Advantage: Old Idea, New Evidence", *American Economic Review*, 102(3), May 2012, pp. 453–58.

15 Sergio Cremaschi and Marcelo Dascal, “Malthus and Ricardo: Two styles for Economic Theory”, *Science in Context*, 11(2), Summer 1998, pp. 229–54.

16 Hemant Mohapatra, “Capex & Opex Supercycles – the Dusk of SaaS and the Dawn of AI-SaaS,” Medium Blog, December 20, 2023, at https://medium.com/@MohapatraHemant/capex-opex-supercycles-the-dusk-of-saas-and-the-dawn-of-ai-saas-8aa5cfe74c93, (Accessed December 25, 2023).

17 Ibid.

18 Ibid.

19 Selina Cheng, “How China Is Churning Out EVs Faster Than Everyone Else”, *The Wall Street Journal*, New York, March 4, 2024.

20 Warwick Goodall, Tiffany Dovey Fishman, Justine Bornstein and Brett Bonthron, “The Rise of Mobility as a Service: Reshaping How Urbanites Get Around”, *Deloitte Review*, Issue 20, 2017.

21 Michael McQueen, Gabriella Abou-Zeid and Kelly Clifton, “Transportation Transformation: Is Micromobility Making a Macro Impact on Sustainability?”, *Journal of Planning Literature*, 36(1), November 15, 2020.

22 Clayton M Christensen, *The Innovator’s Dilemma: When New Technologies Cause Great Firms to Fail*, Harvard Business School Press, Boston, 1997, p. 28.

23 Ibid., p. 25.

24 Clayton M Christensen, Taddy Hall, Karen Dillon and David S Duncan, “Competing Against Luck: The Story of Innovation and Customer Choice”, *Harper Business*, New York, 2016, pp. 16–8.

25 Thomas Arnett, “New Value Networks: The Missing Piece in the K–12 Disruption Equation”, Blog at Christensen Institute, October 4, 2022 at https://www.christenseninstitute.org/blog/new-value-networks-the-missing-piece-in-the-k-12-disruption-equation, (Accessed January 12, 2024).

26 Clayton M Christensen, no. 23, pp. 132–33.

27 Ben Thompson, “Netflix and the Conservation of Attractive Profits”, Blog at Stratechery, July 8, 2015, at https://stratechery.com/2015/netflix-and-the-conservation-of-attractive-profits, (Accessed January 12, 2024).

28 University of California Television (UCTV), “Conversations with History: Manuel Castells”, YouTube, February 16, 2008 at https://www.youtube.com/watch?v=0GBB7U5mv0w, (Accessed January 12, 2024).

29 Manuel Castells, “An Introduction to the Information Age”, in Frank Webster, Raimo Blom, Erkki Karvonen, Harri Melin, Kaarle Nordenstreng and Ensio Puoskari (eds.), *The Information Society Reader*, Routledge, London, 2004, pp 138–49.

30 Tim O’Reilly, “What is Web 2.0?: Design Patterns and Business Models for the Next Generation of Software”, O’Reilly Media Inc, Sebastopol, California, 2009, pp. 1–10.

31 Rob Reid, “Tim O’Reilly on Why the Future Probably Won’T Be All That Terrible”, Ars Technica, October 10, 2017, at https://arstechnica.com/gaming/2017/10/tim-oreilly-on-why-the-future-probably-wont-be-all-that-be-terrible, (Accessed January 12, 2024).

32 Cory Doctorow, “Tim O’Reilly Defines “The Internet Operating System”, Boing Boing, March 29, 2010, at https://boingboing.net/2010/03/29/tim-oreilly-defines.html, (Accessed January 13, 2024).

33 Tim O’Reilly, “Open Data and Algorithmic Regulation”, in Brett Goldstein and Laura Dyson (eds.), *Beyond Transparency: Open Data and the Future of Civic Innovation*, Code for America Press, San Francisco, California, 2013, pp. 289–300.

34 Nithya Ruff, “Comparing the Similarities and Differences between Innersource and Open

Source", Open Source, November 27, 2020, at https://opensource.com/article/20/11/inner-source, (Accessed January 13, 2024).

[35] Tim O'Reily, "Government as a Platform", *Innovations: Technology, Governance, Globalisation*, 6(1), Winter 2011, pp. 13–40.

[36] John Batelle, "A Deficit of Idealism: Tim O'Reilly on the Next Economy", Newco Shift, July 20, 2016, at https://shift.newco.co/2016/07/20/a-deficit-of-idealism-tim-oreilly-on-the-next-economy, (Accessed January 14, 2024).

[37] "Don Tapscott, C.M., BA, BSc, M.Ed, LLD" at https://www.blockchainresearchinstitute.org/don-tapscott, (Accessed January 14, 2024).

[38] "The Blockchain Research Institute" at https://dontapscott.com/research-programs/blockchain-research-institute, (Accessed January 14, 2024).

[39] Don Tapscott and Alex Tapscott, "The Impact of the Blockchain Goes Beyond Financial Services", Technology Analytics, *Harvard Business Review*, May 10, 2016, at https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services, (Accessed January 14, 2024).

[40] Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, Great Clarendon Street, Oxford, 2014, pp. 25–58.

[41] Ibid., p. ix.

[42] Ibid., pp. 87–8.

[43] Ibid., pp. 90–1.

[44] Ibid., pp. 89–90.

[45] Ibid., pp. 25–58.

[46] Soraj Hongladarom, "Floridi and Spinoza on Global Information Ethics", *Ethics and Information Technology*, 10, June 19, 2008, pp. 175–87.

[47] Shyam Krishnakumar, "Reading Floridi: Towards an Informational Ethics of the Infosphere", Medium Blog, The InTech Dispatch, September 27, 2020, at https://medium.com/in-tech/reading-floridi-towards-an-informational-ethics-of-the-infosphere-e38aef2c4409#:~:text=Floridi%20takes %20an%20ecological%20approach,signature%2C%20inforgs%20inhabiting%20an%20infosphere, (Accessed January 20, 2024).

[48] Luciano Floridi, "The Onlife Manifesto: The Onlife Initiative", in Luciano Floridi (ed.), *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Springer Open, New York, 2015, pp. 7–13.

[49] Luciano Floridi, "The Philosophy of Information as a Conceptual Framework", *Knowledge Technology and Policy*, 23(1), June 2010, pp. 1–31.

[50] Yochai Benkler and Helen Nissenbaum, "Commons-based Peer Production and Virtue", *The Journal of Political Philosophy*, 14(4), 2006, pp. 394–419.

[51] Ibid.

[52] Ibid.

[53] Amy Bernstein and Anand Raman, "The Great Decoupling: An Interview with Erik Brynjolfsson and Andrew McAfee", Technology and Analytics, *Harvard Business Review*, June 2015, at https://hbr.org/2015/06/the-great-decoupling, (Accessed January 20, 2024).

[54] Erik Brynjolfsson and Andrew McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, WW Norton and Company, New York, 2014, p. 13.

[55] Ibid., pp. 11–2.

[56] Ibid., p. 16.

[57] Azeem Azhar, *Exponential: How Accelerating Technology Is Leaving Us Behind and What to Do About It*, Diversion Books, New York, 2021, pp. 66–86.

[58] Ibid., pp. 194–218.

59 Ibid., pp. 150–70.

60 Balaji Srinivasan, *The Network State*, Kindle Publishing, New York, 2022, p. 9.

61 Y Combinator, "Balaji Srinivasan at Startup School 2013", YouTube, October 26, 2013, at https://www.youtube.com/watch?v=cOubCHLXT6A&t=1s, (Accessed January 22, 2024).

62 Justin Fox, "Exit, Voice, and Albert O. Hirschman", Organisational Culture, *Harvard Business Review*, December 12, 2012, at https://hbr.org/2012/12/exit-voice-and-albert-o-hirsch, (Accessed January 22, 2024).

63 Balaji Srinivasan, no. 62, pp. 10–1.

64 Y Combinator, no. 63.

65 Balaji Srinivasan, no. . 62, p. 197.

66 Margaret Gould Stewart, "From Techno-optimism to Techno-realism: What It Means to Innovate Responsibly", Medium Blog, September 29, 2021, at https://mags.medium.com/from-techno-optimism-to-techno-realism-what-it-means-to-innovate-responsibly-2b41e47a6470, (Accessed January 22, 2024).

67 "The Techno-Optimist Manifesto by Marc Andreesen" at https://a16z.com/the-techno-optimist-manifesto, (Accessed February 1, 2024).

68 Jim VandeHei and Mike Allen, "Behind the Curtain: A New, Powerful Political Movement", Axios, Washington DC, January 30, 2024 at https://www.axios.com/2024/01/30/techno-optimist-silicon-valley-us-elections, (Accessed February 2, 2024).

69 Dan Reiter and Allan C Stam III, "Democracy and Battlefield Military Effectiveness," *Journal of Conflict Resolution*, 42(3), June 1998.

70 Lex Fridman, "Guillaume Verdon: Beff Jezos, E/acc Movement, Physics, Computation & AGI | Lex Fridman Podcast #407", YouTube, December 30, 2023, at https://www.youtube.com/watch?v=8fEEbKJoNbU, (Accessed January 30, 2024).

71 Bayes, @bayeslord, https://twitter.com/bayeslord?lang=en, (Accessed January 30, 2024).

72 Antong Zhang, Jiani Yang, Yangcheng Luo and Siteng Fan, "Forecasting the Progression of Human Civilization on the Kardashev Scale through 2060 with a Machine Learning Approach", *Scientific Reports*, 13, 2023.

73 Lex Fridman, no. 72.

74 Alexander Wilson, "Techno-Optimism and Rational Superstition", *Techné: Research in Philosophy and Technology*, 21(2), 2017, pp. 342–62.

75 James Hughes and Nir Eisikovits, "The Post-Dystopian Technorealism of Ted Chiang", *Journal of Ethics and Emerging Technologies*, 32(1), January–June 2022.

76 Elizabeth Merritt, "Techno-skepticism: Rethinking the Costs and Benefits of Digital Technology", Centre for the Future of Museums Blog, American Alliance of Museums, May 31, 2023, at https://www.aam-us.org/2023/05/31/techno-skepticism-rethinking-the-costs-and-benefits-of-digital-technology, (Accessed January 22, 2024).

77 Greg Satell, "The 2020s Will Be an Era of Atoms, Not Bits", Digital Tonto, May 23, 2021, at https://digitaltonto.com/2021/why-the-2020s-will-be-an-era-of-atoms-not-bits, (Accessed January 21, 2024).

78 "What is Compute?", at https://www.hpe.com/us/en/what-is/compute.html#:~:text=The%20term%20%22com pute%22%20in%20the,algorithm%20execution%2C%20and%20mathematical%20operations, (Accessed February 12, 2024).

79 Gordon E Moore, "Cramming More Components onto Integrated Circuits", *Electronics*, 38 (8), April 19, 1965, pp. 6.

80 "The Impact of Moore's Law on the Semiconductor Industry" at https://fastercapital.com/startup-topic/Impact-of-Moores-Law.html, (Accessed February 22, 2024).

81 Staney Joseph, "The Future of Artificial Intelligence: How Ray Kurzweil Predicted the

Singularity", Medium Blog, October 30, 2023, at https://medium.com/@staneyjoseph.in/the-future-of-artificial-intelligence-how-ray-kurzweil-predicted-the-singularity-fdbd535aba57, (Accessed February 26, 2024).

82 Tulie Finley-Moise, "What's the Computing Difference Between a TeraFLOPS and a PetaFLOPS?", HP Tech Takes, July 24, 2019 at https://www.hp.com/us-en/shop/tech-takes/computing-difference-between-teraflops-and-petaflops#:~:text=Floating%2Dpoint%20operations%20per %20second%2C%20or%20FLOPS%2C%20is%20the,with%20 integrated %20floating%2Dpoint%20registers, (Accessed January 31, 2024).

83 Marcus Ranney, "AI-Driven Biohacking: How Data & Technology Can Help You Simplify Health?", Medium Blog, July 4, 2023, at https://medium.com/@docmranney/ai-driven-biohacking-how-data-technology-can-help-you-simplify-health-aa00bc6ff17d, (Accessed February 15, 2024).

84 Nipuna Chamara, Md Didarul Islam, Geng (Frank) Bai, Yeyin Shi, and Yufeng Ge, "Ag-IoT for Crop and Environment Monitoring: Past, Present, and Future", *Agricultural Systems*, 203, December 2022.

85 Adam Grissom, "The Future of Military Innovation Studies", *Journal of Strategic Studies*, 29(5), January 24, 2007, pp. 905–34.

86 Barry Scott, Naluahi Kaahaaina and Christopher Stock, "Innovation in the Military", *Small Wars Journal*, 10 February 2019, at https://smallwarsjournal.com/jrnl/art/innovation-military#:~:text=In%20the%20military%2C%20sustaining%20innovations%20reinforce%20the,o ne%20might%20also%20call%20it%20doctrinal%20innovation, (Accessed February 21, 2024).

87 Robert Work, Michael Brown and Ellen Lord, "Innovation Adoption for All: Scaling Across the Department of Defense", War on the Rocks, April 3, 2024, at https://warontherocks.com/2024/04/innovation-adoption-for-all-scaling-across-department-of-defense, (Accessed April 11, 2024).

88 Stephen Peter Rosen, "New Ways of War: Understanding Military Innovation", *International Security*, 13(1), Summer 1988, pp. 134–68.

89 Adam Grissom, no. 87.

90 Robert T. Foley, "A Case Study in Horizontal Military Innovation: The German Army, 1916–1918", *Journal of Strategic Studies*, 35(6), May 15, 2012, pp. 799–827.

91 Adam Grissom, no. 87.

92 Keith B Bickel, *Mars Learning: The Marine Corps' Development of Small Wars Doctrine, 1915–1940*, Routledge, New York, 2000, p. 1–9.

93 Adam Grissom, no. 87.

94 Michael Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power", *Texas National Security Review*, 1(3), May 2018, 36–57.

95 Stephen Peter Rosen, no. 90.

96 Eliot Cohen, *Supreme Command: Soldiers, Statesmen and Leadership in Wartime*, Simon and Schuster Inc., Washington DC, 2002, pp. 132–34.

97 John Arquilla and David Ronfeldt, "Cyberwar is Coming!", *Comparative Strategy*, 12(2), Spring 1993, pp. 141–65.

98 Andrew F Krepinevich, Jr., "The Military-Technical Revolution: A Preliminary Assessment", Centre for Strategic and Budgetary Assessments (CSBA), 2002, at https://csbaonline.org/uploads/documents/2002.10.02-Military-Technical-Revolution.pdf, (Accessed March 12, 2024).

99 Edward Luttwak and Eitan Shamir, *The Art of Military Innovation: Lessons from the Israel Defense Forces*, Harvard University Press, Cambridge, Massachusetts, 2023, pp. 120–23.

100 Tai Ming Cheung, "A Conceptual Framework of Defence Innovation", *Journal of Strategic Studies*, 44(6), June 22, 2021, pp. 775–801.

101 Ibid.

102 Vitaliy Omelyanenko, "National Strategic Innovation Security Conceptualization", *Technology Audit and Production Reserves*, 5(41), January 2018, pp. 36–42.

103 Yingfan Chen, Hamilton Chen and Dingding Chen, "The Broadening Strategy of U.S. Technological Restrictions on China", *The Diplomat*, April 4, 2024, at https://thediplomat.com/2024/04/the-broadening-strategy-of-u-s-technological-restrictions-on-china, (Accessed April 6, 2024).

104 Emily Benson and Gloria Sicilia, "A Closer Look at De-risking", Center for Strategic and International Studies (CSIS), December 20, 2023, at https://www.csis.org/analysis/closer-look-de-risking, (Accessed March 12, 2024).

105 Peter Defazio and Cory Gardner, "Biden, Congress Must Address China's Efforts to Undermine the Inflation Reduction Act", *The Hill*, March 18, 2024, at https://thehill.com/opinion/technology/4525392-biden-congress-must-address-chinas-efforts-to-undermine-the-inflation-reduction-act, (Accessed March 30, 2024).

106 "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence, (Accessed March 12, 2024).

107 Tai Ming Cheung, no. 102.

108 Ibid.

109 Ibid.

110 Tom Galvin, *Leading Change in Military Organisations: Primer for Senior Leaders*, Department of Command, Leadership and Management, School of Strategic Landpower, US Army War College, US Army War College Press, Carlisle, Pennsylvania, 2018, p. 136.

111 Tarique Mahmood and Muhammad Shujaat Mubarik, no. 1.

112 Paul Oling, Sebastiaan Rietjens, Paul van Fenema and Jan-Kees Schakel, "Towards a Cultural Perspective on the Absorption of Emerging Technologies in Military Organizations", *Intelligence and National Security*, 37(4), April 22, 2022, pp. 482–97.

113 Ibid.

114 Martin Lundmark, "Absorbing New Military Capabilities: Defense Technology Acquisition and the Asia-Pacific", in Richard A Bitzinger (ed.), *Emerging Critical Technologies and Security in the Asia-Pacific*, Palgrave Macmillan London, London, 2016, pp. 37–52.

115 Kogila Balakrishnan, "Effective Absorption of Emerging Technologies in Defense Automotives to Enhance Land-Based Military Capabilities", in Richard A Bitzinger (ed.), *Emerging Critical Technologies and Security in the Asia-Pacific*, Palgrave Macmillan London, London, 2016, pp. 75–90.

116 Brian A Jackson, "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption", *Studies in Conflict and Terrorism*, 24(3), August 6, 2010, pp. 183–213.

117 Ibid.

118 Yantsislav Yanakiev, Nikolai Stoianov, Dimitar Kirkov and Grigor Velev, "Defence Strategy and New Disruptive Technologies Nexus: Implications for the Military Organisations", *Journal of Defence & Security Technologies*, 3(1), 2020, pp. 7–41.

119 Ibid.

120 Michael Raska, "Strategic Competition for Emerging Military Technologies: Comparative Paths and Patterns", *PRISM*, 8(3), January 9, 2020,

121 Jodie Kaye Stevens, "Exploring Enablers and Barriers to the use of Mobile Apps for Training and Learning in the Australian Army", Psychology Honours Dissertation, University of Adelaide, 2020, at https://digital.library.adelaide.edu.au/dspace/handle/2440/131291, (Accessed April 2, 2024).

122 Information collected and collated from multiple sources. The main source, however, is: "Technology Readiness Level (TRL) – Overview" at https://acqnotes.com/acqnote/tasks/technology-readiness-level, (Accessed March 13, 2024).

Chapter Two

Innovation Setups in Militaries Around the World

The US Military

The innovation ecosystem in the United States (US) military is extensive, in depth and expansive. Starting from the US Secretary of Defence's Strategic Capabilities Office (SCO),[1] down to the warfighter, the ocean of US innovation ecosystem involves organisations of all sorts. Though this also leads to innovation-fratricides, VoD and acquisition issues at times, as a whole the setup provides incentives to small- and medium-sized enterprises, individuals and college students to develop prototypes of platforms and technologies to give US forces an edge against their adversaries. The entire innovation setup tries to align itself with a number of sequential goals of the US military, however, a number of challenges remain. This chapter will focus only on the US Army, whose long-term goals extend till 2040, when it will be able to conduct multi-domain operations (MDO) against near-peer adversaries.[2] The broad impetus behind this change of approach are the US National Security Strategies (NSS) of 2018[3] and 2022[4] and the National Defence Strategies (NDS) of 2018[5] and 2022.[6] They are themselves inspired to an extent from the Third Offset strategy.[7]

The third offset strategy was a realisation that US's competitors and adversaries, namely, Russia and China had 'implemented modernisation programs to offset the United States' military conventional superiority', challenging them in areas that were 'trans-regional, multi-domain, and multi-functional'.[8] The context behind this apprehension is that the US's post-

Cold War ability to project power around the globe without interference from an adversary is now at risk,[9] especially when near-peer competitors have developed anti-access/area denial (A2/AD) capabilities that do not allow US forces to deploy forces for power projection in the geographic areas of their choice. This perspective has to be internalised before analysing American efforts at innovation since not every country may face the same challenge behind defence modernisation using emerging and disruptive technologies. It is also important to note here that many believe that the Third Offset strategy stands terminated with the publication of the 2018 NDS containing many of its ideas especially the core challenge of competing with China and Russia.

However, if one follows the trajectory of developments within the US Department of Defence (DoD) broadly and the US Army specifically as well as the official publications and speeches, it is clear that the philosophy and guiding points of the Third Offset still sustain. The US's ability to conduct MDO also underscores its attempts to harness the rapid innovations coming out of Silicon Valley and multiple startups for military use, which leads us to study the structure and organisation of the US Army Futures Command (AFC) and the broader US military innovation ecosystem. There are two major issues that may derail this ambitious project. The first is an observable difference between what the Third Offset sets out as mission priorities and that advocated by the six modernisation priorities of the US Army as part of its 2040 MDO preparation.[10] The second is a congestion within the US defence innovation ecosystem (DIE) that threatens to saturate and crowd out genuine technological solutions in the longer term.

The need for the Third Offset strategy branched out from a realisation within the US military leadership, that countries such as China and Russia had closed the technological gap and in certain areas edged out the US in important technological areas such as unmanned systems, hypersonic missiles and battle C2 systems.[11] One of the major reasons behind this was that while the US military focused on sub-conventional conflicts in the wider West Asia and Af–Pak belt, specifically Iraq, Afghanistan and the frontier areas of Pakistan, China expanded its investment in 'anti-ship cruise and ballistic missiles, anti-satellite technology, diesel and nuclear submarines, and other advanced capabilities' that targeted US vulnerabilities, as per ex Defence

Secretary Robert Gates.[12] Some examples of this include the development of the J-20 stealth aircraft, island building spree in the South China Sea and routine harassment of US ships transiting the region.[13] This was the time when Russia and China were modernising their forces and force structures rapidly and at the same time, using an array of political, informational, military and economic tools to cement their control over their respective regions of influence.[14]

It was also felt that due to the nature of adversaries, the US forces had become habituated to certain operational 'luxuries' such as the omnipresence of air supremacy,[15] light infantry footprint[16] and uncontested logistics.[17] A decision was therefore made to reorient the military towards 'great-power competition' in three stages: competition, crisis and conflict.[18] This segregation of stages was done under the assumption that war will not break out that easily between near-peer nuclear armed adversaries, but Russia and China will use actions calibrated to remain beneath the conventional war response of the US military to achieve politico-military objectives – grey zone warfare[19] – and therefore the US will be found wanting in its overall objective of projecting power or defending allies without resorting to outright military operations. There was also an apprehension that, given the long-range nature of domains such as space and cyber, even the US homeland was not safe from attacks, though not necessarily in the kinetic domain.

A new operational doctrine was therefore required, which would, in effect, restructure the entire armed forces to a new format of warfighting. The precursor to this doctrine was a study undertaken by Robert O Work (at the time the chief executive officer of the Centre for a New American Security or CNAS and later the key figure responsible for implementing the Third Offset as the deputy secretary of defence from 2014 to 2017). Called '20YY: Preparing for War in the Robotic Age', the document laid out the reasons for a new approach towards warfighting, one that would 'spark a new military technical revolution', combining US's post-Cold War era dominance of precision guided weapons and automated battle C2 systems with advanced technologies driven by the civilian sector.[20] It envisioned a future where the US forces would face a war scenario dominated by 'proliferated sensors, electric weapons, and ubiquitous unmanned and autonomous systems in all operating domains'.[21] Work called it the Age of Robotics and assumed that US's near-peer adversaries had already achieved significant headway in this field.

By the time Work was appointed as the deputy secretary of defence, a beginning had been made when SCO was set up by then-Deputy Secretary of Defence Ash Carter in August 2012. Using a combination of repurposing and integrating systems, fusing them with commercial technology, SCO intended to create counters to China's rapidly modernising arsenal and technological capabilities. Employment of these techniques is illustrated by the examples of SCO repurposing the US Navy's (USN) Standard Missile (SM)-6 surface-to-air missile (SAM) from an air defence (AD) to an offensive weapon for attacking and destroying enemy ships at extended ranges. SCO also introduced the Arsenal Plane Program, which acts as a flying inventory or restocking arsenal for forward deployed fighter aircrafts to conduct their missions and resupply in the air. Finally, smart sensors, computing and networking capabilities were fused into existing technologies.[22] Robert Work's apprehension regarding China was the latter's extensive A2/AD in the Indo–Pacific region, designed keeping US capabilities in mind.[23] He felt that Russia and China's investments in precision-guided munitions (PGMs), battle networks and AD over the last 20 years while the US was involved in fighting insurgencies and terror cells around the globe had enabled them to attain near-parity in technological superiority with the US.[24] As per him, maintaining the US's technological superiority against its adversaries required investments in 'aerial and naval unmanned systems, AI, computer-assisted human operation systems, and AI-enabled battle networks, among other technological innovations',[25] which would require an unprecedented collaboration and even the integration of the civilian sector such as Silicon Valley firms, academia and startups.

This is how the idea of the Third Offset came into being. Known initially as the Defence Innovation Initiative (DII),[26] the aim was to create a narrative of continuity and the importance of technology in America's attempts to wrest the technological mantle from its adversaries. While the First Offset focused on using nuclear weapons and the Second Offset on precision weapons, both were aimed at countering the erstwhile Soviet Union and the wider Warsaw Pact's quantitative superiority in men and materiel, the former through invoking use of battlefield nuclear weapons and the latter using a combination of precision and stealth technologies to target the follow-on forces of the second echelon. The Third Offset, like its immediate predecessor, was focused on small wins in this direction since Work acknowledged the complexities of the long-term acquisition processes of the forces and started ordering war games in order to familiarise the Services with the need for new technologies.[27] Another aim of the Third Offset was to put the US DoD back in the driving seat of technological innovations.[28] Since most technological innovation was now concentrated in Silicon Valley and other firms in the private sector, commercialisation, as per the DoD view, had led to so much diffusion of advanced technology around the globe that even America's adversaries had access to the same technologies. Moreover, they had crafted their operational concepts for leveraging these technologies to initiate actions that threatened to but did not violate the US military's bounds for initiating a conventional conflict. The Third Offset intended to claw back this advantage by positioning DoD as a worthy buyer, collaborator and investor in emerging technologies.

Since both China and Russia had already created effective and highly sophisticated PGMs and long-range fire capabilities, the areas where the US could now gain superiority was autonomy.[29] Incidentally, autonomy and AI were also areas that had achieved rapid growth in the private industry, powered by the availability of massive amounts of data, significant computing power and new, evolved algorithms and learning techniques. The digital industry had also just woken up from the AI winter and was rapidly innovating in the field.[30] This led to revolutions in many associated areas such as biotechnology, edge computing and computer vision among others. More importantly, 'pure' physical domains were also being digitally converted due to the proliferation of sensors and miniaturisation of computing devices along with falling prices. On a broader scale, unlike the two offsets before it, technological innovation was accorded the highest priority in the Third Offset for competing against Russia and China.[31] The strategy intended to replace the current relationship between the US DoD and the industry, realising that it is now the private sector that drives technological innovation rather than the other way round. Finally, the strategy placed emphasis on 'enterprise', that is, change in the acquisitions process, driven by an understanding that industrial age processes may not work, given the exponential change oriented and iterative nature of technology deployment.[32] It also required new operating concepts and doctrines to optimise the use of these technologies by the armed forces.

In 2014, the Defence Science Board (DSB) published a 'Summer Study on Autonomy'.[33] The DSB is an advisory body composed of members from the fields of science and technology (S&T), manufacturing, acquisition process and other fields and advises the defence secretary, the various deputy defence secretaries and the chairman and vice chairman of the joint chiefs of staff, among other important DoD functionaries.[34] The 2014 study on autonomy affirmed that autonomy could mitigate six types of operational challenges, namely, rapid decision making, high heterogeneity and/or volume of data, intermittent communications, high complexity of coordinated action, danger of mission and high persistence and endurance.[35] The interesting part of the recommendations given in the study was the reference to 'non-traditional R&D communities in novel ways to speed up DoD's access to emerging research results'.[36] The DSB also acknowledged that given the current budget it would be very difficult to recommend major new programs but certain experiments and prototypes could be tested and conducted to demonstrate the operational value of this concept. Finally, the study stated that autonomy had reached a 'tipping point'[37] and that autonomous capabilities were 'readily available to allies and adversaries alike'[38] due to the involvement of commercial enterprises in the development of this technology.

The literature on Third Offset and the US Army's innovation efforts generally does not mention two organisations that were setup to tie up coordination and policy issues at the very top. Both were created in 2014 and terminated in 2018. These were the Advanced Capabilities and Deterrence Panel (ACDP) and the Breakfast Club.[39] The former comprised senior leaders in the military hierarchy, members of the intelligence community (IC) and civilians and was used to brainstorm issues on how to implement the strategy. The IC representatives provided the panel with a broad overview of the technological developments happening in other countries and that they were also eager customers for the same set of technological advancements emanating from the Silicon Valley.[40] Three 'pathfinder' initiatives were setup under ACDP, namely, the Special Program Missile Defeat,[41] Joint Interagency Combined Space Operations Center[42] and the Algorithmic Warfare Cross-Functional Team (Project Maven).[43] The aim of the first program was to use AI and machine learning (ML) to improve the understanding and analysis of spy satellite imagery.

The second program, shortened to JICSpOC, was designed to 'perform battle management and command and control of the space constellation under threat of attack'.[44] JICSpOC worked in conjunction with the US Strategic Command, Air Force Space Command and IC and had capabilities for data fusion and 'develop, test, validate and integrate new space system tactics, techniques and procedures' for both DoD and IC.[45] It was later renamed and institutionalised as the National Defence Space Center under the then-newly formed US Space Command with a responsibility to conduct 'unified space defence operations'.[46] Project Maven, which also created a rift between the DoD and certain segments of civilian programmers working for Google,[47] was used to process and analyse the massive trove of drone footage data from the West Asian region and elicit actionable intelligence for targeting Islamic State (IS) militants.[48] Launched in 2017, it has now come under the auspices of the US National Geospatial-Intelligence Agency (NGA)[49] and proven its worth in multiple iterations of the Project Convergence (PC) exercises. One of the main aims of the program, tested and experimented through the annual PC exercises is to analyse and process data at machine speed, enabling the activation of a sensor-processor-shooter web. In PC 2020, for example, an MQ-1C Gray Eagle drone was equipped with a Maven Smart System and an Algorithmic Inference Platform, which captured and processed data at the edge.[50] This means that the data was not required to be sent to a command post for processing and was acted upon by the drone itself.

The ACDP and the Breakfast Club were respectively and very broadly the policy and implementation groups for the Third Offset. While ACDP comprised the senior hierarchy and was used as a platform to break down resistance to the idea of implementing the Third Offset, especially with respect to budgeting and reaching out to civilian players other than the established defence contractors, the Breakfast Club consisted of mid-level officers who also acted as an informal secretariat to the ACDP. They coordinated ACDP meetings, prepared drafts and set the agenda for further meetings. Both these organisations were responsible for entrenching certain aspects of the Third Offset strategy within the military, IC and DoD ecosystem.[51]

Another lasting achievement during the heydays of the Third Offset was the creation of the Defence Innovation Unit – Experimental (DIUx), which was later renamed by removing the experimental suffix from the name as, DIU.[52] This organisation, as per Work, was part of an innovation continuum with the Defence Advanced Research Projects Agency (DARPA) and SCO anchoring either ends.[53] While DARPA looked at potential technologies with a longer-term horizon of more than 20 years, DIU looked at near-term solutions. The main role of SCO was to look at the current platforms and technologies and look at how they could either be repurposed or used in multiple permutations and combinations to create new capabilities using existing weapons systems.

DIU took inspiration from a venture capital (VC) fund created by the Central Intelligence Agency (CIA) called In-Q-Tel in 1999 through which it approached 'technology firms and start-ups to identify and invest in promising new technologies'.[54] The broad technology areas identified by the organisation include digital intelligence, trusted infrastructure, autonomous systems, industry 4.0, intelligent connectivity, AI and ML.[55] In-Q-Tel also has an IQT lab that focuses on open-source solutions for IC in three areas, namely, edge, data and trust.[56] The lab has multiple projects ranging from automatic collection of labelled data sets, improving synthetic data with generative deep learning (DL) networks, using low cost sensors to locate the source of a radio frequency (RF) signal and detection of deepfakes within videos, among others.[57] By converting classified intelligence problems into unclassified problem statements for Silicon Valley, In-Q-Tel creates a best-of-both-worlds scenario where while it does not have to break security classifications, it can also recruit the assistance of startups. Taking a leaf out of In-Q-Tel's book, DIU was created and its office setup in Mountain View, California. Later other DIU offices were also setup in Austin, Texas; Boston, Massachusetts; and Washington, DC.[58] Since the mandate of DIU was to look at short-term solutions, it shortened the time for execution of contracts. Once it received a problem statement from a unit, it took a set of actions. It ensured that the unit requesting for a solution would co-invest with the DIU involving that unit or formation as a stakeholder in the successful execution of the project. The time between request for a proposal (RFP) and the formalisation of the contract is just 60 days with expected delivery within six months.[59] The current catalogue of solutions from DIU include AI for flight optimisation, next generation small class UUVs (SCUUV), operationalising the Blue sUAS program, which classifies and vets commercial UAS for DoD use, collaborative mission autonomy algorithms, space situational awareness, cyber threat intelligence, short-range reconnaissance and persistent maritime ISR, among others.[60]

A distinguishing characteristic of DIU is the organisation and who helms it. Currently, it is led by Doug Beck, who served as vice president at Apple for close to 15 years. Doug is also a captain in the US Naval Reserve and served in Iraq and Afghanistan.[61] This unique blend of corporate management and military service provides DIU with an unparalleled view of the convergence of the commercial sector with national security and defence in particular. DIU has a total of 18 people in its leadership team with extensive experience in multiple subject areas spanning government agencies and corporate firms.[62] The agency handles portfolios such as space, human systems, autonomy, AI & ML, energy and cyber & telecommunications. These are the major areas where DIU engages with the commercial sector.[63] Very briefly, the subtopics within these areas include ML predictions, responsible AI development, emerging AI technologies and AI infrastructure for AI & ML portfolio; small UAS, counter UAS, mission autonomy, logistics, manufacturing using 3D printing, ground mobility and maritime autonomy for autonomy portfolio; assessment, defence, enabling and security of cyber and telecom infrastructure for the cyber portfolio; installation resilience and operational energy for the energy portfolio; lethality, survivability and readiness for the human systems portfolio; and peacetime indications & warnings, responsive access to mission-designated orbits, reduced latency communications & GPS resiliency, hardware to software transformation modernisation and multi-orbit operations and logistics for the space portfolio.[64]

DIU has created a Commercial Solutions Catalog, which contains commercial solutions designated successful by DIU and available to all branches of DoD for immediate purchase.[65] DIU utilises something called the Other Transaction Authority (OTA) for research, prototyping and production, meant for technologies and prototypes that do not have a commercial equivalent in the market.[66] It is a legal contract between the federal government and a non-profit organisation, which allows for other transactions, such as research and development (R&D), prototype development and other projects – basically any procurement that does not require a formal contract covered under the Federal Acquisition Regulations

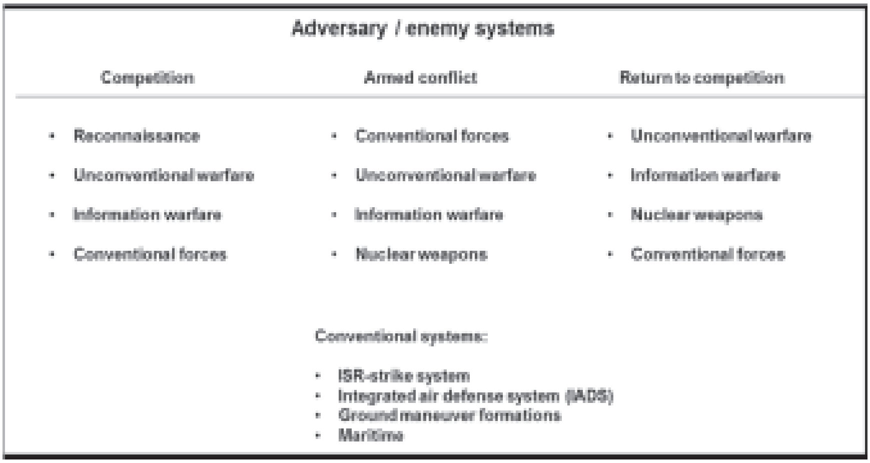
(FAR) or Defence FAR (D-FAR).[67] There are certain caveats in the usage of OTA such as a ceiling of $500 million and the contracting party being a defence startup or small business. However, OTA provides a lot of flexibility to organisations such as DIU and DARPA to cater to new and emerging technologies and prototypes.

Summarising the Third Offset, it was many things at once. As an attempt to create countervailing technological capabilities against what it considered were competitors, that is, China and Russia, it attempted to create a narrative of continuance from the 1950s to the present. The First and Second Offsets were connected to this one and technological superiority was emphasised, both as a necessity and imperative, both normative and prescriptive. It introduced the term 'competition' within the US military lexicon[68] as a method of dealing with countries that the US may have to fight in the future but had to contend with currently in a grey-zone method. Thirdly, the Third Offset also provided a proof of concept for how acquisitions could be reformed while dealing with new vendors such as defence startups and Silicon Valley firms. In doing this, the strategy also focused on how military organisations absorbed innovation and created operational concepts to leverage them into capabilities. Lastly, by focusing on A2/AD capabilities of its adversaries, both for countering and creating its own, it birthed the concept of MDO,[69] which has today become critical against A2/AD setups due to the necessity of having a mesh or web of interconnected sensors and weapons platforms across multiple domains. The basic concept was the likely inability of the US Army to close in with the adversary due to their A2/AD shields and thereby depending on other domains to perform the task, therefore networking with that domain actor and communication became critical.

The US Army's concept of MDO, which partially stems from the Third Offset, is based on four types of threats that the US Army feels it faces from its near-peer adversaries such as China and Russia. These are A2/AD capabilities; integration of space, cyber, information and electronic warfare (EW) capabilities; faster, lethal and distributed battlefields that feature AI, autonomy and robotics; and employment of chemical, biological, radiological and nuclear (CBRN) weapons that add to the standoff capabilities of US's adversaries.[70] The concept of MDO was originally introduced in a TRADOC pamphlet in 2017 titled 'Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025–2040'.[71] The document details the ability of the US Army, as part of US Joint Forces, to 'maneuver and deliver effects across all domains in order to develop and exploit battlefield opportunities across a much larger operational framework'[72] and suggest the use of a whole of government (WoG) approach, as well as increased dependence on multinational partners and allies.

The document centres the role of US forces on 'competition', which is the ability of US forces to advance or defend national interests without the threat of combat-related violence.[73] In competition, the adversary has a two-fold objective: achieve results below the level of armed conflict and posture forces to support the escalation of activity into armed conflict. The US Army describes competition in three ways: narrative competition or rise and fall in a country's reputation based on strength, reliability and resolve; direct competition or 'full range of competitive activities, from the lowest intensity competition below armed conflict through general state conflict'; and indirect competition or gaining advantage against their adversaries.[74] 'The concept of "convergence" is introduced here which calls for an "integration of capabilities across domains, environments, and functions in time and physical space to achieve a purpose"'[75] This is a much deeper and organic level of integration that requires multiple organisations and capabilities to be networked together in both peace and wartime. There is an acknowledgement of the critical role of advanced technologies within the adversaries' arsenal including unmanned systems, AI, robotics along with the pairing of ISR systems such as sensors, spies, special operations forces, UAS and space-based imagery with long-range precision fire systems.[76] Combined with the rapid prototyping and scaling offered by manufacturing techniques such as additive manufacturing, there is a danger that US forces will be overwhelmed during conflict.

The following diagrams describe what capabilities the adversary can bring to bear on US forces in various stages. To clarify the diagram and make the connection between this operational concept and the American military innovation ecosystem, it is important to define some US military terms specific to the MDO.



Adversary / enemy systems

Competition	Armed conflict	Return to competition
• Reconnaissance	• Conventional forces	• Unconventional warfare
• Unconventional warfare	• Unconventional warfare	• Information warfare
• Information warfare	• Information warfare	• Nuclear weapons
• Conventional forces	• Nuclear weapons	• Conventional forces

Conventional systems:

- ISR-strike system
- Integrated air defense system (IADS)
- Ground maneuver formations
- Maritime

Figure 1: The three different conceptions of competition as per the US Army's concept of MDO[77]

The MDO operational framework divides the area of operations into deep fire (operational and strategic) areas, deep manoeuvre areas, close areas and support (strategic, operational and tactical) areas. The deep fire areas are beyond the maximum range of movement for conventional forces, but special forces, joint fires, information and virtual capabilities can be employed here. Operational deep fire areas would be too far away for conventional forces while strategic deep fire areas would be locations prohibited to be interfered by law or policy. Since only selected capabilities can be employed here, targeting these areas depends on an optimum utilisation of long-range assets and advanced technologies. The deep manoeuvre areas witness the employment of ground, air and maritime manoeuvre forces supported by significant multi-domain capabilities. Close areas feature locations where adversary forces are in physical contact. This is the area where multiple technological and tactical solutions, usually scalable, can be employed.[78] Examples from the Russia–Ukraine war will be used later to amplify this concept. Finally, the support areas are locations that the US Joint Forces will use for 'maximum freedom of action, speed, and agility and to counter the enemy's multi-domain efforts to attack friendly forces, infrastructure, and populations'.[79]

Figure 2 details the kind of capabilities available with adversaries during different stages of confrontation. These include various combinations of reconnaissance, unconventional warfare (UW), information warfare (IW), nuclear and conventional forces during the competition, armed conflict and return to competition stages. One can observe the need for a diverse inventory of hi-tech solutions for all these challenges including long-range ISR assets, integrated air defence systems (IADS), SAMs, surface-to-surface missile (SSM) batteries, maritime task forces, AI-enabled C2 systems, social media analytics tools and open-source intelligence (OSINT), among others. The US Joint Forces and the US Army foresee three solutions for conducting a successful multi-domain battle. These are **force posture,** which is a mix of forward presence forces, expeditionary forces and partner forces. The mix of technologies used in this case will be counter IW systems, strategic heavy lift, small UAS and counter A2/AD systems. The second solution is **resilient formations,** which are scalable and task-organised units with ISR, mobility, firepower and endurance. These will contain technological solutions such as IADS, layered and long-range precision fire capabilities. The third solution is **convergence,**[80] which will produce 'physical, virtual, and/or cognitive windows of advantage that provide the freedom of maneuver required for forces to defeat adversary systems'.[81] These will integrate domains of space, cyberspace, air, land, maritime, electromagnetic (EM) spectrum and information.

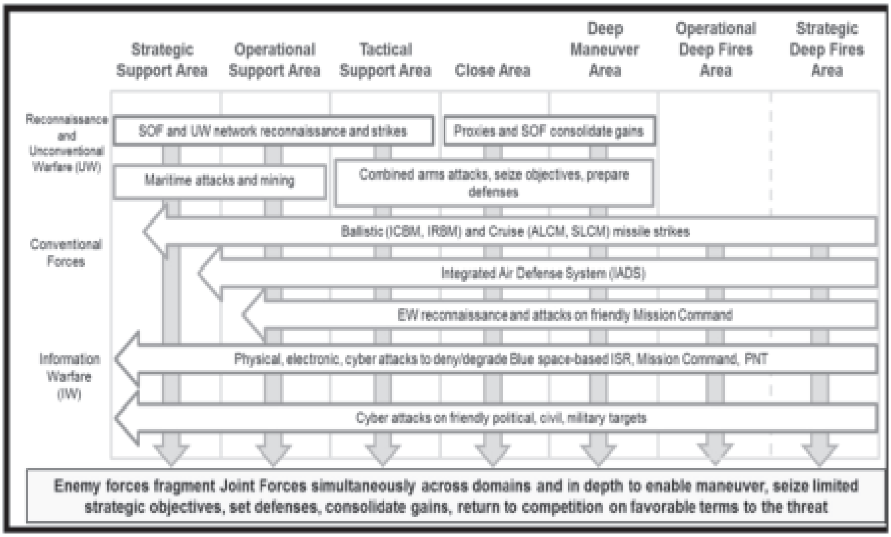

Strategic Support Area
Operational Support Area
Tactical Support Area
Close Area
Deep Maneuver Area
Operational Deep Fires Area
Strategic Deep Fires Area
Reconnaissance and Unconventional Warfare (UW)
Conventional Forces
Information Warfare (IW)
SOF and UW network reconnaissance and strikes
Proxies and SOF consolidate gains
Maritime attacks and mining
Combined arms attacks, seize objectives, prepare defenses
Ballistic (ICBM, IRBM) and Cruise (ALCM, SLCM) missile strikes
Integrated Air Defense System (IADS)
EW reconnaissance and attacks on friendly Mission Command
Physical, electronic, cyber attacks to deny/degrade Blue space-based ISR, Mission Command, PNT
Cyber attacks on friendly political, civil, military targets
Enemy forces fragment Joint Forces simultaneously across domains and in depth to enable maneuver, seize limited strategic objectives, set defenses, consolidate gains, return to competition on favorable terms to the threat

Figure 2: Different capabilities available with US's adversaries during armed conflict[82]

The document mentions in detail the components that form the key required capabilities and supporting actions. A majority of these requirements depend on the availability of advanced technological solutions. These capabilities are required in the areas of mission command, intelligence, movement and manoeuvre, fires, manoeuvre support, sustainment and engagement. Some of these, in short, are energy efficient power management technologies; autonomous maintenance, repair and overhaul (MRO); convoy operations using manned-unmanned teaming (MUM-T); precision supply operations using robotic systems; use of autonomous and robotic systems across domains to increase personnel survivability and effectiveness as well as to detect, identify and penetrate high-risk areas; integration of land- and sea-based air and missile defence capabilities; integration of counter-UAS and short-range AD; planning, integrating and employing information-related capabilities to conduct information environment operations; integration of cyberspace, EW attack, EM spectrum sensors and jamming capabilities in conjunction with automated electromagnetic battle management capabilities; synchronisation and employment of lethal and nonlethal cross-domain fires to project power from land by delivering timely and accurate effects into other domains; employment of robotic and autonomous systems to lighten the warfighter's physical workload; complementing land, air and maritime manoeuvre capabilities with manoeuvre in space, cyberspace and the electromagnetic spectrum; improving processing of multi-intelligence data, including that from non-traditional sources such as social media, blogs, internet and periodical media; employment of improved intelligence collection, analysis and synthesis capabilities; and employment of a combination of integrated and interoperable C4ISR systems and networks.[83]

The second pamphlet by TRADOC named 'The US Army in Multi-Domain Operations 2028' upgrades multi-domain battles to an overarching concept of MDO. Here the core challenge is that of 'layered standoff',[85] which is the comprehensive integration of the adversary's capabilities in the land, air, space and cyber space domain to separate US and allied forces temporally, spatially and functionally, leading to final defeat. To counter this challenge, the central idea advanced is that of 'rapid and continuous integration of all domains of warfare' for competition, and if conflict occurs, then use army formations to penetrate and disintegrate enemy A2/AD systems to force them to return to competition.[86]

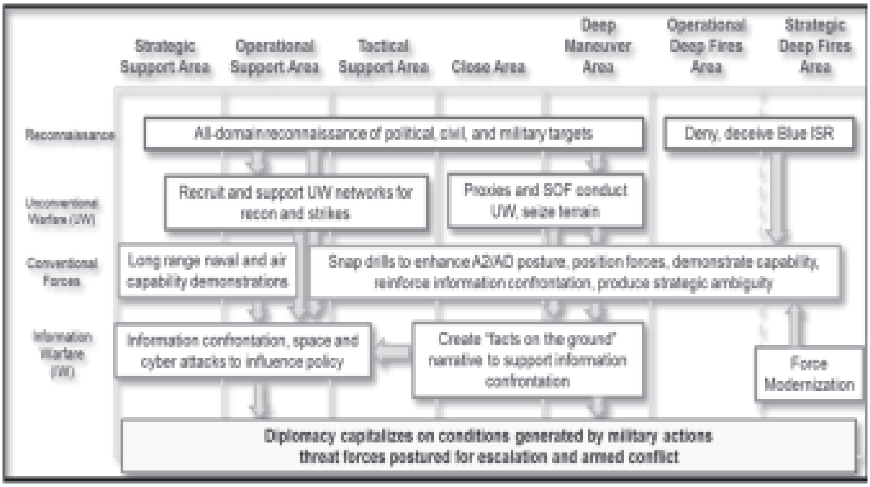
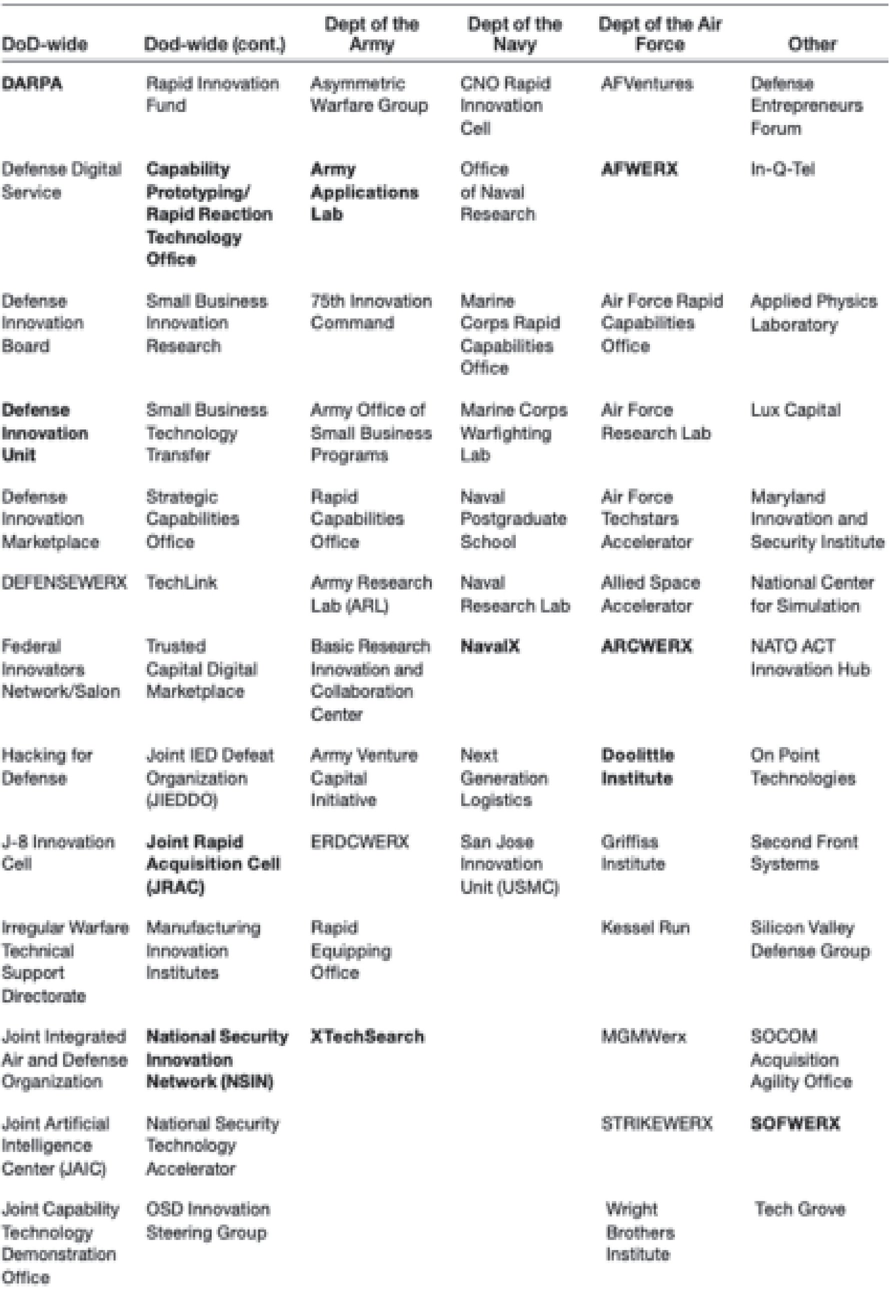

Strategic Support Area
Operational Support Area
Tactical Support Area
Close Area
Deep Maneuver Area
Operational Deep Fires Area
Strategic Deep Fires Area
Reconnaissance
All-domain reconnaissance of political, civil, and military targets
Deny, deceive Blue ISR
Unconventional Warfare (UW)
Recruit and support UW networks for recon and strikes
Proxies and SOF conduct UW, seize terrain
Conventional Forces
Long range naval and air capability demonstrations
Snap drills to enhance A2/AD posture, position forces, demonstrate capability, reinforce information confrontation, produce strategic ambiguity
Information Warfare (IW)
Information confrontation, space and cyber attacks to influence policy
Create "facts on the ground" narrative to support information confrontation
Force Modernization
Diplomacy capitalizes on conditions generated by military actions
threat forces postured for escalation and armed conflict

Figure 3: Adversary military systems during competition[84]

The tenets of MDO remain almost the same as the previous document with the term 'resilient formations' replaced by 'multi-domain formations'.[87] Here a new set of operating conditions are assumed that include: contestation of domains including physical and newly emerging ones such as EM spectrum, cyberspace and information; expanded, lethal and hyperactive battlefield, which on a comparative scale makes the armies smaller; complex environment, which makes it difficult for nation states to impose their will; and the ability of near-peer states to compete below armed conflict.[88] Six modernisation priority areas have been set out, which can be correlated with the requirements of the US Joint Forces and the US Army. The requirements are calibration of force posture geographically, building partner capacity, precision logistics, conduct MDO in dense urban terrain, support credible US narrative, shift capabilities rapidly between domains and organisations and create multi-domain formations. The third iteration of the MDO concept within the US Army – the October 2022 Field Manual (FM) 3-0 –[89] is the official publication that cements the US Army's focus on MDO.

This manual, however, breaks away from the previous two documents and focuses largely on the two concepts of long-range fires and combined arms operations against the threats posed by both Russia and China.[90] This is a climbdown, since the previous two documents had a competition component that could leverage technological innovation to achieve primacy in grey-zone operations. By abandoning those tenets and reverting back to a fire-power heavy conventional mindset, the US Army seems to have visualised the use of emerging technologies in a conventional sense, using them to augment conventional capabilities, rather than devising new ones. The priority areas are long-range precision fires, next generation combat vehicles, future vertical lift, air and missile defence, network and soldier lethality.[91] These six areas are supposed to drive the materiel development of the US Army to be ready for MDO. However, the army has also designated eight priority research areas (PRAs), which are disruptive energetics, RF electronics materials, quantum, AI, autonomy, synthetic biology, material by design and science of additive manufacturing.[92] As per Field Manual (FM) 3-0, these eight PRAs will allow the US Army to develop and leverage emerging technologies for modernising itself.

In order to clearly identify the different defence innovation organisations within US DoD, it is important to start from the top. Post the release of the NDS, a National Defence S&T Strategy (NDSTS) is prepared by the office of the Chief Technology Officer (CTO) of DoD, which is the Under Secretary of Defence for Research and Engineering (USD(R&E)).[93] Fourteen critical technology areas grouped under three broad categories have been identified in 2023.[94] The categories are seed areas of emerging opportunity (biotechnology; quantum science; future generation wireless technology or FutureG; and advanced materials), effective adoption areas (trusted AI and autonomy; integrated network system of systems; microelectronics; space technology; renewable energy generation and storage; advanced computing and software; and human-machine interfaces) and defence-specific areas (directed energy; hypersonics; and integrated sensing and cyber).[95] The induction of these technologies is being addressed through a host of defence innovation organisations (DIOs) such as the National Security Innovation Network (NSIN),[96] DIU,[97] DEFENSEWERX,[98] SOFWERX,[99] AFWERX,[100] NavalX,[101] Army Applications Laboratory (AAL),[102] xTechSearch,[103] ARCWERX,[104] Joint Rapid Acquisition Cell (JRAC)[105] and Kessel Run,[106] among others. A snapshot of the various organisations created to liaise, coordinate, co-develop and sponsor defence startups, small businesses and firms is given below.



DoD-wide	Dod-wide (cont.)	Dept of the Army	Dept of the Navy	Dept of the Air Force	Other
DARPA	Rapid Innovation Fund	Asymmetric Warfare Group	CNO Rapid Innovation Cell	AFVentures	Defense Entrepreneurs Forum
Defense Digital Service	**Capability Prototyping/ Rapid Reaction Technology Office**	**Army Applications Lab**	Office of Naval Research	**AFWERX**	In-Q-Tel
Defense Innovation Board	Small Business Innovation Research	75th Innovation Command	Marine Corps Rapid Capabilities Office	Air Force Rapid Capabilities Office	Applied Physics Laboratory
Defense Innovation Unit	Small Business Technology Transfer	Army Office of Small Business Programs	Marine Corps Warfighting Lab	Air Force Research Lab	Lux Capital
Defense Innovation Marketplace	Strategic Capabilities Office	Rapid Capabilities Office	Naval Postgraduate School	Air Force Techstars Accelerator	Maryland Innovation and Security Institute
DEFENSEWERX	TechLink	Army Research Lab (ARL)	Naval Research Lab	Allied Space Accelerator	National Center for Simulation
Federal Innovators Network/Salon	Trusted Capital Digital Marketplace	Basic Research Innovation and Collaboration Center	**NavalX**	**ARCWERX**	NATO ACT Innovation Hub
Hacking for Defense	Joint IED Defeat Organization (JIEDDO)	Army Venture Capital Initiative	Next Generation Logistics	**Doolittle Institute**	On Point Technologies
J-8 Innovation Cell	**Joint Rapid Acquisition Cell (JRAC)**	ERDCWERX	San Jose Innovation Unit (USMC)	Griffiss Institute	Second Front Systems
Irregular Warfare Technical Support Directorate	Manufacturing Innovation Institutes	Rapid Equipping Office		Kessel Run	Silicon Valley Defense Group
Joint Integrated Air and Defense Organization	**National Security Innovation Network (NSIN)**	**XTechSearch**		MGMWerx	SOCOM Acquisition Agility Office
Joint Artificial Intelligence Center (JAIC)	National Security Technology Accelerator			STRIKEWERX	**SOFWERX**
Joint Capability Technology Demonstration Office	OSD Innovation Steering Group			Wright Brothers Institute	Tech Grove

Figure 4: A snapshot of the various organisations in the US involved in the defence innovation ecosystem[107]

A RAND study has conceptualised an ideal way of thinking about DIE and its interaction with the commercial marketplace. This is illustrated in the figure below:

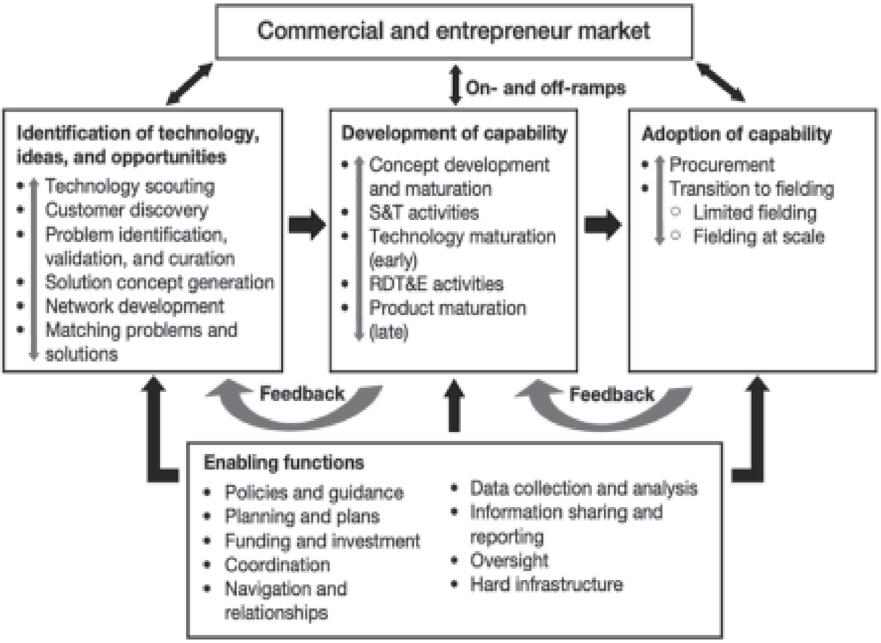

Commercial and entrepreneur market
On- and off-ramps
Identification of technology, ideas, and opportunities
• Technology scouting
• Customer discovery
• Problem identification, validation, and curation
• Solution concept generation
• Network development
• Matching problems and solutions
Development of capability
• Concept development and maturation
• S&T activities
• Technology maturation (early)
• RDT&E activities
• Product maturation (late)
Adoption of capability
• Procurement
• Transition to fielding
○ Limited fielding
○ Fielding at scale
Feedback
Feedback
Enabling functions
• Policies and guidance
• Planning and plans
• Funding and investment
• Coordination
• Navigation and relationships
• Data collection and analysis
• Information sharing and reporting
• Oversight
• Hard infrastructure

Figure 5: An ideal Defence Innovation Ecosystem[108]

There are two ways of thinking about how DIE works in the US military. The first is based on pure innovation, where a particular innovation organisation, such as the DIU, is placed totally outside the military in order to gel well with startups and commercial technology providers, and function outside the traditional hierarchy of the forces, which may constrain innovation and eccentric thinking. This also has the disadvantage of missing the particular arm/services' modernisation priorities in favour of the technology – a classic end-means mismatch. The second is aligning the priorities of the innovation organisation with the modernisation priorities of the service from the very start. Though this confers the advantage of never being out of step of modernisation priorities, it blinkers one to the advantages of certain new techniques and technologies that may provide outsized advantages to the warfighter on the battlefield, but which haven't been incorporated into the procurement plans or problem statements. Organisations such as AAL fall into the latter category.

Overall, there are significant shortcomings within this wider process. A lack of centralised data sharing and institutional mechanisms lead to redundancies and inefficiencies across various DIOs. This fragmentation is exacerbated by the absence of a single overarching body to guide efforts, resulting in a confusing landscape for startups and small businesses seeking to engage with the military. There is a critical misalignment between innovators and end-users, with the armed forces often changing requirements mid-development and DIOs pursuing technologies that may not align with immediate military needs. The acquisition process is split into two parts: a relatively fast-tracked initial phase followed by a lengthy, conventional procurement process, which often causes promising technologies to falter in the 'valley of death' between development and commercialisation. The proliferation of DIOs, estimated at over 100 within the DoD, creates confusion for businesses trying to identify the appropriate consumer for their technologies. This issue is compounded by the difficulty in forecasting which emerging technologies will be relevant to the military in the long term, particularly in rapidly evolving fields such as synthetic biology and advanced materials.[109]

There is also a major cognitive gap between the two types of end-users: those designing qualitative requirements (QRs) and the actual units and soldiers. DIOs often fail to differentiate between these groups' distinct needs, leading to mismatches in product development and expectations. Small businesses, or MSMEs, and startups face particular difficulties navigating the complex DoD bureaucracy after initial entry through competitions or innovation programs. The lack of clear next steps and sustained assistance often stalls promising technologies. Many small businesses remain unaware of the funding opportunities available through various innovation initiatives.

The US DoD's acquisition process is described in some detail below. This will help place the role of the Army Futures Command in perspective later. The DoD works on a milestone framework with milestones A, B and C serving as gates to control the transition from one phase to the next. The figure below shows the various phases.

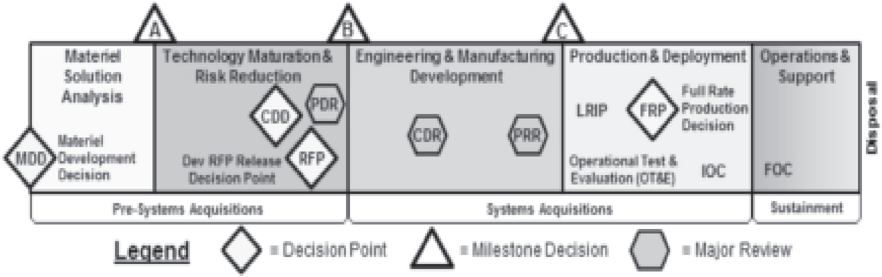

A
B
C
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
Production & Deployment
Operations & Support
Disposal
MDD
Materiel Development Decision
CDD
PDR
Dev RFP Release Decision Point
RFP
CDR
PRR
LRIP
FRP
Full Rate Production Decision
Operational Test & Evaluation (OT&E)
IOC
FOC
Pre-Systems Acquisitions
Systems Acquisitions
Sustainment
Legend
= Decision Point
= Milestone Decision
= Major Review

Figure 6: Milestone A, B and C in the US DoD's Acquisition Process[110]

There are basically five phases in the defence acquisition framework. The Material Solution Analysis (MSA) phase determines the right set of technologies to address a military need. Milestone A marks the end of this phase, transitioning into technology maturation. Technology Maturation and Risk Reduction (TMRR) focuses on reducing risks and determining appropriate technology solutions. Milestone B provides the approval to begin the Engineering and Manufacturing Development (EMD) phase. This phase develops the system design, completes all required testing and prepares for production. Milestone C approves the system for low-rate initial production.

The Production and Deployment (P&D) stage includes Low-Rate Initial Production (LRIP) and Full-Rate Production (FRP). Full Operational Capability (FOC) is achieved at the end of this phase. The last stage is Operations and Support (O&S), which is the longest phase, involving the life-cycle management of the system, including sustainment and eventual retirement.[111] Small businesses, startups and the Small Business Innovation Research/ Small Business Technology Transfer (SBIR/STTR) program[112] participants typically engage in the earlier phases of the acquisition process, such as MSA and TMRR. SBIR and STTR programs are designed to encourage small businesses to develop innovative technologies that meet specific research and development (R&D) needs of the federal government. SBIR Phase I can be viewed as corresponding to early concept exploration, which can be said to align with DoD's MSA phase, focusing on feasibility studies and conceptual design. SBIR Phase II aligns with parts of the TMRR phase, where technologies are further developed, and prototypes are created. SBIR's Phase III involves commercialising the technology for military or private sector use, despite not being funded by SBIR.[113] This can align with later stages of TMRR, EMD or even P&D, where the technology is matured enough for integration into larger systems or for direct acquisition by the DoD as part of a system.

For small businesses and startups participating in SBIR or STTR programs, it is crucial to understand where their projects fit within the DoD acquisition process. These businesses often develop critical components or technologies that become part of larger systems. They need to work closely with prime contractors (Lead System Integrators or LSI) and understand the acquisition milestones to align their development timelines with the DoD's procurement cycle.[114] Again, a major lacuna is painfully visible. Instead of being flexible enough to iterate and rapidly acquire the advantages inherent in commercial tech-based emerging and disruptive technologies, startups dealing with these technologies are usually made to align themselves with an industrial age policy of a deliberate and multi-year acquisition process.

Army Futures Command (AFC)

The organisation responsible for integrating novel technological solutions for the US Army for designing Army 2040 and delivering Army 2030 is the Army Futures Command (AFC), which was raised in Austin, Texas in 2018. It has six major functions in the field of future operational environment, research, concepts, experimentation, requirements and integration and is supported by the industry, academia and joint/multinational partners.[115] AFC has a number of teams and supporting commands under it. It follows the tradition from the Third Offset of cross-functional teams (CFTs) – overall nine CFTs have been raised with the 10th likely to be unveiled by the end of March 2024 in the field of deep sensing.[116] The existing CFTs – teams of army specialists in training and doctrine writing, sustainment experts, acquisition officers and system operators – are Air and Missile Defence (AMD), Assured Positioning, Navigation and Timing/Space (APNT/Space), Contested Logistics (CL), Future Vertical Lift (FVL), Long Range Precision Fires (LRPF), Network (NET), Next Generation Combat Vehicles (NGCV), Soldier Lethality (SL) and Synthetic Training Environment (STE).[117] With certain objectives of some CFTs getting achieved, there is also a high probability that they may be replaced by CFTs focusing on human-machine teaming (HMT), AI etc. Apart from the nine CFTs, AFC is supported by the Combat

Capabilities Development Command or DEVCOM, the Futures and Concepts Centre (FCC), Army Software Factory (ASWF), The Research and Analysis Centre (TRAC), AAL and the AI Integration Centre (AI2C).[118] Two units support AFC directly. These are the 75th Innovation Command (75IC) and the Army Test and Evaluation Command (ATEC).[119] These are the in-house innovation and S&T organisations of the army that have an outreach approach but still involve teams of army personnel and civilian scientists, technocrats and innovators working together under the US Army leadership. We will now take a look at some of these in brief, post which we will look at the various DIOs that look exclusively at the commercial sector for inducting and absorbing emerging technologies.

Combat Capabilities Development Command (DEVCOM)

US Army's DEVCOM has eight centres under it, namely, Armaments, Aviation & Missile, C5ISR, Chemical Biological, DEVCOM Analysis, Ground Vehicle Systems and Soldier Centres apart from an Army Research Laboratory (ARL).[120] Each of these centres supports one of the six priority modernisation areas of the army as the 'lead integrator' with a proportion of the rest supporting as per the requirements. For example, the armaments centre is the lead integrator for the LRPF CFT, and the ARL, C5ISR, Aviation & Missile and Analysis centres support the LRPF CFT based on the requirements.[121] DEVCOM also has the Americas, Atlantic and Indo–Pacific Forward Elements, which are used to scout for technologies in these regions that could support the US Army.[122] One of the unique aspects of DEVCOM is that it is predominantly peopled and helmed by civilians, including scientists, contractors and acquisition specialists. Apart from the centres, DEVCOM's innovation is the creation of ARL. It has three functional responsibilities: cutting-edge scientific discovery, technological innovation and transitioning capabilities for the future army. The lab consists of three departments: the Army Research Office (ARO), Research Business Directorate and the Army Research Directorate (ARD). ARO is responsible for conducting basic science research for the US Army in areas of future capabilities and reaching out to academia and industry around the globe. ARO's task is to look at a long-term horizon for capabilities that may be 20–30 years away in the making. ARD is the prime user of the research generated by ARO.[123]

In terms of internal funding and organisation, the US Army funds ARO significantly. For example, ARO's total funding for the 2022 financial year was $609 million, out of which $202 million were from the Army's Research, Development, Test & Evaluation (RDT&E) account, $57 million were from Congressional additions and $350 million from agencies such as DARPA, Office of Naval Research (ONR), Defence Threat Reduction Agency (DTRA) and the Air Force Office of Scientific Research (AFOSR), among others.[124] ARO's outreach is quite extensive and includes the Core Research Program funded by the army's basic research funds. There are six functional areas within the core program.

- **Single Investigator (SI):** Based on a three-year cycle, this program funds faculty members, graduate and post-doctoral students for the most innovative, high risk and high payoff ideas. The solicitation for proposals is based on a global broad agency announcement (BAA). The short cycle provides the army with a dynamic method to quickly analyse and invest in or reject a proposal.
- **Early Career Program (ECP):** It supports the research of young faculty members for army specific requirements and in the long run, supports their teaching and research careers.
- **Short-Term Innovative Research (STIR) Program:** It explores high-risk ideas within a nine-month cycle and seek proposals from private industry and academia. Approved projects may be shifted to SI.
- **Conferences, Workshops and Symposia Support (CF) Program:** It funds scientific and technical conferences, workshops and symposia relevant to the long-term interests of the army.
- **Research Instrumentation (RI) Program:** It improves the capacity of higher education institutions in the US to conduct research and educate scientists and engineers in the areas of national defence by providing funds to purchase instrumentation.
- **International Program:** Now placed under the military department (MILDEP)'s international program, this coordinates with DEVCOM's Forward Elements to search for S&T opportunities for the US Army's needs in the international arena.[125]

Three University Affiliated Research Centres (UARCs), that is, the Institute of Collaborative Biotechnologies at University of California, Santa

Barbara; the Institute for Creative Technologies at the University of Southern California; and the Institute for Soldier Nanotechnologies at the Massachusetts Institute of Technology (MIT) are also funded by the US Army and managed by ARO.[126] Apart from this, ARO manages three foundational research centres, that is, the Army Centre for Synthetic Biology, Army Ultra Wide Bandgap RF Electronics Centre and Army Energetics Basic Research Centre as well as the university research initiative (URI).[127] The lab also participates in the SBIR and manages the STTR program for feasibility studies on demonstration of prototypes. The SBIR program's priorities include enabling technological innovation, increasing private sector commercialisation of innovations granted through US federal government's R&D and using small businesses to participate in the federal government's R&D requirements.[128] The SBIR program is structured in three distinct phases.

Phase I is the feasibility study phase, where the aim is to establish the technical merit, the feasibility and commercial potential of the proposed R&D efforts and to determine the quality of performance of the small businesses prior to providing further federal support in Phase II. Typically, Phase I awards are smaller in amount and shorter in duration. Phase II focuses on the development phase, where the initial R&D efforts are expanded upon to produce well-defined deliverables. Phase II is intended to continue the R&D efforts initiated in Phase I. Funding is based on the results achieved in Phase I and the scientific and technical merit and commercial potential of the project proposed in Phase II. Phase III is intended for the commercialisation of the innovations developed during Phases I and II. Phase III does not involve SBIR funds; instead, the small business or research institution is expected to obtain funding from the private sector or other non-SBIR federal agency funding. STTR is a sister program to SBIR that also supports R&D. The key difference is that STTR requires the small business to formally collaborate with a research institution (often a university, federally funded research and development centre or non-profit research institute) in both Phase I and Phase II. STTR is designed to bridge the gap between basic science and commercialisation of resulting innovations. Like SBIR, STTR also has three phases following the same structure as SBIR, with a strong emphasis on the transfer of technology from research institutions to the market.[129]

ARO also receives funding from the Office of the Secretary of Defence

(OSD) for managing three programs: Research and Educational Program (REPs) for minority institutions, National Defence Science and Engineering Graduate (NDSEG) Fellowships and High School Apprenticeship and Undergraduate Research Apprenticeship programs. ARL has identified 11 foundational research competencies in the areas of Biological and Biotechnology Sciences; Electromagnetic Spectrum Sciences; Energy Sciences, Humans in Complex Systems; Mechanical Sciences; Military Information Sciences; Network, Cyber, and Computational Sciences; Photonics, Electronics and Quantum Sciences; Sciences of Extreme Materials; Terminal Effects; and Weapons Sciences. These competencies support 11 Essential Research Programs (ERPs), which are cross-disciplinary programs identified with quantifiable end points.[130] These competencies are:

- **Artificial Intelligence of Maneuver and Mobility (AIMM)**: AIMM ERP supports NGCV-CFT in developing autonomous capabilities for ground vehicles for the US Army. It works in conjunction with DARPA's Robotic Autonomy in Complex Environments with Resiliency (RACER) program and other academic partners. It has three internal thrust areas and two external cooperative research programs. Thrust 1 uses ML to enable the ground vehicle to negotiate complex terrains. Thrust 2 improves autonomy during reconnaissance by using natural language processing (NLP) for soldier interaction, context-aware perceptual processing and reasoning about mission context under time and resource constraints. Thrust 3 attempts to form collaborative teams of autonomous systems and uses reinforcement learning (RL) for developing cooperative autonomous behaviour to deal with adversaries. The two external initiatives are Scalable, Adaptive and Resilient Autonomy (SARA), which invites solutions in autonomy from academic institutions and Tactical Behaviours for Autonomous Maneuver (TBAM) Collaborative Research Alliance (CRA), whose aim is to 'develop coordinated behaviors for small groups of autonomous agents to perform doctrinal as well as novel tactical maneuver in realistic simulations of complex military-relevant environments'.[131]
- **Emerging Overmatch Technologies (EOT)**: EOT ERP looks at the issue of enhancing protection of combat vehicles by using autonomy.

The program also examines the issue of protectiveness through the lens of emulating combat vehicle behaviours by autonomous agents for increasing the speed of decision making.[132]

- **Foundational Research for Electronic Warfare in MDO (FREEDOM)**: FREEDOM ERP enables persistent and survivable situational awareness in global positioning system (GPS)-denied environments, develop novel RF, cyber technique, hardware and sensor architectures for closed-loop EW. The program also looks at EW fingerprinting and options for disaggregated and adaptive EW.[133]
- **Human Autonomy Teaming (HAT)**: The aim of HAT ERP is to see how future military systems can distribute cognitive and computational resources for better utilisation of capabilities in a mixed MUM-T; improve data collection for assessing soldier autonomy teams; enable soldiers to train autonomous systems at the edge; and improve resilience and adaptiveness of the mixed teams.[134]
- **Long Range Distributed and Collaborative Engagements (LRDCE)**: This ERP supports LRPF-CFT in the field of ballistic science for overmatch in energetics, propulsion, flight, guidance and warheads. Specifically, the program looks at increasing the range, speed and manoeuvrability of projectiles, accuracy of long-range fires in a contested environment and improvement in munition survivability.[135]
- **Physics of Soldier Protection to Defeat Evolving Threats (PSPDET)**: There are three thrust areas in this ERP, namely, terminal ballistics, armour materials and computational mechanics. The aim is to improve the survivability of the warfighter in terms of ballistic protection from future combat threats and enhance soldier battlefield effectiveness.[136]
- **Quantum Information Sciences – Position, Navigation and Timing (QIS-PNT)**: This ERP focuses on improving the manoeuvrability, fires and communication capabilities of the US Army through improvements in accuracy and resiliency of army's PNT and quantum sensing capabilities. In effect, QIS-PNT aims to provide high-precision positioning, which is more precise, robust and unhackable than GPS. Additionally, the ERP has developed a host of sensing capabilities based on quantum mechanics, which have the potential

to revolutionise sensing and communications. For example, a microelectromechanical system (MEMS) inertial sensor has been developed using a resonant quadruple-mass gyroscope (QMG), which can provide navigation-grade performance.[137]

- **Transformational Synbio for Military Environments (TRANFORME)**: TRANSFORME aims to revolutionise US military readiness by leveraging synthetic biology for developing advanced materials and rapid countermeasures, enhancing logistics and operational adaptability. Its focus is on creating synthetic biology (synbio) capabilities for adaptive protection, and agile tools for innovative, cost-effective materials.[138]
- **Versatile Tactical Power and Propulsion (VICTOR)**: The objectives of this ERP are to develop comprehensive expertise in material science, design, sensing and control to enable autonomous systems with efficient energy solutions, optimising hybrid-electric propulsion for stealth, reliability and range in contested environments. The impact of the program has been enhanced unmanned aircraft systems (UAS) performance and survivability via agile, silent, multi-fuel propulsion systems and superior energy management, bolstering operational effectiveness and lethality through advanced propulsion and power distribution.[139]

Futures and Concepts Centre (FCC)

The FCC can be thought of as a bridge that connects the various US Army formations involved in warfighting with the innovations and new S&T concepts emanating from DEVCOM through the four core functions of concepts, experimentation, requirements and integration. It comprises solely uniformed personnel and consists of the Joint Modernisation Command (JMC) and various capability development and integration directorates (CDID), including cyber, aviation, fires, intelligence, manoeuvre, manoeuvre support, medical, mission command and sustainment CDIDs.[140] JMC is the unit responsible for planning and conducting exercises for the US Army's goals of 2030 and 2040. It consists of three operations groups: Operations Group Alpha and Bravo conduct the PC exercises, joint warfighting assessments and other Persistent Experimentation Events.[141] They are used to test and exercise concepts related to MDO, conceptual and technical interoperability including joint and multinational and ensuring that emerging technologies are integrated into the exercises. Operations Group Zulu integrates special forces, cyber and space in the exercises.[142]

PC, as the army's 'campaign of learning', plays a crucial role in integrating the army into the joint forces and advancing the Department of Defense's (DoD) Joint All Domain Command and Control (JADC2) vision.[143] This annual event, characterised by experiments, technology evaluations and soldier feedback, is centred around five core elements: soldiers, weapons systems, command and control, information and terrain. PC 2020, held at Yuma Proving Ground, Arizona from August 11 to September 01, 2020 with about 500 personnel, was aimed at enhancing the 'close fight' through the integration of new technologies at the tactical level.[144] It focused on Brigade Combat Teams (BCTs), Combat Aviation Brigades (CABs) and Expeditionary Signal Battalion-Enhanced (ESB-E), involving systems such as the MQ-1C Grey Eagle unmanned aerial vehicles (UAV) and Air Launched Effects (ALE).[145]

Experiments included using low-earth orbit (LEO) satellites and UAVs for rapid target acquisition and engagement, demonstrating a process that could be completed within 20 seconds. PC 2021 expanded the scope to include about 7,000 personnel and 107 different technologies. Conducted across multiple US installations from October 12 to November 10, 2021, PC 21 explored penetrating A2/AD capabilities and integrating AI, ML and autonomy across domains. Units such as the Multi-Domain Task Force (MDTF) and elements from the 82nd Airborne Division participated, with scenarios testing joint situational awareness, defence against missile attacks, joint fires operations and AI-enabled reconnaissance, among others.[146]

However, while planning the next iteration of PC exercises, it was felt that lessons learnt during these exercises were not being absorbed at the same pace therefore the yearly 'rhythm' of the conduct of the exercises has been broken to be replaced by a continuous series of small exercises, culminating in a major test of a majority of the service's capabilities to integrate the other two services, multi-national partners and most importantly, emerging technologies. PC 24 will be executed in two phases, at two locations, that is, Marine Corps Base Pendleton and Fort Irwin, both in California. Operations will focus on 'air, sea, space and cyberspace domains, as well as focus on inter-service cooperation, offensive and defensive fires, and ensuring the right sensors deliver the right information to the right force at the right time'.[147] The army's PC initiative is trying to coordinate with the US Air Force's Advanced Battle Management Systems (ABMS) and the US Navy's Project Overmatch, with efforts to ensure compatibility and ease of data sharing between systems.[148] PC provides a near-similar battle inoculation environment for companies and soldiers to interact with new systems and technologies, and has led to a number of inductions.

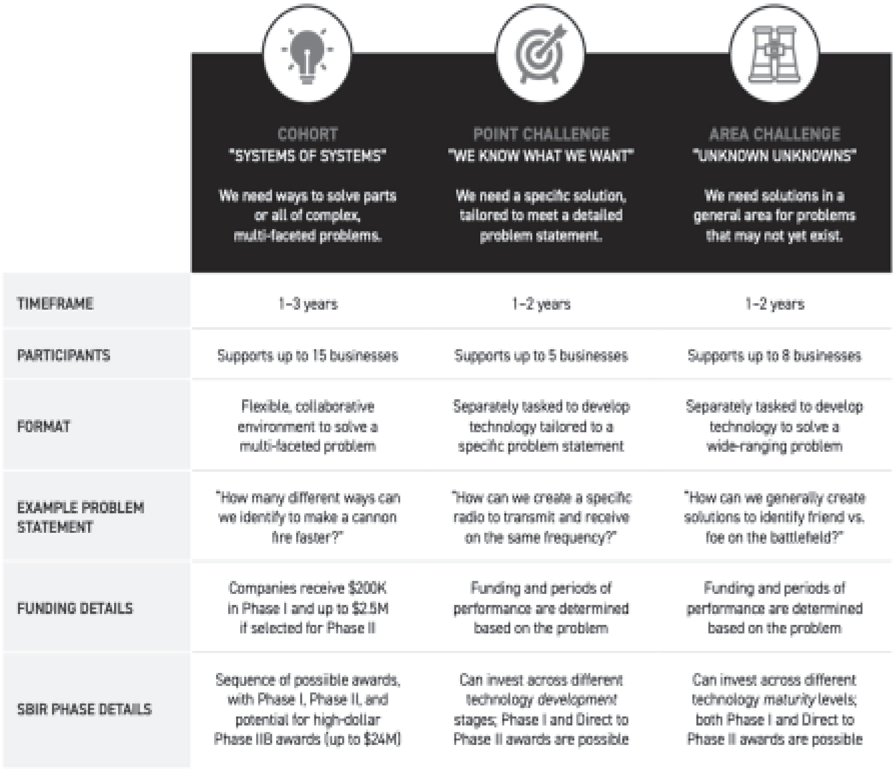
Army Software Factory (ASWF)

ASWF has three overarching priorities. It intends to enable army soldiers to be proficient in IT skills to cater for a digitised battlefield in the future, solve current army problems using cloud and cyber security and finally create a body of soldiers that can fight through a complex and contested environment on a self-sustaining basis rather than looking at centralised command post for 'debugging' issues.[149] This is in view of the increasingly sophisticated and networked capabilities that the US Army will field in view of MDO. Training in ASWF is soldier-centred and consists of three phases.

The first phase is the technical accelerator (six months) and lays a common foundation for the members. The second phase is that of subject matter expert (SME) training for six to 12 months. Here the batch of trainees is broken into sub-groups, assigned an army problem and paired with an industry expert. The third and final phase is that of sustained factory, which is of 18–24 months duration and is meant to crystallise the members into steady state product teams and branch some off to act as SMEs for the incoming batch. Four 'tracks' or specialisations are currently envisaged for ASWF, which are product manager, user experience (UX)/user interface (UI) designer, software engineer and platform engineer.[150]

Army Applications Laboratory (AAL)

AAL is known as the US Army's innovation unit and matches companies with army stakeholders, including other commands and even individual units. The focus areas for AAL are power and energy (low-power electronics, compact power sources); human performance enhancement through AR/VR; robotics and tactical AI; and CL (robotics and autonomy). AAL performs three major functions of market intelligence, solution evaluation and solution innovation.[151] It has a flexible funding model that mixes various government funding with private capital. The ultimate aim of AAL is to match army sponsor organisations with technologies or companies either through CFTs or by directly interacting with an operational unit. One of its models called Special Program Awards for Required Technology Needs (SPARTN) aims to fast-track convergence of end users and small companies using methods such as faster contracting speed by involving acquisition teams early so that the new technology can be built into recurring budgets.



	COHORT "SYSTEMS OF SYSTEMS" We need ways to solve parts or all of complex, multi-faceted problems.	POINT CHALLENGE "WE KNOW WHAT WE WANT" We need a specific solution, tailored to meet a detailed problem statement.	AREA CHALLENGE "UNKNOWN UNKNOWNS" We need solutions in a general area for problems that may not yet exist.
TIMEFRAME	1–3 years	1–2 years	1–2 years
PARTICIPANTS	Supports up to 15 businesses	Supports up to 5 businesses	Supports up to 8 businesses
FORMAT	Flexible, collaborative environment to solve a multi-faceted problem	Separately tasked to develop technology tailored to a specific problem statement	Separately tasked to develop technology to solve a wide-ranging problem
EXAMPLE PROBLEM STATEMENT	"How many different ways can we identify to make a cannon fire faster?"	"How can we create a specific radio to transmit and receive on the same frequency?"	"How can we generally create solutions to identify friend vs. foe on the battlefield?"
FUNDING DETAILS	Companies receive $200K in Phase I and up to $2.5M if selected for Phase II	Funding and periods of performance are determined based on the problem	Funding and periods of performance are determined based on the problem
SBIR PHASE DETAILS	Sequence of possiible awards, with Phase I, Phase II, and potential for high-dollar Phase IIB awards (up to $24M)	Can invest across different technology development stages; Phase I and Direct to Phase II awards are possible	Can invest across different technology maturity levels; both Phase I and Direct to Phase II awards are possible

Figure 7: Detailed structure of AAL's SPARTN Program[153]

The program has three phases. Phase 1 is where multiple companies work on problems and engage with end users. This phase culminates with a concept demonstration to army stakeholders. The second phase involves retaining some companies for a period of performance to advance their technology and for some projects, these companies can ask for additional funding from the government provided they can demonstrate evidence for a one-for-one match from the private sector. In the third and final phase, the selected companies can access higher value contracts and in the end be registered as a program of record within the army, which is an official term for being recognised as a formal inventory item. SPARTN uses three different types of funding approaches. These are cohort, point challenge and area challenge.[152] Detailed information about these programs is given below in the form of an infographic.

Artificial Intelligence Integration Centre (AI2C)

AI2C is located in the Carnegie Mellon University (CMU) and is responsible for planning, integrating and operationalising AI efforts within the army. The centre lists five core competency areas, which are infrastructure and data; workforce development; transformation of platforms; AI governance and partnerships; and AI ethics.[154] AI2C supports the planning parameters of AFC's CFTs and is most deeply involved in ramping up capacities of the US Army to showcase at the annual PC exercises.[155] CMU also hosts DoD's Advanced Robotics for Manufacturing group,[156] and there is a likelihood that a new Robotics Innovation Centre is going to be constructed soon, adding to the possibility of AI2C moving beyond software solutions to systems that act and change the physical environment directly.[157]

A team of faculty from CMU has been awarded a $10.5 million contract for using predictive AI for fighter planes through AI2C.[158] There are three pathways that AI2C is looking at for providing capabilities from startups. These are the data analyst pathway through Heinz College. This confers a master's degree in information systems management with a specialisation in business intelligence and data analytics. The other is data engineer through the School of Computer Science with a master's in computational data science degree. The third is the autonomous systems engineer pathway, which is through the College of Engineering for master's of science and engineering in AI. This is the data science team at the apex of the triangle shown below. Next comes the AI technicians, which form the connecting level for both the AI scholars as well as the AI users. AI technicians also integrate horizontally with engineers from ASWF and the cyber capabilities division. Finally, at the base is the AI users course, which provides a ground understanding of how AI is meant to be utilised within the force. Integration of ethics is paramount at every level of AI development and use, from users to leaders.

This section on the US innovation ecosystem will be the largest and most comprehensive amongst all other countries' models due to the availability of all doctrines, organisations and critiques in the open domain. The US DoD is amongst a very few that has managed to articulate all parts of the innovation system, though it suffers from discontinuities and lack of a causal change.

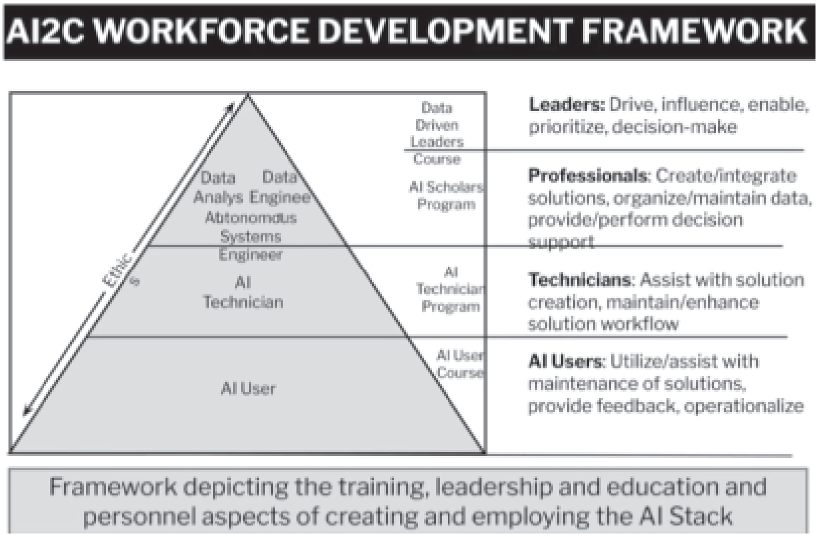

AI2C WORKFORCE DEVELOPMENT FRAMEWORK
Data Driven Leaders Course
AI Scholars Program
AI Technician Program
AI User Course
Data Analys
Data Enginee
Abtonomous Systems Engineer
AI Technician
AI User
Ethics
Leaders: Drive, influence, enable, prioritize, decision-make
Professionals: Create/integrate solutions, organize/maintain data, provide/perform decision support
Technicians: Assist with solution creation, maintain/enhance solution workflow
AI Users: Utilize/assist with maintenance of solutions, provide feedback, operationalize
Framework depicting the training, leadership and education and personnel aspects of creating and employing the AI Stack

Figure 8: A graphical representation of the AI2C Workforce Development Model[159]

Zooming out, it is easy to get entangled and confused in the sea of alphabets and abbreviations that characterise the US defence or military innovation ecosystem. A number of agencies deal with defence startups to incorporate new technologies within the forces, apart from organic laboratories and innovation setups. However, it is necessary to reiterate certain issues that merit attention on a broader scale. The US MDO concept still functions on the assumption of conventional warfighting despite the emphasis on integrating emerging and disruptive technologies. Though organisations such as DIU and NavalX, AFWERX and others have reached out to hi-tech firms in the Silicon Valley, the priorities remain conventional warfighting platforms and how the new technologies can fit into an existing framework. The events in Ukraine, Gaza and before them, Armenia have shown that disruptive technologies create asymmetric effects on the tactical battlefield. The issues of leveraging commercially available off the shelf (COTS) equipment and adapting to a do-it-yourself (DIY) version has still not been internalised by

US forces.[160] This is also due to a vision that imagines future wars to be intense state on state combat involving conventional and so-called legacy systems, though with substantial technological improvements.

Though all documents and doctrines refer to the phase of peacetime competition using niche technologies and concepts to prevail in the grey zone, the underlying foundation is that of using legacy platforms. Another issue is that while the Third Offset strategy was correct in assuming that novel technologies will change the character of war, its implementation on ground has led to a fragmented approach in identifying, developing and adopting commercial technologies, where none of the innovation organisations function as part of an integrated system. Instead, the idea is to patch a number of commercial solutions to problem statements given by units/ formations or suo-moto proposals by the companies themselves. This results in adoption but not absorption since issues of compatibility, complementarity and scale occur often. Thirdly, and finally, the US military despite its multiple DIOs and innovators, still hasn't grasped the concepts of the new and evolving DIY warfighting paradigm of three Cs, that is, compute, collaboration and compatibility where speed, scale and rapidity are of paramount importance. The three Cs framework necessitates that free and open-source software (FOSS), open-source hardware (OSH) and COTS equipment be leveraged to rapidly equip the units and soldiers at the cutting edge with a significantly massive quantity of systems that can talk to each other, provide soldiers with situational awareness and speed up the sensor-processor-shooter link through ruggedised and intelligentised communication links.[161]

It is only with the lessons gleaned from the Russia–Ukraine conflict and the recently conducted Armenia–Azerbaijan war that the US military has started thinking seriously about the importance of mass of relatively low-cost unmanned systems as a means of countering Chinese superiority in numbers. The Replicator initiative, for example, aims to induct thousands of 'attritable autonomous systems' across the three Services in all domains within 18–24 months. So far, the US Army has homed on to the Switchblade 600 one-way attack drone for induction with two more systems on the way.[162] The US Navy and the US Air Force are also looking at the commercial sector to provide them similar capabilities in the fields of unmanned surface vessels (USVs) and loitering munitions.[163] There is a lot of secretiveness surrounding the initiative with details such as funding streams, type of platforms and names of vendors not being available in the open domain. However, reports from various news outlets have revealed that the Pentagon is aiming at spending close to $1 billion in the next two years on this initiative.

Apart from finding new attritable system vendors, the US DoD is also looking at fast-tracking projects of a similar nature that are either in the services' or combatant commands' pipelines. The budget of one billion dollars is likely to be divided in two tranches of $500 million each for financial year (FY) 2024 and 2025.[164] It is also likely that DoD may shut down or curtail certain programs to finance the initiative. For example, the FY2025 budget, which allots close to $186 billion for the US Army will see the service investing heavily in R&D and the purchase of unmanned systems for ISR, specifically the Future Tactical Unmanned Aircraft System (FTUAS) and Air Launched Effects (ALE), the latter being developed and supported by the FVL CFT.[165] The likely induction of UAS under the Replicator initiative may mark a turning point for a service that still sees the fielding and deployment of heavy duty traditional platforms in a future scenario as the more likely deployable option. Despite this and as seen from the proportion of money allotted to traditional platforms and military contractors vis-à-vis emerging technologies and commercial sector, the gap is visibly wide. All the efforts by entities such as DIU notwithstanding, the US military still depends on legacy platforms for its war-waging capabilities.

Before ending this section, it is also important to stress that the US Army did attempt opening a venture capital fund of its own. Known as the Army Venture Capital Corporation (AVCC), it was established in 2002 by the US Congress and was meant to provide seed capital to promising defence startups and individuals in the field of national security and defence applications that could be used by the army.[166] The army brought in Jake Chapman, a trained lawyer who led firms in the biotech and aerospace sectors to revitalise AVCC and for some time it looked that he would be able to do so, but the basic mismatch of philosophies between a hierarchical, highly bureaucratic organisation, that is, the US Army and the fail fast and high risk functioning of VC firms did not align, and the AVCC seems to have been closed for good. There is not much information in the open domain regarding AVCC and the fact that Mr Chapman has opened a new VC firm lately called Marque

Ventures in the field of national security and defence tech, seems to suggest that AVCC has been closed.[167] The VC firms in the US have, however, marked out the defence tech sector as one of the most lucrative markets.[168]

The creation of Shift, a program founded by six of the top VC firms in the US, including Andreesen Horowitz, Box Group, Expa, PeopleTech Partners, Structure Capital and Tim Ferriss, is unique in its vision. The Shift Fellowship Program embeds high-potential individuals from DoD within top VC firms and defence-focused startups. The program facilitates knowledge exchange, increased retention rates, improved industry engagement and attracts private investments.[169] The result is that both sides are able to understand each other's strengths and challenges. The program under which this convergence happens is known as the Defence Ventures Program, and this is the only private initiative to have been mentioned in the National Defence Science and Technology Strategy of 2023. However, the program was not renewed for 2024.[170] The reasons may have been varied, but at least this program has attempted something unique and as we will see in the case of Ukraine, this is a model that some countries have started following more seriously. One of the grouses of the private sector, especially the sector called 'non-traditional defence contractors' is that it is very difficult for industry and investors to validate demand signals from DoD, leading to either intuiting it for the department and wasting significant amount of money or looking at the most lucrative areas where most of the investment is taking place, skewing the field even more. While China takes the cake in implementing its military-civil fusion strategy (MCF), Ukraine, through the BRAVE1 defence tech cluster, is also doing the same thing, albeit more efficiently than the Americans. It needs to be mentioned, however, that successful induction of commercial tech does not necessarily lead to a positive military outcome for the side inducting since there are numerous factors that come into play during war and warfare.

The Israeli Defence Forces

The failure of Israeli intelligence to detect Hamas's attack on 07 October 2023 has been attributed to over-reliance on technological superiority within the Israeli strategic community.[171] Notwithstanding the critique, one needs to acknowledge the culture of innovation embedded within Israel's Ministry of Defence (IMoD) as well as the Israeli Defence Forces (IDF), which are known for devising novel weapons and technological platforms in a telescoped time frame, and that too repeatedly. Known as 'macroinnovation', this form of innovation is always bold, unheard of and takes advantage of the 'countermeasures holiday', which comes from fact that no counters can be developed for a platform that no one has heard of.[172] Between the time it takes to understand the technology or platform, witness it in action on the battlefield and then start an R&D cycle for a counter, the prime mover advantage will go to the side wielding it first. Being surrounded by hostile actors and continuously in battle against multiple adversaries, the IDF has pioneered military macroinnovation, which is also known as qualitative military edge (QME).[173]

QME involves both the induction as well as the operation of sophisticated weapons and technologies. The IDF and IMoD have been known for their pioneering macroinnovations and are now leveraging the same in the field of emerging technologies. But before delving into the process, it is important to know the structure and history that sets IDF apart from its military counterparts in other countries, as well as certain innovations that the force has devised since its inception in 1948. As per authors Edward Luttwak and Eitan Shamir, IDF's novelty and the way it approaches development of new weapons and technologies is defined by a philosophy of scarcity and optimisation.[174] While a big component of scarcity is in the way the force is structured in terms of ranks and a deliberate shortage of senior officers, the optimisation is in terms of a single General Staff and a single IDF HQ responsible for operations, planning, induction and administration of the entire force, including the Israeli Air Force and the Navy. These are not separate forces in the conventional sense, as is evident from other countries, but are controlled by a common General Staff. Also, the Directorate of Defence Research and Development (DDR&D or MaFat in Hebrew) is the sole agency responsible for R&D for all three forces.[175] We will look at its role in detail in the succeeding paragraphs.

Coming back to the issue of scarcity and optimisation, one can appreciate that the artificial shortage of senior officers at the top forces the mid-rung and junior officers to come up with innovative solutions for novel situations and challenges. The IDF General Staff also passes broad directives and instructions during operational planning, providing significant room for interpretation and manoeuvre to officers and soldiers to complete their task using their problem-solving skills and ingenuity. In terms of optimisation, IDF has a single service structure. It has one commander with the title 'Head of General Staff' who is under the immediate authority of the defence minister and overall authority of the Prime Minister as the head of the cabinet.[176] This setup does away with the notion of conflicting priorities of different arms and services, optimising the budget for weapons and platforms actually required by the forces, without fighting over funding issues. The next innovation and one of the most critical ones for the state of Israel has been the concept of reserves.

While everyone has to mandatorily serve in IDF for a period of two years, these individuals then move into the reserve category where they have to attend a month of training each year, with the rest of the time available for their civilian careers. In order to mobilise the reserves in time, an effective early warning system has been instituted. This innovation ensures that the IDF is able to sustain itself in peacetime with a comparatively small team of conscripts and a smaller core group of careerist officers without the requirement of a bigger standing army, which may be difficult for a country with a total population not even crossing 10 million.[177] This innovation has also ensured an informal hierarchical culture within the IDF where even the junior most soldiers can approach the senior hierarchy, pitch his/her ideas, and if found valuable, these ideas are used to modify tactics, strategies and development of weapon platforms.[178] There is no requirement of a formal qualification or being in any particular position or appointment for suggesting a new idea. In many cases, the IMoD or IDF also provide funding for these efforts. Another advantage of a huge reservist corps is the revolving door policy where reservists can directly get in touch with troops and work at the cutting edge of technology, expedite creation of solutions for the warfighter.[179]

The IDF has been at the forefront of many firsts in the history of modern warfare and it is important to have a brief look at what it has accomplished in the last seven decades, in terms of scale, capabilities and innovations. The list of IDF's achievements includes the creation of the Iron Dome, air-launched armed decoys and RPVs (forerunners of today's UAVs and drones), tactical stealth submarines, helmet-mounted display (currently in use with F-35

Lightning IIs), Trophy active protection system for armoured vehicles, the Iron Fist, reactive armour boxes and even multirole fighter jets (1950s).[180] IDF has also been credited with fighting the first computerised war with the use of a data processing system called Periscope for fusing data from multiple sources and then directing multiple sorties of fighter-bombers stacked at various altitudes. This was during the Syrian war of 1982.[181]

These achievements were made possible due to the improvisation and innovation culture embedded within IDF. Two major factors that enhance this culture are the lack of institutional traditions and mores and the IDF being the pre-eminent educational institution within the country.[182] The former ensures that traditions or culture do not stifle innovation as at times innovation actually means moving fast and breaking things. The latter is responsible for imparting critical life skills, literacy and advanced academic opportunities to conscripts, including those from disadvantaged backgrounds. Its distinctive, improvisational ethos champions innovation, allowing ideas to be heard and developed regardless of formal qualifications, fostering an environment where creativity and problem-solving are paramount. This culture positions the IDF as an incubator for groundbreaking advancements, accessible to both Israelis and international contributors.

For example, Unit 8200, part of IDF's Intelligence Corps, is known as 'the best tech school on earth', whose functions include signals intelligence (SIGINT), decryption, cyberwarfare and cybersecurity.[183] While its main aim is to provide advance warning to the government and IDF, it also undertakes significant offensive cyber operations in order to pre-empt certain actions by hostile actors.[184] Some of its successes include the monitoring of Ugandan army communications and air movements during Operation Entebbe in 1976 and foiling an airline bombing plot hatched by ISIS in 2017. The unit, along with American agencies, has also been suspected of being behind the creation of the Stuxnet malware that disabled Iranian nuclear centrifuges.[185] Admission inside the unit is not voluntary but is based on constant monitoring of academic scores of high school students, which is followed by an invite for testing and selection. Those with knowledge and proficiency in Arabic and other Middle Eastern languages as well as high scores in computer science, mathematics and physics, generally receive higher priority while selection. The unit gets priority over all units of IDF. Alumni of Unit 8200 have gone on to found leading tech companies, including Check Point Software Technologies, one of the world's leading cybersecurity firms. The unit's focus on signal intelligence and decryption has provided its members with unique skills in problem-solving, cybersecurity and software development.[186]

Coming to the official structure of the innovation organisation(s) within IMoD and IDF, the official organisation is the MaFat or DDR&D. MaFat is a cornerstone of military technology expertise within the country, crucial for maintaining Israel's qualitative military edge. It embodies a collaborative effort between civilian and military personnel, led by a director appointed through a joint agreement by the Minister of Defence, the Chief of the General Staff, and the Ministry of Defence Director General.[187] This entity stands at the forefront of developing, producing and maintaining advanced defence technologies for the IDF and the broader defence establishment. MaFat has five major units under it.

The units are the Military R&D unit that has two functions, namely, conducting research and promoting technology and 'building blocks for future systems'; and monitoring and ensuring the progress of prototypes to 'full scale development'. This unit collaborates with academia, research institutes, tech companies and defence industries. It consists of uniformed as well as civilian personnel who have advanced engineering degrees. This unit is further sub-divided into multiple departments. These include the Missile and Rocket Department, which has been pivotal in driving the innovation and development of rocket and missile systems tailored to a spectrum of operational needs, ensuring IDF maintains superiority across air, land and sea.

The needs of the IDF include crafting solutions for aerial defence, precision targeting of ground objectives, engaging in land-based operations within hostile territories and securing naval dominance with advanced missile technologies, as well as supporting aircraft and UAVs. It is also behind some of the defence market's most sophisticated systems, such as the Iron Dome missile defence system, alongside a host of advanced missiles for air-to-air, anti-tank and ground-to-air engagements. Other departments include the Armament Systems department (created Trophy active protection system and develops 'unmanned vehicles, weapons and ammunition, non-lethal weapons' and 'future combat vehicles'); Optronics Department (development of laser systems, technology components and antennas for electro-optical systems); Communications, Command and Control Department (responsible for cyber, communication, satellite communication, command and control systems, navigation, visual information processing and mapping); Systems Department (all RF sensors and R&D in the domains of SIGINT, radar, EW and underwater acoustics); Small Units Department (microelectronics for radar, communications and other systems); Performance Analysis Department (responsible for assisting in the decision-making process and development of technology, particularly during the early stages); and finally, the Chief Technology Officer (CTO) Department for R&D in emerging and cutting edge technologies. The CTO department integrates the R&D efforts of the IDF, IMoD, deals with the R&D of dual use technology and manages IMoD's Innovation Centre.[188]

The second unit under MaFat is the Science and Technology Unit, previously called the Unit for Research and Technological Infrastructure. It is a scientific research organisation that is responsible for identifying and developing scientific solutions for IDF's current and future security needs. It deals with subjects and topics such as infrastructure, facilities and simulators, quantum technology, nanotechnology, military medicine, autonomous systems, aerospace engineering and chemical and energetic materials. This unit also conducts interdisciplinary research and interacts and collaborates with international researchers and academics.[189] The third unit is Israel's Missile Defence Organisation (IMDO), which oversees the development and enhancement of Israel's multi-layered defence systems. These systems include the Arrow-2, Arrow-3, David's Sling and Iron Dome, each designed to protect against a range of airborne threats.[190] Historically, the IMDO's formation was catalysed by a 1985 memorandum of understanding (MoU) with the US for missile defence against long-range threats, leading to the Arrow program's initiation.

The Iron Dome, operational since 2011, is the world's first system to intercept short-range rockets and UAVs, showcasing a high success rate during operations such as Pillar of Defence (2012) and Protective Edge (2014). Developed in collaboration with the US, key contractors include Rafael Advanced Defence Systems, Elta and mPrest. David's Sling, operational since 2017, addresses threats from large calibre rockets and short- to medium-range ballistic missiles. It represents a pivotal component of Israel's aerial defence, developed jointly with the US, with Rafael, Raytheon, Elta and Elisra as main contributors. The Arrow-2, part of Israel's upper-layer defence, was fully deployed by 2002 and is designed for medium to long-range missile interception, with Israel Aerospace Industries (IAI) as the primary contractor. Arrow-3, operational since 2017 and developed alongside the US Missile Defence Agency (MDA), extends defence capabilities with its high-altitude, long-range missile interception ability. Key partners include IAI's MLM division, Elisra, Boeing, Tomer and Rafael.[191]

The fourth organisation is the UAV Administration, which was established in 2001 and is responsible for developing cutting-edge UAV systems and sub-systems, including payloads. IDF currently operates four types of UAVs: Eitan (Heron TP), Shoval (Heron 1), Hermes 450 and Hermes 900. All UAVs are classified into three tiers: upper tier with a maximum altitude of 40,000 feet and a carriage capacity of up to a ton of fuel and systems; intermediate tier with maximum altitude of 20,000 feet; and the lower tier with a maximum altitude of 5,000 feet are used by IDF Ground Forces for reconnaissance.[192] The fifth major organisation is the Space and Satellite Administration, which was established in the 1980s and is responsible for the 'development of satellites and launchers, guaranteeing Israel's independence in space'. The organisation has spearheaded Israel's launch of its indigenous Ofek series satellites.[193]

In terms of emerging technologies, the IDF and IMoD have devised a three-pronged approach, most of whose elements have already been detailed in previous paragraphs. The first is to create an elite corps of military innovators, second to use proof of concept and technological prototypes directly in operations in order to ensure a spiral development model and finally, to maintain a close relationship between military R&D, front line units and the commercial world. For the last part, reservists are the common link. Not only do they serve and are ready to be re-enrolled into the IDF at a moment's notice, but in the peacetime they also head some of the leading tech, management and manufacturing companies in Israel. Since almost all citizens have operational experience, in conventional or counterinsurgency/counter-terrorism (CI/CT) operations and there are always family members involved in ongoing operations, the level of personal involvement and attention to detail is extensive. The added urgency of getting the best technology in the hands of the soldier makes for a unique combination where the attempts to absorb latest and niche technology is one of the world's highest. Under MaFat, the Talpiot (bastion in Hebrew) and Psagot programs are meant to create an elite group of scholars and soldiers, who are excellent engineers and scientific researchers, especially in the fields of mathematics, computer science and physics plus are aware of the challenges facing the fighting force in the field.

The Talpiot program, conceptualised in 1979, recruits 50 of the brightest Israeli students annually and then puts them under three years of 'rigorous training in research, development and ethics of the defence establishment', which includes training and interaction with all types of units so that the Talpiot graduates (known as Talpiots) are aware of the peculiarities of each platform and system. Projects such as the Trophy active protection system, Iron Dome and Arrow all originated as Talpiot projects. Post their training, Talpiots serve for six more years as commissioned officers in various military units and R&D organisations, after which some of them are absorbed in the regular IDF while most become successful entrepreneurs in the vibrant startup ecosystem in Israel.[194] Another program called Psagot involves a similar approach as the Talpiot program but instead of selecting officers adept in both science and war fighting, it aims to train and induct scientists and technologists who can research cutting-edge technologies in defence R&D establishments.[195]

The second part is bridging the gap between invention and operational deployment, or VoD. For this, Israel employs operational demonstrator experiments, facilitated by MaFat. This process is crucial for disruptive innovations that lack formal requirements, allowing for rapid development and testing in real-world conditions. Given that Israel doesn't have government defence laboratories, the defence industry is responsible for advancing new military technologies from the drawing board to the battlefield, with MaFat's financial support ensuring that these innovations progress through to the operational demonstrator phase. In this phase, prototypes are field-tested by IDF units, providing critical feedback for technological refinement and building military support for the technologies.

This approach is characterised by its speed and willingness to embrace risk – attributes made possible because operational demonstrators are part of

R&D efforts rather than formal military acquisition programs. The IDF's role is primarily to select units for participation, with MaFat managing the financial support. This structure gives MaFat the flexibility to shift funds between projects as needed, facilitating the execution of multiple demonstrator projects each year. Prototypes are usually introduced to units during training sessions. However, due to the IDF's active engagement in various operations, these technologies often see combat sooner than anticipated. This real-life testing environment not only accelerates the refinement process but also aids in garnering essential military backing for the technologies. For example, the Iron Dome system's prototype batteries were deployed in Beersheba and Ashkelon in 2011 during a rocket offensive, where their successful interceptions converted sceptics into supporters.[196]

Other demonstrator projects have similarly transitioned from testing to adoption, reinforcing the value of this model. The Trophy Active Defence System for the Merkava Mk 4 tank, initially tested during a 2010 IDF exercise, and a smart gunsight for infantry rifles evaluated during training – resulting in dramatically improved accuracy among recruits – underscore the impact of operational demonstrators.[197]

Finally, for the third part, the Israeli defence innovation ecosystem emphasises strong collaboration and development of information and relationship networks across various sectors, including between military R&D initiatives and the commercial industry. MaFat acts as a critical conduit linking the civilian governance of defence with military strategic operations. At more granular levels within MaFat, a symbiotic relationship exists with operational military units. This is in part because many of MaFat's staff are serving military personnel, including Talpiots. Discussions about R&D working plans are a routine part of interactions with the military at the mid-rung levels, ensuring a deep mutual understanding of operational requirements and R&D capabilities. The Israeli technology sector benefits from this collaborative defence innovation system, as many of its scientists, engineers and executives are IDF reservists who bring first-hand knowledge of military needs to their civilian roles. This dual experience facilitates the transition of military technologies to civilian applications, creating significant economic opportunities.

At the more operational level, junior and intermediate MaFat officers frequently engage with industry counterparts, conducting initial assessments of industry innovations. These officers are encouraged to visit technology firms, especially startups, regularly (at least once or twice a week – the limited length and breadth of the country helps in the frequency of these visits) to foster relationships and identify potential collaborations. These engagements often lead to prototype development and operational testing, supported by agile and adaptive contracting processes tailored to work effectively with commercial entities.

In terms of dealing with commercial entities and dual use technologies and encouraging startups to focus on defence related R&D, the MaFat created a program in 2019 called 'Innofense', which acted as an innovation centre for startups looking towards military R&D. Innofense liaises with VCs and helps in tracking commercial solutions to military problems.[198] Israel's civilian Innovation Authority and MaFat have emphasised the importance of bioconvergence as a field of critical importance for Israel.[199] Apart from this, areas such as lasers, AI, cyber and AD especially for C-UAS solutions are being looked at in the commercial sector.[200] The program connects startups with foreign and domestic VCs, and is known for cutting red tape.

Innofense is not particularly keen that all startups focus exclusively on military problems, acknowledging the fact that technology by its very nature is dual-use and innovations in the civil arena can be re-purposed for military uses later. In fact, only a small fraction of the companies being handheld by Innofense are defence oriented. Innofense is part of the wider and much grander Momentum strategy of IDF (2020–23), which considered asymmetric threats the main challenge for the force and focused on the destruction of adversary capabilities rather than holding ground. MaFat also collaborates with the US on a host of technology regimes – at least seven working groups at the level of the US undersecretary of R&D. The US DoD also formed a US Israel Operations Technology Working Group (OTWG) in November 2021 with its Israeli counterpart, the IMoD.[201] OTWG has established six sub-groups: artificial intelligence/autonomy, directed energy, counter-unmanned aerial systems, biotechnology, integrated network systems-of-systems and hypersonic capabilities.[202]

Not only the IMoD, even within the IDF, the J-8 or the Force Build Up

Directorate is responsible for furthering the avenues of innovation. J-8 comprises two divisions: Planning Division responsible for a broader outlook and multi-year approach towards force design and the Shiloah Division (Combat Methods and Innovation or CMI Division) for developing, promoting and adopting with a 'multi-agency vision'. Another Directorate, the J-5, is responsible for connection and integration across agencies. Both directorates have combined to formulate IDF's Innovation Strategy, according to which the first International Military Innovation Conference was organised by IDF in September 2022.[203] The five pillars of the innovation strategy are entrepreneurial culture; empowering partnerships; research and education; applied mechanisms and tools; and innovation management.[204]

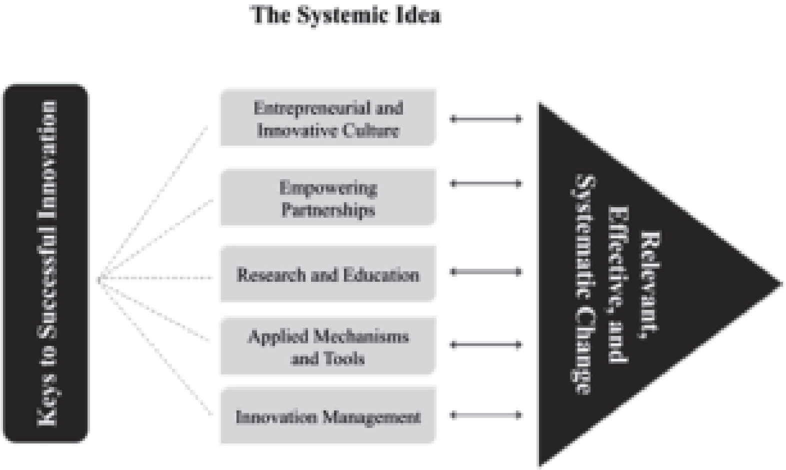

The Systemic Idea
Keys to Successful Innovation
Entrepreneurial and Innovative Culture
Empowering Partnerships
Research and Education
Applied Mechanisms and Tools
Innovation Management
Relevant, Effective, and Systematic Change

Figure 9: A flowchart of innovation as visualised by the IDF[205]

Innovation within the IDF is closely coordinated with MaFat, where the Shiloah Division acts as IDF's integrator component with DDR&D. Along with elements from the industry, academia and the International Cooperation Division for international partners, IDF's approach towards innovation is a holistic one and is based on breaking down barriers, creating blue oceans or common and interconnected areas across countries, agencies and organisations, shared infrastructure and finally, employment of classic management tools for a healthy innovation ecosystem that looks to devise tailor-made solutions for IDF's unique challenges. Briefly, the innovation initiative as an organisational imperative started in 2014 with the establishment of an innovation section within the Israeli Air Force. This was supplemented by the creation of Base 108 and Ofek 324 again in the air force, followed by a combat lab in the IDF Ground Forces Technology and Logistics Division, Technology and Maintenance Corps HQ, C4I and Cyber Defence Directorate and the Yahalom Unit, among others. These sections organised innovation events such as Machanet, Innovation Week, un-conferences and hackathons to connect civilian innovation setups with the IDF bodies.[206]

Due to IDF's unique culture of mandatory conscription and reservists, this huge network was leveraged for creating technology accelerators and incubators within the air force and other sections of the ground forces. Apart from this, veterans were contacted, and military veteran communities were sought out to further avenues for innovation, including raising reserve innovation reconnaissance units. These different islands of innovation proliferated across the force, at times working at cross purposes to each other. That is why there was a deliberate attempt to create an ocean of innovation connected by an archipelago – in other words, multi-domain threats required joint approaches towards innovation therefore a common network or archipelago will connect all the different innovation islands together. As a result, the CMI was raised and now controls and manages a host of innovation structures including a research institute, entrepreneurship centre, Defence College of Innovation, Intrapreneurship and Transformation, Reserve Centre of Excellence, experimentation centre and the innovation management department, among others.

The aim of CMI or Shiloah is again unique in that it acknowledges innovation to be a profession and a specialisation that requires specialised support in terms of funding, facilities and personnel. CMI therefore invites personnel from all units and formations within the IDF irrespective of arms, and in fact, supports decentralised innovation across the force.[207] For this CMI posts standardisation procedures, profiles, training programs and professional development in advance in order to intimate the schedules for prospective innovators.

The IDF released two documents during 2019–20 – 'The Momentum Multiyear Plan' and 'The Operational Concept for Victory'. While the former, also known as Tnufa in Hebrew, was to be operationalised from 2020 to 2024 as part of periodic four-year plans for the IDF,[208] the latter was meant to focus IDF capabilities towards asymmetric and non-state threats. The Tnufa plan entailed several changes, such as splitting of the IDF Planning Directorate or Agat into the Multi Armed Forces Planning Directorate and the Third Circle Directorate responsible for Iran and regional threats. The plan also emphasised the use of unmanned platforms, PGMs and incorporating AI for targeting and increasing coordination amongst units.[209] Another innovation attempted by IDF has been the creation of a Ghost Unit, which combines capabilities from multiple arms and Services for tailormade missions against adversaries. This team may include armour, infantry, UAVs, cyber, artillery etc to create a multi-arms team, which also requires technological exploitation for coordinating between the diverse elements of the team as well as enabling a flexible response against a rapidly changing scenario.[210]

The Momentum plan and the Operational Victory concept were based on the common threat of rocket-based terror armies initially considered to be diffuse, amorphous terrorists 'groups' but later acknowledged as trained, networked and disciplined forces with asymmetric capabilities. In addition to calling for the exploitation and leveraging of the Fourth Industrial Revolution, both plans rejected the notion of deterrence and limited war and instead focused on the notion of a decisive victory.[211] The IDF's Operational Concept of Victory was based on three principles, all of which required the rapid induction of commercial technology into the IDF. These were multi-domain operations, smart responses and negating enemy capabilities. Consequently, three capabilities were identified to be strengthened: ending of rocket fire; faster sensor to shooter cycles; and delivering the full range of IDF capabilities at the hands of the frontline IDF soldier.[212]

Momentum is in the process of being upgraded to the Ma'alot plan (Ascent in Hebrew), which identifies four action areas: strengthening people and military society relations to ensure that the best individuals continued serving the state through the IDF; boosting Israel's intelligence, defence and offence capabilities keeping in mind Iran's ascent in the region; improved training and readiness for manoeuvre warfare and multi-force coordination; and strengthening the young commanders on ground. In practical terms, the IDF has moved on to harnessing increasingly niche and mostly commercial technology for an individual-focused, network centric, capabilities-based approach towards modern warfighting, which also sustains the cutting edge of all these technologies, that is, the human element.[213]

As a practical example, the IDF's Namer and Eitan armoured personnel carriers (APCs) are heavily protected from small and medium calibre fire through the deployment of the Trophy active protection system as well as mounting sensors on the outside so that the soldier does not need to peer outside of his/her protective shell. As a result, the influx of data to the soldiers inside needs processing at machine speed and that is why a number of Israeli AI startups have devised solutions that process and integrate data from not only the organic sensors of the APC but also from UAVs flying overhead, and are working towards solutions that integrate all the different algorithms and aspects of the platforms into a single combat cloud. The IDF has also allied with Elbit Systems for a simulation and testing program called Edge of Tomorrow, which uses augmented reality (AR) goggles, computerised assault rifle system, digital helmet mounted display (HMD), hostile fire detection technology, location tracking systems for GPS-denied environments and tactile sleeves for navigation and communication.[214] The focus is on increasing the lethality and effectiveness of IDF troops against terrorists and extremists in an urban environment.

In conclusion, the Israeli state faces very unique challenges in terms of the number of adversaries whose numbers and nature have oscillated over the years – conventional state actors such as the neighbouring Arab nations till the late 1970s to non-state actors such as the erstwhile Palestinian Liberation Organisation (PLO) and now a combination of state (Iran) and non-state (Hamas and Hezbollah) actors. As a result, despite having a comparatively smaller frontage to defend, Israel has to constantly innovate by keeping the cost-benefit analysis of defence in its favour, since the shape of the country and nature of terrain has placed Israeli civilians next to the border, making them vulnerable to the thousands of rockets fired by groups in the Gaza strip.

In terms of defence, the state needs to look at the price per engagement, generally higher on the defence side due to the need for sophisticated detection, identification and engagement routines and technologies as compared to the non-state adversary or state proxy, which can use a combination of DIY technologies to create an economic disadvantage for the defence. Here, the defence also needs to look at offsetting capabilities in the domain of emerging technologies as well as capabilities available in the commercial sector. As a rough example, one Tamir interceptor missile of the Iron Dome system costs between $40,000 and $50,000.[215] On the other hand, crude rockets fired on Israeli territory are priced at just a fraction of this amount. An attendant danger is the proliferation of these missiles and rockets in the region and improvement in precision guidance of these missiles. As a result, MaFat is attempting to find cheaper solutions to the problem of counter-rocket, artillery and mortar (C-RAM). Some of the solutions include the laser-based Iron Beam system[216] and the Legion-X drone swarm.[217]

For Israel, the need for innovations and emerging technologies is more immediate and urgent. Some examples from the recent war against Hamas will serve to clarify this point. The IDF's campaign against the Hamas terror group has been mainly localised in the Gaza strip, with some operations also in South Lebanon against Hezbollah. There have been reported use of AI systems such as Jasmine, drone swarms and unmanned M113 armoured personnel carriers (APCs) in the ongoing conflict. However, some observations regarding the balance between technology and scale are relevant here. While the IDF is miles ahead in the creation and use of technological systems, Hamas has been using human shields, tunnels and urban warfare to frustrate the efforts of the Israeli forces. It is to the credit of the Israelis that they have been able to come up with technological solutions to most of these challenges, but they face issues of scale and depend on friendly countries for material such as ammunition. The pace of war is relentless and Israel is expending ammunition at a very high rate. Though there have been massive improvements in precision, ISR, AD and C2 technologies, the issue of scale still plagues the forces. This is the most important observation and lesson for the Indian military. Technology, as has been reiterated on multiple occasions, is not a panacea in itself. It has to be absorbed within the military through organisational, operational and doctrinal changes and at the time, the scale of manufacturing the platforms should be commensurate with the envisaged danger.

Ukrainian Armed Forces

The use of emerging technologies by the Ukrainian Armed Forces (UAF) has been extensively documented but most of this usage, from the start of the war till very recently has been ad-hoc and supported by individual soldiers, units, Western countries and Ukrainian businesses. Numerous non-governmental organisations (NGOs) and volunteer groups have been at the forefront of activities that are typically identified with the state. These include R&D, induction of technologies, interfacing with Western nations, speaking to Ukrainian soldiers regarding their requirements, creating data analysis centres, developing apps, imbibing joint forces operations principles and at times, operating certain platforms. This last function creates challenges of reciprocal actions by states against civilians as per international humanitarian law (IHL), keeping the tenets of the law of armed conflict (LOAC) in mind. It is only recently that the government has actively started to invest and link these private initiatives with mass manufacturing facilities to create low-cost systems at scale. Though the use of platforms such as Starlink, multiple drones and app-based targeting systems have revolutionised tactical warfare for the Ukrainians, they suffer from issues of scaling of systems, ammunition, fortification and trained manpower. Despite this, they have shown, more so in Russian emulation of their tactics, that the character of warfare has changed in favour of the defender, relevance and, in fact, criticality of open-sourced commercial systems and integration of niche technologies. This section will focus on open-source literature on the Ukrainian procurement process and may suffer from gaps due to the lack of adequate literature and/or news items on the same.

Public Private Innovation: Bypassing Government Bureaucracy

One needs to look back from the current situation of Ukraine's defence procurements in order to make sense of their induction and absorption process. Ukraine's defence establishment, when looking at inducting technologies or capabilities to field in the current conflict, has lagged behind its civilian counterparts. There are many reasons behind this lag primarily corruption, an ossified bureaucracy and Soviet style warfighting doctrines. Though changes have started occurring in some areas, most efforts have come from volunteers, civil society groups, students and individual soldiers and officers of the Ukrainian Air Force (UAF), who have directly connected with institutions and universities to get prototypes of drones, ISR apps and at times tinkered with existing civilian-facing apps to modify them for military use. As per some analysts, though this model may be aptly called public private innovation, the role of the Ukrainian society is paramount.

Aerorozvidka Group

Aerorozvidka, a volunteer group has been instrumental in creating the Delta app, along with support from North Atlantic Treaty Organization (NATO), the UK, Canada and Germany. Aerorozvidka was founded in 2014 by a group of PhDs and college students and its official mission is to 'assist Ukraine's security and defence forces in defeating Russian aggressors'.[218] A brief history of the group is essential to understand the criticality of civil society organisations and volunteer groups in Ukraine's military operations. The group was formed in 2014 during Russia's initial attack on Ukraine and coalesced into a military unit in 2015, called A2724.[219] Work on the Delta app started in the same year. It started cooperating with NATO from 2016 onwards through the latter's command, control, communications and computers (C4) Trust Fund.

The fund is led by Canada, the UK and Germany and operated by NATO's Communications and Information Agency (NCIA).[220] The aim of this fund is to assist Ukraine in improving its C4 capabilities and increase interoperability with NATO. The fund has three major thrust areas: the regional airspace security program, which aims to increase civil-military air traffic coordination and early warning of air space threats; Secure Communications Project, which provides secure satellite communications and blue force tracking (BFT) capabilities to the UAF; and Knowledge Sharing Project, which provides information to Ukraine on NATO C4 standards and processes.[221] The year of 2016 was also when A2724 launched the first working prototype of the Delta app. Between 2017 and 2019, the app was showcased multiple times at NATO's Think Tank for Information Decision and Execution (TIDE) Hackathon and Sprint events where the group won back-to-back the first place in the modelling and coding challenges.[222] The TIDE Hackathon and Sprint events are organised by NATO's Allied Command Transformation's Strategic Warfare Development Command.

The aim of these competitions is to look at future challenges by engaging a diverse group of participants in a time limited format.[223] As part of NATO's 'interoperability continuum', the third event, which is the Coalition Warrior Interoperability Exercise (CWIX), enables NATO members and partner entities to test for C2 in terms of 'de-risking' interoperability. A2724 also participated in CWIX through showcasing Delta from 2018 onwards,[224] which also included interoperability testing based on the Multilateral Interoperability Program Baseline 4 – Information Exchange Specifications (MIP4-IES), with multiple demonstrations culminating in Delta's approval as an authorised C2 platform for both the UAF and the Ukrainian government in 2023.[225] The app adheres to NATO communications and interoperability standards as per their Federated Mission Networking (FMN)[226] program. A2724 itself was terminated in 2020, to be replaced by the Aerorozvidka NGO in late 2020 and its creation of the Centre for Innovations and Development of Defence Technologies in mid 2021. The group was also instrumental in the creation of the first ISTAR unit in late 2022, most likely September 2022.[227]

The group, currently headed by Yaroslav Honchar,[228] is divided into four project areas: command and control information systems (C2IS), ISTAR, robotic systems and knowledge management.[229] The group is unique in the sense that it directly interacts with military advisers from Western countries in the fields of joint forces operations, implementing network centric capabilities and claims to have deployed robotic units on the battlefield. This has generally been seen as the task of the military authorities or the wider defence departments. The scale of this network centricity, however, is low both due to the size of the UAF as well as its scope of operations. Another aspect that separates this group is that its members fly missions themselves. As per one estimate, volunteers from the group clock 20 hours per day on ISR missions for UAF.[230] It has created nine situational awareness centres at Kyiv, Mykolaiv, Kherson, Zaporizhzhia, Kryvyi Rig, Kharkiv, Sumy, Chernihiv and Donbas, where all means of information from cameras, sensors, drone data and human intelligence (HUMINT) as well as informational support from Ukraine's allies is merged, processed and analysed and then passed on to the relevant units as well as the UAF HQ.[231] More than 450 UAF personnel have undergone training and internship with the group's ISTAR team with the use of tools such as Mission Control and Vezha apart from Delta, to become ISTAR officers at the brigade and battalion level.[232] The figure below provides a graphical representation of the same.

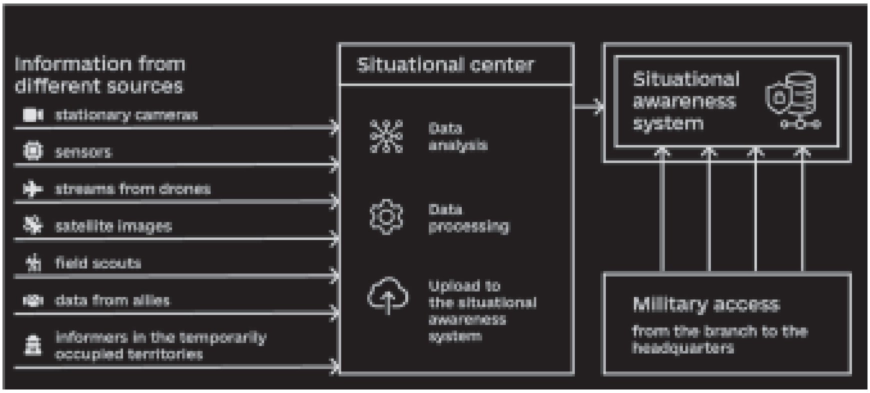

Information from different sources
stationary cameras
sensors
streams from drones
satellite images
field scouts
data from allies
informers in the temporarily occupied territories
Situational center
Data analysis
Data processing
Upload to the situational awareness system
Situational awareness system
Military access
from the branch to the headquarters

Figure 10: Aerorozvidka's C2 system connecting innovators and warfighters on the Ukrainian battlefield[233]

Technology is leveraged by the group extensively. This includes the creation of chatbots that connect the UAF troops to informers in territories occupied by Russian forces.[234] eVorog, the Ukrainian defence ministry's chatbot is integrated with the Diia application[235] and provides a comparative analysis of the information received from HUMINT and technical intelligence (TECHINT) to provide fast, rapid and accurate data to the military commanders on ground.[236] In addition to data fusion, the group uses COTS drones such as Autel and DJI for ISR and has created an indigenous octocopter called R18, which is equipped with 11 lb bombs with a 40 minute flight time and a range of 2.5 miles.[237] Delta integrates ISTAR streams to provide situational awareness to troops on ground and enables tactical commanders to make rapid decisions using a host of sensors and data streams fused on to a single user interface.

This app has also received extensive support from Aerorozvidka, both in the design as well as improving its cyber-resilience. For the latter, the group provides a Fast Identity Online (FIDO) key, developed by the FIDO Alliance, which is an association of more than 250 members including companies such as Google, Apple, Meta and Visa, among others. Broadly, the key is a two-factor authentication for providing secure access to systems and applications.[238] The group also conducts UAV pilot training capsules, which are run for five days on the frontline and include both theory and practical examinations. The curriculum of the course is based on the various functions of UAVs in battle such as ISTAR, artillery spotting and kinetic attacks, the types of UAVs and their parameters and important aspects such as how to plan attacks using UAVs, how to ensure their survivability and loss. The pilots are also given detailed instructions on the use of the Delta app. Aerorozvidka has also established a hub for further interaction with experienced pilots and certifies pilots in a 'train the trainer' fashion to proliferate drone pilot training across the UAF.[239]

The Knowledge Management area has created two knowledge management groups and has conducted a number of studies for introducing a systematised training in higher military educational institutions, creation of a knowledge management portal and a space for the exchange of knowledge within the Delta ecosystem. The robotics area focuses on cross-platform planning and execution of tasks using unmanned robotic systems and development of precision weapons to be mounted on robotic systems. It currently focuses on the development of a guided free fall munition, ammunition logistics systems for UAVs, studying pros and cons of using aerostats in modern war, purchase of the R18 octocopters and their delivery to UAF personnel and construction of secure communication protocols for unmanned systems. The group is also very active in guiding policy making in the Ukrainian parliament. For example, it was involved in passing resolutions 10062 for legalisation of the use of cloud services of allies for Ukrainian governmental use and 4210 for aligning the methods of managing UAF personnel with NATO standards.[240] The group also supports the BRAVE1 defence-tech cluster.[241]

Most volunteer groups in Ukraine have interfaced directly with units on the ground and with their inputs created solutions such as the Kropyva (Nettle) targeting software. Kropyva, which was developed in 2015 by Army SOS, a Ukrainian volunteer group, amalgamates sensor data from a number of UAV operators and passes it on to Ukrainian armoured units, which then use the targeting data to fire on Russian tanks. Kropyva is a C2 system that can be used for an individual vehicle, platoon, company and a battalion.[242] Volunteer groups have also assisted in developing home-made Valkyria reconnaissance drones, Punisher strike drones, Beaver fixed wing precision strike drones and the Sea Baby USVs.[243] The last has gained notoriety for being responsible for the bombing of the Kerch bridge. Even Ukrainian individuals have started designing apps for integrating C2 systems with fire units across military zones.

For example, GISArta, known as the 'Uber for Artillery' was designed by Yaroslav Sherstyuk in 2013. Initially named ArtOS and meant to be a calculating app for ballistic trajectories for artillery commanders, this app evolved into GISArta, which optimises across variables such as target type, position and range to match targets with artillery batteries in range. The app also allows multiple batteries to fire on a single target or conversely for a battery to take on multiple targets.[244] Like other apps, this is also one more example of using technology for rapid decision making on the battlefield that can be termed as 'JADC2 Lite'.

Before looking at the reforms initiated by the Ukrainian government and analysing their level of success, it is important to look briefly at some other volunteer initiatives such as Army SOS and the Serhiy Prytula Foundation. These will provide a wider snapshot of the nature of defence innovation within Ukraine. This becomes important since Ukraine is the only country right now that is constantly and continuously innovating while engaged in conflict. Army SOS is a volunteer foundation that focuses on providing UAVs to UAF personnel. The organisation has also been instrumental in designing and deploying the Kropyva defence mapping software amongst UAF frontline units. The software is used for a number of purposes including planning, calculations and orientation.[245] The Military Division of the Serhiy Prytula Foundation helps connect a particular unit's demands with the wider world and acts as a bridge to deliver funds and supplies in the domains of transportation, optics, communication, drones, UAVs and tactical medical supplies. Its Help Army initiative has led to the purchase of strike UAVs, first person view (FPV) drones, upgradation of AD capabilities and repair of armoured vehicles. The foundation has also contributed significantly to the cost of running and equipping the Boryviter Centre of Excellence, which trains Ukrainian soldiers in piloting UAVs, battle C2 systems and topography and land navigation.[246]

The Government Steps In

The Ukrainian government took initial steps to scale up volunteer effort in soliciting immediate effort to stop the Russian attack. For example, initiatives such as 'dronations' and Army of Drones project through the United24 initiative,[247] are being used to collect money through international donation efforts that can be used for procuring drones of different varieties as well as provide certain discretionary powers to the UAF for purchasing mostly non-lethal military assistance. The United24 fundraising initiative was operationalised within months of the Russian special military operation. It is meant to act as a consolidated platform for receiving grants from across the world and ensure transparency in their distribution and use. United24 has six areas or projects, namely, Urgent, Defence, Medical Aid, Rebuild Ukraine, Humanitarian Demining and Education and Science.[248]

Within the Defence project, United24 prioritises induction of drones. The initiative is called 'dronation' and has been used multiple times since the beginning of the hostilities to get specific drones into the hands of the UAF personnel. The Army of Drones project, the flagship program of United24 and jointly owned and executed by the General Staff of the Armed Forces, State Special Communications Service and the Ministry of Digital Transformation includes both procurement as well as pilot training courses.[249] As of date, the program has managed to induct drones such as the American ISR Puma-long endurance (LE) drone, the Polish Warmate 3.0 loitering munition (LM), the Ukrainian Skyeton tactical UAVs as well as Chinese DJI and Autel drones.[250] As of the date of writing, the Army of Drones has just finished raising funds for 10 Danish RQ-35 recce drones.[251] Apart from dronations, United24 has collected funds for the world's first fleet of naval drones, Shahed hunter anti-drone system, 5000 FPV drones as part of Operation Unity Part II and Sea Baby naval drones under Operation Sea Baby.[252] As of now, they are looking at raising money for a situational alert system for Ukraine's AD Forces.[253]

These efforts have filled in some of the operational voids for UAF at the tactical level but the Ukrainian government has realised that these are fillers at best and there is a need to link low cost innovation with high scale state manufacturing capacity. As a result, efforts are being made at the government level to cut down red tape, synchronise functions and actions of various departments and ministries dealing with procurement and prototyping and finally cutting down the time window between receiving a proposal for a military problem and vetting it to 45 days. The previous regulation was two years.[254] Ukraine has also been nicknamed the AI lab, battle lab and technology lab for commercial companies that want to test their products and technologies in battlefield companies and check if their offerings are robust enough to be used in other battlefields.[255] In fact, the Ukrainian battleground can be compared to that of pre-World War 2 era Spanish civil war where countries from the then emerging Allied and Axis camps tested their latest weapon systems and technologies against each other.

Apart from operationalising BRAVE1 defence-tech cluster, the Ukrainian government has created the Innovation Development Accelerator (IDA) under the Ministry of Defence, headed by the deputy minister of defence who is in charge of weapon issuance, defence industry and military technology. The accelerator, which was created in June 2023, has six goals, chief being the reduction of bureaucratic red-tapism within the ministry, reduction of time taken from issuance of orders to delivery to frontline units and the introduction of the concept of project management in the domains of weapons, defence and military technology.[256] Some of the ways through which the accelerator achieves these goals are a single window clearance system for official communication with defence startups and reduction in paperwork from 100 documents to five.[257]

Process simplification through the accelerator was achieved in stages and one can see the fruits of these aims in the recent months. For example, the decision-making time for evaluating a particular proposal has been reduced from two years to 45 days. In terms of capabilities, the program looks at six major ones: Weapons 1.0+ (modernisation and improvement of existing weapon platforms and ammunition); robotisation and AI (unmanned systems spanning all domains with use of AI); communications, EW/SIGINT (for protected communications and portable EW/SIGINT); Weapons 2.0 (weapons based on new technologies); intelligence, cyber defence, psyops; and IT solutions (automation of processes and data analysis within the Ukrainian defence ministry).[258] Moreover, in order to ensure compatibility, once a project is approved, the sample weapon system is codified either in Ukraine and/or in NATO's registry.[259] The NATO Codification System (NCS) is a program that uses a NATO Stock Number (NSN) to standardise the name, description and classification of a particular weapon system.[260]

In September 2022, seven months after the start of the conflict in Ukraine, Resolution Number 345 was passed in the Ukrainian parliament, which led to the fast-tracking of new weapon systems and technologies, with an aim to extend state support for mass production. A national defence hackathon was held in November 2022, which included not only the Ukrainian state and private actors but also representatives from NATO and international experts. The event focused on three areas: technical, counter-disinformation and legal, and involved close to 3,000 participants. In April 2023, a Committee on Arms Management was established to synchronise the functioning of the different branches of the defence ministry to assist the defence minister in making decisions related to strategy, policy and weapons technology. An action plan was created in May 2023 for the implementation of Ukraine's weapon systems portfolio to minimise the issues of lack of effective communication and cooperation between the different branches of the defence ministry, as well as to update obsolete methods of military management. Finally, in June 2023, an accelerator was created that looks at inducting technologies at TRL 7 and above. The accelerator has instituted dedicated units for interacting with counterparts from other countries, such as DIU, Defence Information Systems Agency (DASA) and NSIN from the US, Defence and Security Accelerator from the UK, Defence Innovation Hub from Australia and Defence Innovation Accelerator from the North Atlantic (DIANA) and Innovation Unit from NATO, for technological advancements.[261]

Now let us take a look at the BRAVE1 defence-tech cluster in detail since it is one of the most high-profile initiatives undertaken by the Ukrainian government to connect startups with the UAF HQ and commercial backers. Other initiatives, whose functions will be mentioned in brief, that focus on dual-use capabilities are also underway.

BRAVE1 was launched in April 2023 with an aim to connect private initiatives with a demonstrated level of technological maturity with the defence ministry for scaling up production.[262] This cluster connected a number of state entities, such as the Ministry of Defence, General Headquarters of the Armed Forces of Ukraine, the National Security and Defence Council, the Ministry of Strategic Industries and the Ministry of Economy, with the initiative being headed by the Ministry of Digital Transformation. The goal of BRAVE1 is to enhance the speed, innovativeness and capability of technological solutions provided to Ukrainian soldiers on the frontline. For this, the Ukrainian government offers foreign partners access to Ukrainian defence innovations with a 'soft landing procedure', enables their participation in hackathons and networking events and finally, provides investment opportunities in the most modern and cutting-edge defence tech developments in the country.[263]

The cluster has 10 priority areas, namely, weapon system, protection and security, UAVs, robots, supply and logistics, demining, cyber security, intelligence, navigation and medical support.[264] The organisation also features a defence advisory council that includes military personnel, investors, businessmen and diplomats from Europe and the US. Experts estimate the number of projects undertaken under the BRAVE1 umbrella to be between 820[265] and 1,010[266] as of date. Any project that passes the military expertise level of the UAF General Staff is certified BRV-1.[267] Technologies and platforms even at relatively lower technology readiness levels (TRLs) are being fielded and are deliberately being made modular and simple to use to enable soldiers on the battlefield to tinker with them in a DIY manner. Since its inception, BRAVE1 has, as per the Minister of Digital Transformation Mykhailo Fedorov, distributed a total of 173 grants exceeding three million dollars and the likely amount to be distributed in 2024 totalling $39 million.[268] A news source puts the number of projects to have been granted BRV-1 status till date to be 473.[269] A majority of the grants have gone to individuals and businesses dealing with ground robotic complexes, UAVs and military defence and security systems.[270] These grants are given out in packets of $10,000, $25,000, $50,000, $100,000 and $200,000.

Ukrainian startups are also being supported by the European Innovation Council (EIC), which has pledged nearly 20 million euros for supporting close to 200 Ukrainian tech startups with up to 60,000 euros provided per project.[271] This initiative is also being supported by 20 other organisations such as FundingBox, an accelerator based in Warsaw under the Seeds of Bravery project.[272] Some of the successes of BRAVE1 are now visible – Ukraine now produces more than 90 per cent of the drones used by its military and aims to be the world capital in unmanned systems.[273] As per one estimate more than 200 companies produce drones in the country, up from seven in 2022.[274] President Zelenskyy has already announced the creation of an Unmanned Systems Forces whose units and personnel will be embedded in all the three Services of the army, navy and air force. The plan envisages the production of close to a million light drones in 2024 as well as more than 11,000 of the medium to heavy variety. These heavier drones are reported to have ranges of more than 1,000 km, able to target multiple regions and cities inside Russia.[275]

This model of public–private grassroots innovation also creates a number of challenges. As one Ukrainian analyst has noted, there is a gap in the 'identification of urgent operational requirements' and in 'making the connection between available technologies and mission needs'.[276] The ideal way of ensuring the placement of latest technologies at the hands of the warfighter on a scale that impacts a combat situation significantly depends on a smooth process of identifying technological solutions for operational challenges, and ensuring that standardised models of these systems are inducted into a manufacturing establishment with adequate commercial backing that ensures mass availability. This requires policy modification at the government level.

A solution advanced for Ukraine by the Hudson Institute calls for a 'mission integration process' with six functions: 'problem definition; solution development and experimentation; material procurement; digital integration; resourcing and requirements; and operational refinement'.[277] This is being implemented in Ukraine by volunteers and NGOs who work in an ad-hoc manner, linking frontline officers and soldiers with startups since the emphasis is time-crucial, and at times, even products in the prototype stage are being inducted, tested and then sent back with observations for further amendments – the most rigorous example of a spiral development model. Another solution advanced is the establishment of a capability accelerator, which integrates acquisition with concept development and experimentation. Here the focus is on stakeholder engagement from the very start and where startups and military officials can chalk out issues such as performance, security, maintainability and interoperability from the genesis to the conclusion of the project.

Indian Innovation Ecosystem

One may wonder why there is a large focus on India's civilian S&T ecosystem when in the previous chapter only defence innovation ecosystems were considered. There are two major factors involved here. In the case of the US and Israel, the S&T innovation ecosystem is well entrenched and long established. In fact, most of the technologies around the world today have been the product of Silicon Valley. So, the criticism around their defence innovation does not go to the root but focuses mainly on the gap between their military's requirements as per their conception of MDO operations and the ability of civilian startups to cater to them. Of course, the case is not that simple and though the US military desires acquisition and absorption of emerging and disruptive technologies, there are significant procedural issues. In Israel's case, again, the S&T ecosystem evolved in parallel with the state and has been the harbinger of technological innovations both in the military and civilian sphere. Ukraine is a unique case for four reasons: it is a testing ground for a rapid shift of military organisational structure from a Soviet model to a Western one; Ukrainian forces have been recipients of major military aid both of conventional and disruptive nature; it is a testing ground for a number of technology companies to ruggedise their products; and finally, the war effort in general has been led by civilian entrepreneurs due to Ukraine's pre-war status as a digitally literate and innovation nation.

India's case is different. Similar to the West, a lot of innovation is happening in startups and micro, small & medium enterprises (MSMEs), but in the fields of fintech, edtech and consumer-facing applications. One of the major points of departure for the Indian technology scene is the major role played by the government. Examples such as the Digital Public Infrastructure (DPI) have placed the state firmly in the driver's seat of innovation. So, the vast S&T infrastructure in India needs to be described initially. Also, the relevance of emerging and disruptive technologies within the Indian Armed Forces has been realised a little late. Though the uptake has been fast, a time lag remains, which needs to be filled by having multiple associations across the civilian S&T spectrum in the country.

Innovation in general is majorly a product of two factors: funding or investment in R&D and the S&T ecosystem in a country. The Indian S&T ecosystem, befitting the size of the country, is large and comprehensive. At the apex consultative level is the office of the Principal Scientific Advisor (PSA) to the Government of India, whose role has been to evolve policies related to S&T innovation, provide catalytic support to R&D projects that straddle ministries and domains, enable cross-sectoral and cross-domain R&D and coordinate between the relevant ministries, departments and agencies of the state and the central government.[278] The PSA is the chairman of the

Scientific Advisory Committee to the Cabinet, as well as the Chair of the Prime Minister's Science, Technology and Innovation Advisory Council (STIAC).[279] There are 15 government bodies including Defence Research and Development Organisation (DRDO), Department of Science and Technology (DST), Department of Biotechnology (DBT), Department of Space (DoS), Department of Atomic Energy (DAE), Ministry of Earth Sciences (MoES), Council for Scientific and Industrial Research (CSIR) and the Ministry of Electronics and IT (MeitY), among others, that are involved in cutting-edge R&D in the multiple areas of S&T.

There are 20 Centres of Excellence (CoEs) such as the Centre for Nanotechnology (CNT) at Roorkee, Centre for Advanced Functional Materials at Kolkata, Centre for Excellence in Robotics (CER) at Kharagpur etc. Two categories of thematic centres cater to important functional areas of geospatial analysis and environmental research. In the former category, institutions such as Survey of India at Dehradun, Remote Sensing and Application Centre in Uttar Pradesh and Science and Technology Park at Pune are doing important work, while the latter is being looked at by the National Biodiversity Authority and Directorate of Forest Education and 21 other such bodies. Multiple centres of higher learning such as the Indian Institutes of Technology (IITs), National Institutes of Technology (NITs) etc are important centres that not only are fully functioning universities and colleges but are also incubators for multiple startups in the domains of disruptive technologies. Multiple organisations in the civil society, industry-related organisations and labs run by organisations form a part of a vast, interconnected and complex network of S&T organisations.

The real impetus to innovation and subsequently defence innovation came with the Indian Prime Minister Narendra Modi's speech during the 2014 Independence Day celebrations where he stressed on self-reliance and the importance of technical education and e-governance to create a dream of Digital India. The push for both Made in India and Make in India were made during this speech.[280] Post this speech, a meeting of chief secretaries of all ministries was called and told to submit the major challenges facing the country in terms of increasing the gross domestic product (GDP) of the country. Four main challenges emerged: lack of a robust manufacturing ecosystem; low S&T and R&D base in the country; lack of easy access to capital and excessive regulations; and major impediments to ease of doing business in the country.[281]

To address each of these challenges, the Indian government created structures and issued policy directives. For improving the quality of the manufacturing ecosystem and the attendant issue of low technical skills, the Skill India program was created under the National Skill Development Corporation (NSDC),[282] a Section 8 company under the Companies Act 2013, which essentially meant that it was a non-profit organisation and structured on a public–private partnership (PPP) model. The Indian government, through the Ministry of Skill Development & Entrepreneurship (MSDE), accounts for 49 per cent of the share capital of the organisation with the private sector accounting for the balance 51 per cent. NSDC promotes skilling in more than 37 areas and offers close to 580 different skilling courses.[283] The issue of a low S&T and R&D base in India was addressed through the creation of the Startup India initiative. This was launched in January 2016 and all programs are managed by a dedicated Startup India team reporting to the Department of Industry and Internal Trade (DPIIT).

Startup India has a number of features that enable Indian startups to access funding and organisational support from both the government as well as angel investors and VC funds. The Startup India Seed Fund Scheme (SISFS) was created with an outlay of Rs 945 crores to provide financial assistance to startups for 'Proof of Concept, prototype development, product trials, market entry, and commercialization'.[284] The program acknowledged that the Indian startup ecosystem suffered from lack of capital funding in the seed and proof of concept development stage, or the early-stage funding. An Expert Advisory Committee (EAC), comprising experts in the government, private and VC sector has been constituted to assess the ideas of the startups.[285] Certain technology incubators have also been identified in the government and private space to assist the startups in managing and assisting with the expenditure of the seed fund. A large number of incubators have been established and recognised by the Startup India scheme in multiple sectors and across the country, almost all of them are physically based inside the premises of recognised public and private colleges and universities.

For example, in the defence sector, the Startup India website lists eight incubators, which are the Coimbatore Innovation and Business Incubator

(FORGE) in Coimbatore, Entrepreneurship Development Centre in Pune, Pilani Innovation and Entrepreneurship Development Society in Jhunjhunu, Nashik Engineering Cluster at Nashik, KLE Centre for Technology Innovation and Entrepreneurship (CTIE) in Hubli-Dharwad, Association for Bio-Inspired Leaders and Entrepreneurs (ABLEST) in Chennai, Atal Incubation Centre (AIC) Social Alpha in Delhi and Sharda Launchpad Federation in Gautam Buddh Nagar.[286] The impetus to the growth of startups has been the belief across the Indian government and private sector that the startups are at the cutting edge of technological innovation and it is only by supporting these setups that India can actually pole vault itself into the hi-tech club of nations and attain technological sovereignty.

The third challenge of remedying lack of easy access to capital in India is in progress and includes measures such as raising foreign direct investment (FDI) limits. The fourth challenge is improving India's environment of ease of doing business, for which Invest India was created. Invest India is a national investment promotion and facilitation agency, which was established in 2009 but revitalised post September 2014 with a special focus on startups ('empower Startups to grow through innovation and design through [...] initiative')[287] and on promoting innovation through Project AGNII, which is short for Accelerating Growth of New India's Innovations ('support the ongoing efforts to boost the innovation ecosystem in the country by connecting innovators across industry, individuals and the grassroots to the market and helping commercialise their innovative solutions').[288] Alongside, in order to encourage the spirit of innovation in children, the Atal Innovation Mission (AIM) has been launched and Atal Tinkering Labs (ATLs) created in a number of schools. The ATL initiative, a pioneering venture aimed at embedding state-of-the-art laboratories within schools to catalyse the curiosity and inventive spirit of students ranging from the 6th to the 12th grade nationwide.[289]

These ATL labs are equipped with advanced 21st century tools and technologies, including Internet of Things (IoT), 3D printing, rapid prototyping tools, robotics and miniaturised electronics, along with a suite of DIY kits. The primary objective of this initiative is to cultivate a problem-solving and an innovative mindset among the students and the surrounding community. Till now, AIM has successfully rolled out 10,000 ATLs across schools in the country, marking a significant milestone in fostering a culture of innovation and critical thinking among the younger generation. Atal Incubation Centres (AICs) have been strategically positioned within universities, institutions and corporate entities across the nation.[290] These incubators function similar to command centres for nurturing the innovative prowess and entrepreneurial spirit of the country's youth. With a current operational strength of 72 AICs,[291] these centres are designed to equip emerging innovators and dynamic entrepreneurs with the arsenal needed to develop scalable and sustainable ventures. The strategic objective of the AIC initiative is to engender a robust ecosystem conducive to world-class innovation. The deployment of these centres has catalysed the incubation of over 3,500 startups, effectively creating more than 32,000 jobs within the innovation ecosystem. The AICs straddle multiple domains, supporting ventures across a wide spectrum of sectors including healthtech, fintech, edtech, space and drone technology, AR/VR, food processing and tourism,[292] among others.

Before moving on to describe the Indian defence innovation ecosystem, it is important to mention that apart from specifically focused initiatives such as Startup India, certain other government departments and ministries have also developed their own innovation acceleration and startup promotion programs. This section will focus on one: Project AGNII since this is likely to have a major impact on India's defence innovation ecosystem in the future. AGNII deals with Indian 'Deep Tech Startups', which are defined in the 2023 draft of the National Deep Tech Startup Policy (NDTSP) with two major parameters: involving 'early-stage technologies based on scientific or engineering advancements, which are yet to be developed for any commercial applications' and producing a solution 'along an unexplored pathway based on new knowledge within a scientific or engineering discipline or by combining knowledge from multiple disciplines'.[293]

Deep-tech startups are distinguished from their non-deep tech counterparts by two factors: creation of intellectual property (IP) in S&T disciplines and greater technical or scientific uncertainty due to the nature of the technology or innovation.[294] The draft policy, recognising the limited support available within the country to deep-tech startups, calls for the establishment of a deep-tech centred single window platform for creating a unified IP framework customised for deep-tech startups, promulgating guidelines for the creation of design IPs, implementing strong cybersecurity protocols, monitoring mechanisms, streamlining of the patent application process and creating a consolidated database of all higher education institutes (HEIs) along with their patents and publications with a special focus on easing accessibility and searchability.[295] For deep-tech startups working either in the national security sector or in domains with specific national security implications, the policy recommends certain measures.

The concept of Government Purpose Rights (GPR)[296] has been introduced, which is a non-exclusive and non-transferable irrevocable license that the government can use for internal manufacturing or consumption, either directly or through a sub-contractor. This clause envisions suitably compensating the innovator, though this may discourage deep-tech startups from entering the defence or national security space with the apprehension of a cap on profits as well as no rights to export. The second clause is that of the government being endowed with 'March-In' rights[297] over all items governed by GPRs, primarily for national security and strategic considerations. These rights entail the ability to utilise the patent, either directly or through a designated entity, if (i) the patent holder fails to enact it within a reasonable timeframe or (ii) if control of the patent holder is assumed by a foreign entity without government approval. However, the exercise of these rights necessitates compensation to the patent holder or the relevant production agency.

In terms of funding and facilitating deep-tech startups' access to the same, the Deep Tech Startup policy suggests the creation of a Fund of Funds (FoF), called the Deep Tech Capital Guidance Fund.[298] In this structure, the government, private investors and foreign investors would commit money to the fund. The main fund, called the Mother Fund, would oversee investments in smaller funds, called Daughter Funds, which focus on investing in high-risk deep-tech startups. The FoF would have a longer duration than typical funds to match the extended time needed for deep-tech startups to develop their products. Deep-tech startups typically require more money for research, testing and manufacturing compared to software or service startups. The FoF's aim is to coordinate with existing grant programs and involve startups in procurement programs to help them scale up. They may also seek additional funding from corporations, government institutions, venture capitalists and private equity firms. The policy suggests that early-stage funding should be larger and last longer, possibly over 10 years, and should be benchmarked against successful deep-tech ecosystems in other countries. Initially, funding for inventors would be in the form of grants rather than equity or debt-based investments to encourage participation. These grants could come with conditions, such as giving investors the first right to invest further if the startup succeeds.

The draft policy mentions the Innovation for Defence Excellence (iDEX) as a successful program that involves the entire government in an innovation validation ecosystem and calls for the government's sustained financial support to deep-tech startups that are involved in addressing national priorities.[299] This support can be in two stages: proof of concept and tested prototype. There is also the concept of a pilot testing fund that will allow startups to access testing facilities, tailor their products and demonstrate experimental prototypes on ground before entering the market for commercialisation. The policy calls for constituting a debt fund to service the working capital requirements of startups and calls for banks to design 'specialised financial products' for ensuring that the unique needs of these startups are catered for in a unique manner rather than clubbing them with regular commercial loan requirements. The 'Frontier Scientific Infrastructure (FSI)'[300] model is suggested to enable deep-tech startups to access shared S&T infrastructure and finances from HEIs, incubators and R&D establishments. This infrastructure may be located to industry clusters and be domain specific. Finally, the policy report lays down certain recommendations such as adapting a 'failing by design' strategy, including options of writing off expenditure and the inclusion of a sunset clause; funding sensitisation programs for startup founders; creating a deep-tech investor meet platform; and establishing a centralised core mission office for the Indian deep-tech startups to succeed.[301]

Indian Defence Innovation Ecosystem

Since independence the main institution vested with the responsibility for innovation and R&D within the Indian defence ecosystem has been the DRDO. It was formed in 1958[302] and has been instrumental in developing multiple state-of-the-art weapons platforms such as nuclear missiles, submarines, tanks, anti-satellite weapons, radars and a host of other technologies. Here one has to be careful to highlight that development does not equate to deployment and in many cases platforms have struggled to make the leap from either technology demonstration or development of prototypes to mass production.[303] It is headed by a chairman who is also designated as the secretary department of Defence R&D (DD R&D), which is one of the five departments under the Indian Ministry of Defence (MoD).[304]

DRDO comprises eight clusters, namely, naval systems and materials; aeronautical systems; armament and combat engineering systems; missiles and strategic systems; electronics and communication systems; microelectronic devices; computational systems and cyber systems; and life sciences.[305] These clusters encompass 41 laboratories and five DRDO Young Scientist Labs (YSLs).[306] Apart from this, at the HQ level, DRDO consists of five main verticals of Resources and Management (R&M); Production Coordination and Services Interface (PC & SI); Technological Management (TM); Systems Analysis and Modelling (SAM) and Human Resource (HR).[307] Three independent verticals of Advanced Technology Vessels Program (ATVP),[308] Aeronautical Development Agency (ADA)[309] and Brahmos[310] are also a part of DRDO. In addition to the DRDO, there are the nine Defence Public Sector Undertakings (DPSUs), close to 40 Ordnance Factory Boards (OFBs) and certain major private players, such as Ashok Leyland Defence Systems, Bharat Forge Limited, Larsen & Toubro (L&T), Tata Group, Reliance Defence Limited, Adani Defence and Mahindra Defence Systems, which have been given the status of original equipment manufacturers (OEMs).[311]

In order to boost the innovation base and ecosystem in India, certain policy directives were announced and organisations setup. The philosophy behind these new establishments and policy directives was the recognition that in the long term, control over the design and ideation of emerging technologies should be in India's hands. It was further decided that in the short term, technology should be used as a part of innovation to create viable products. In fact, this is one of the reasons behind the push for supporting deep-tech startups and creating patents and IPs.

The importance of technology within the national security ecosystem can be gleamed from the fact that several Group of Ministers (GoM) and expert committee reports mention the importance of technology and innovation, either in detail or in passing. For example, in the 2001 K Subrahmanyam Report, there is a passing mention of technology but not much thought is given to the subject within the report itself. The GoM Report on National Security of 2001 has a comprehensive perspective on the importance of technology for national security, which is given in the next paragraph.

The report acknowledges that the IT revolution has deepened the process of globalisation, and that IW and revolution in military affairs (RMA) will have a dramatic impact in the coming decades. In parts, the report states that the forthcoming strategic landscape will undergo profound shifts driven by unprecedented technological advancements. Furthermore, advancements in communication and space technologies are fundamentally reshaping daily life and the economy, often beyond conventional recognition.[312] The report warns that China's wide-ranging defence modernisation will have to be taken special note of, especially with their focus on force-multipliers and high technology weapon systems.[313] A prescient paragraph from the report needs to be quoted in full:

> The concept of border security has undergone a sea change with the growing vulnerability of the coastline and also of the airspace. In response to the gradual expansion and strengthening of security, so far, mainly along what has long been perceived as a sensitive land border, the transgressor is already on the look out for soft gaps, either on the land or along the coast and if need be, from the air. The Purulia incident of 1995 has already demonstrated our vulnerability from the air. The transgressors, with unprecedented money power, access to latest technology, organisational strength, manoeuvrability and scope for strategic alliances with other like-minded groups, can select their theatre of action for surprise strikes.[314]

When one compares the total and complete strategic surprise achieved by Hamas in its attack on Israel on October 07, 2023, this report seems almost messianic in its foresight and tone. Further the 2001 Report argues for the establishment of an inter-ministerial task force to carry out a 'Strategic and Technological Environment Assessment (STEA)', whose assessment will be used to strengthen the capabilities of the armed forces.[315] The immense support and push given to startups is foreshadowed in the report when it calls for a continuing support to the private sector, given the fact that India has emerged as a 'leading player in several technology areas, particularly IT'.[316]

One has to remember the context here. The world had just been saved from the Millennium or Y2K bug, largely due to the expertise and hard work of Indian software developers.[317] Further, efforts to leverage the benefits of IT call for the timely implementation of office automation across the MoD, Service Headquarters and all associated establishments.[318]

The authors of the report recognise the technological potential of the country and argue for a greater role of technology in the field of defence and national security. Certain challenges are highlighted, which, as per the report, will hamper the development and absorption of technologies within the armed forces. There is a noticeable gap between planning and development in equipment development, especially in the connections between R&D, production agencies (PAs) and the end users, that is, the military. This includes crucial links between the Services' long-term plans and the budget for defence R&D. There is also a lack of appreciation for quickly adapting technologies and production processes in PAs. Additionally, there is a need for better coordination between entities such as OFB, DPSUs and private sector institutions to effectively serve both the military and R&D needs. Addressing these issues requires a thorough reassessment of procedures, systems and methods to manage these complex interactions.[319]

While DRDO has achieved notable successes in its core areas, there's a recognised need to establish collaborative partnerships with the private sector. This collaboration aims to foster competitiveness and enhance focus on achieving results in both research and production endeavours. Identifying specific areas where private sector involvement is beneficial is crucial, and swift action should be taken to implement these partnerships within a defined timeframe.[320] All these point to a two-fold concern and apprehension, back even in 2001, that the Indian Armed Forces needed to absorb and leverage new technologies quickly and that this will not be accomplished without involving the private sector. However, as we will see below, the mere mention or involvement of the private sector does not automatically lead to innovation, either defence or military, due to certain entrenched mindsets and organisational idiosyncrasies that prevent the civil–military integration required for innovation.

In fact, the GoM Report emphasises that the DRDO '*needs to focus more on core technologies, in which expertise is neither available within the country* *nor can be procured from alternative sources. At the same time, on a case to case basis, short term R&D on parts, components and sub-assemblies can be undertaken by the PAs and in certain cases also by the Services.*'[321] Continuing with the report's recommendations to accelerate technological advancements and ensure access to cutting-edge weapon systems, it is equally imperative to leverage both domestic and international expertise, including non-resident Indians (NRIs). Instead of heavy investments in developing technologies already available or achievable with NRI assistance, prudent utilisation of existing know-how is advised. DRDO can offer guidance to facilitate successful project completion by PAs and the Services when needed. Over time, select PAs could be designated as key agencies for platform development and production, with DRDO providing necessary technical support.

Rationalising DRDO laboratories and fostering closer collaboration between specific labs and production agencies/Service entities are crucial. A committee led by the secretary of Department of Defence Production & Supplies (DDP&S), alongside the scientific adviser to the defence minister and the three Service chiefs, should promptly evaluate this rationalisation and present recommendations to the defence minister for consideration.[322] The report's final recommendations with respect to technology absorption called for an urgent need for a swift review of procedures governing procurement decisions for major weapon systems/platforms under 'make', 'buy' or 'buy and make' categories. Additionally, it adds that there was a pressing requirement to refine the linkage between financial commitments in R&D and performance milestones to enhance accountability and timeliness, which the MoD must address promptly. It concluded with refining the Decision Aid for Technology Evaluation (DATE) formulation by DRDO for project indigenisation before it could be effectively utilised for decision-making purposes.[323]

If one looks at two issues: the restructuring of the DRDO where it has been told to focus on basic R&D and not get into prototype or proof of concept, and how problem definition statements are defined, who initiates them and how they are collated by the Army Design Bureau (ADB) from different arms (line directorates in Indian Army jargon) to be further disseminated to the industry, it is clear that the philosophy enshrined in the 2001 Report is alive and kicking.

Now, coming to the ways and means through which MoD has involved itself with R&D and innovation. The Defence Innovation Organisation (DIO) was created on the lines of the DIUx during one of the bilateral visits between officials from India and the US as part of the Defence Technology and Trade Initiative (DTTI).[324] It was officially launched during DefExpo 2018, and is meant to act as a corporate VC for Indian defence and national security requirements. DIO as a board organises iDEX (which can also be termed as the executive arm of DIO) and the challenges are called Defence India Startup Challenges (DISC). DIO is a Section 8 (Companies Act of 2013) company that has been formed by an initial contribution of Rs 50 crores each by two DPSUs, that is, Hindustan Aeronautics Limited (HAL) and Bharat Electronics Limited (BEL). The organisational structure of DIO comprises a DIO Board consisting of the chief managing directors (CMDs) of HAL and BEL, secretary defence production (DP), assistant secretary DP (AS DP) and the MD of AIM. Secretary DP is the chairman of DIO, while AS DP is the chief executive officer (CEO). Apart from these appointments, the DIO Board also selects a chief finance officer (CFO), advisor and chief secretary (CS).

The main task of interacting with defence startups and MSMEs, through partner incubators (PIs), is given to the program directors (PDs) and program executives (PEs), who are tasked by the chief operating officer (COO). The funding for the program is provided through a Defence Innovation Fund (DIF) under the Department of Defence Production (DDP), which has a total amount of Rs 500 crores to be handed over to 300 startups and MSMEs as well as partner incubators and defence innovation hubs (DIHs). Apart from DIF and the initial corpus, additional funds for the startups are being solicited by inviting DPSUs such as Bharat Earth Movers Limited (BEML), Bharat Dynamics Limited (BDL), Mazagon Dock Limited (MDL) and similar bodies to contribute up to 2 per cent of their profits to DIO. DPSUs are required to mark 25 per cent of their corporate social responsibility (CSR) funds to support iDEX.[325] Other government departments may also fund iDEX if they feel that some of the challenges being solved by iDEX are relevant for them.

DIO, through iDEX, or its common nomenclature DIO-iDEX, performs three critical functions of co-innovation and/or co-creation (with organisations that are likely to absorb these technologies); piloting of technologies through a feedback loop; and indigenisation of platforms related to defence and aerospace. The main tasks of iDEX, as the executive arm of DIO is to manage the iDEX network in the form of independent DIHs, communicate the needs of defence and aerospace to startups and innovators through the DIHs, organise various challenges and hackathons, evaluate technologies and products, enable and fund pilots, interface with the military and facilitate scaling, indigenisation and commercialisation of successfully piloted technologies.[326] The initial focus on defence and aerospace has been expanded to cover specific problem definition statements (PDS) by the forces and to direct interaction with startups, at least up to the selection stage.

Overall, the aim of iDEX is to coordinate between the requirements of the end-user, that is, the military, existing system integrators and assemblers such as DPSUs and the innovation ecosystem, which consists of defence startups and MSMEs. This is done through coordinating with iDEX PIs such as independent DIHs like FORGE in Coimbatore and T-Hub at Hyderabad[327] in addition to two officially created DIHs at Coimbatore District Small Industries Association (CODISSIA), Coimbatore and Nashik Industries and Manufacturers Association (NIMA), Nashik.[328] The PIs have been given a critical role and are supposed to act as a facilitating medium between iDEX and the users.

Among the main roles given to PIs are supporting iDEX–DIO in creating an ecosystem to interact with startups and MSMEs to address the technological needs of the armed forces; assisting iDEX winners and MSMEs with prototyping; providing mentoring, incubation and accelerator support to iDEX winners and MSMEs; and promoting defence innovation in schools and colleges.[329] The PIs are also supposed to assist iDEX in setting milestones and objectives of the projects of the iDEX winners, this is in addition to providing techno-financial due diligence of grant winners at each milestone.[330] iDEX also runs the Innovate for Defence (i4D) internship program, which offers a 45-day internship opportunity to a batch of 75–100 students from schools and HEIs.[331]

A short addendum on TRLs before we move further. The question of technology maturity and its associated risks emerges primarily when dealing with nascent or novel technologies that are yet to prove their effectiveness in practical applications. Technologies at lower levels of maturity pose inherent risks when transitioning into downstream stages of production or manufacturing. At this juncture, design and engineering activities face challenges as the technology may not be mature enough to optimise cost, time, inventory and defect management effectively.

Since TRL methodology was created when space and military applications drove technological innovations and advances in multiple fields, the same needs be contextualised. From the Indian perspective, where the maturity of the technology is less risky than the military grade product it has to be embedded in and the functionality of that product as a whole.

This is the reason why iDEX was designed to include the parameters of functional compliance, performance, design readiness and level of integration at each TRL from one to nine. There are seven product categories defined for TRLs and customised for end use operations, land platforms, naval platforms, air platforms, platforms/systems not operating in tactical warfare, software only products operating in field systems and software only products integrated with existing IT systems.[332] Categorisation of likely solutions and products for TRL levels is a good option but the current typology may not function effectively; this shortcoming will be explained in the challenges section. Also, iDEX's approach is towards product management rather than technology management where the former orients a particular technological solution to an expressed requirement by the user. Though the PMA guidelines advocate an 'open innovation' approach, implying co-creation and co-development with the user to create a right product mix,[333] as of now, this has been limited to defining the PDS by the user.

An R&D branch within most of the user agencies may be seen as amendment to this approach. The parameters that need to be defined by the user include features & functionalities; usage/usability/operational constraints; performance parameters/metrics; integration/verification to target platform; test plans and procedures for end-user trials; and applicable quality assurance (QA)/military grade standards. The granularity of the details should be so that the product can be mapped to TRL 8, which enables a system to be completed and qualified through test and demonstration. The end product of all the development, trials, testing and validation is the minimum viable product (MVP), which is the stage all solutions are supposed to reach and denote an acceptability of the solution to the user.[334] The MVP is broken down into five parts, which are hierarchical in nature. At the top is the product itself, followed by sub-system, module, component and attribute. The first two, that is, the product and the sub-system are subject to the TRL methodology while the last three are subject to development progress indicators. Once the MVP stage is reached, the government can also exercise its GPR and March In rights[335] if the product is considered to be too sensitive from the perspective of national security.

How does DIO–iDEX Function?

The handholding impetus to startups given by the Indian government and the opening up of the defence sector to them inundated the Services with multiple options from startups with no in-house expertise to select, co-develop or co-create. DIO was then created as the bridge between the startups and end users (the three Services). Now, the basic process through which the interfacing between iDEX and the user Service is done is that first the specific arms or directorates within the army provide their requirements to the ADB, which curates the requirements, vets the problem statements from a procedural perspective and hands it over to the DIO.[336] DIO curates the statements and launches the problem statements in the form of either iDEX,[337] iDEX Prime[338] or the newly launched Acing Development of Innovative Technologies with iDEX (ADITI).[339] The iDEX challenges are either through DISC or Open Challenges (OC).[340]

OCs are based on discussions with the Services or on certain revolutionary technology that the startup(s) feel(s) will benefit the forces. Initial scrutiny is done by DIO for checking for duplicity or incomplete forms. The final list is given to the forces, which with their recommendations is sent it to a high-powered selection committee (HPSC). Once proposals are received from the startups, they are sent to the Services for review and shortlisting. DIO then convenes a HPSC with representatives of DPSUs, industry, subject matter experts (SMEs), DRDO and end users. The HPSC is chaired by the head of the organisation that has requested the proposal, for example, the Additional Director General (ADG) ADB or head of a particular DPSU. Startups are given 10 minutes each for their proposals. They can pitch for five minutes, which is followed by a question and answer (Q&A) session of five minutes. Then members of the HPSC score the proposal individually, post which the fate of the proposal is decided based on a majority basis.[341] This process needs to be lengthened as 10 minutes may be inadequate to get into the details of the proposals.

Once the startups are selected, they are issued with the PDS and allocated product functional units (PFUs). The latter translate the PDSs into sub-system component level functional units.[342] After this, the five milestones are given. Milestone 0 is the signing of the Support for Prototype and Research Kickstart (SPARK) agreement where for every stage of approving a grant of Rs 1.5 crores based on a division of 10-20-30-20-10 per cent a matching contribution from a civilian partner is also mandated. Milestone 1 is technical evaluation, milestones 3 and 4 are single stage composite trials (sometimes the Services start their procurement from here) and milestone 5 is the delivery stage when the conventional acquisition phase, that is, the request for information (RFI) and request for proposal (RFP) stage starts.[343] DIO outsources the hand holding of startups to PIs, which are mostly based inside IITs and other reputed technical universities and colleges. Their task is to look at milestone reports, techno-commercial reports and financial reviews. They are paid annually by the government based on the number of startups supported by them. Each incubator is paired with certain number of startups, based on their request. The role of PIs is also to facilitate access to government facilities such as labs and ranges through DIO on a free or nominal price, provide technical guidance and most importantly, institutional support.

The Indian Army Innovation Ecosystem

The Indian Army's defence innovation ecosystem is centred around the ADB whose role is 'to undertake technology scan, identify technologies for acquisition and development, facilitate R&D efforts with Industry, Academia, DRDO & DPSUs, provide inputs and enable them to understand user requirements while initiating cases of design & development with the industry, all with the aim of promoting indigenisation'.[344] The mandate of ADB is to promote indigenisation. An in-house R&D innovation body created in parallel with the ADB may be envisaged to promote grounded innovation within the army. The ADB uses a number of pathways to involve defence startups and MSMEs in solving specific problems and challenges facing the different arms and branches of the Service. These pathways include the Army Technology

Board (ATB), handled by ADB and headed by the Deputy Chief of Army Staff (Capability Development and Sustenance) (DCOAS CD&S); Technology Development Fund (TDF), handled by DRDO, iDEX, Make projects (I, II and III); and direct commercial sales through the Army Commander's Special Financial Powers (ACSFP).[345]

Coming to the first method, the ATB identifies, approves and funds technological research, studies and development projects using the Indigenisation, R&D (INRD) fund under the schedules 9.1 to 9.3 provisions of the Army Schedule of Powers (ASP) 2021, which forms a part of the Delegation of Financial Powers to Defence Services (DFPDS) 2021.[346] The fund gives powers of up to Rs 16.5 crores to the Vice Chief of the Army Staff (VCOAS), Rs 7.5 crores to the General Officer Commanding in Chief (GOC-in-C) of the Army Training Command (ARTRAC) and DCOAS (CD&S), Rs 5 crores to Director Generals of the Electronics and Mechanical Engineers (EME), Engineer in Chief (E-in-C) and Signals Officer in Chief (SO-in-C) and Rs 1 crore to all other army commanders to undertake a host of design and development activities for undertaking R&D activities through the private sector.

These respective powers are increased to Rs 27.5 crores, Rs 12.5 crores, Rs 6.25 crores and Rs 2 crores for undertaking R&D through in-house defence agencies, army units and formations, government organisations or technical institutions such as the IITs on a proprietary basis.[347] The projects that can be undertaken using this fund are very comprehensive. They include weapon system integration, software development, design and development (D&D) activities for the army, model test analysis, expenditure on fabrication and manufacturing, procurement of stores for testing and trials and even offloading certain D&D activities to the academia.[348] The INRD fund has started in the past two years to be used extensively for promoting innovative solutions for the army.[349] The ATB convenes an annual board meeting chaired by the DCOAS CD&S,[350] which vets and selects proposals received in response to the compendium of problem definition statements (CPDS).[351] However, the ATB route limits itself to the development of a prototype with an initial minimum order quantity (MOQ) for the startup. If the startup's equipment or technology is felt to have created an impact on the ground, it has to compete under the conventional acquisition process for further orders.

The second process is that of TDF, which is managed by DRDO. It provides a funding support of up to Rs 50 crores, subject to a maximum of 90 per cent of the total project cost, to defence startups and MSMEs whose potential use for the forces have a development period of maximum two years.[352] The TDF was formed as a joint collaboration between DRDO and Global Innovation and Technology Alliance (GITA), a non-profit venture of the Confederation of Indian Industries (CII),[353] and has now enrolled the expertise of Invest India for promoting the scheme.[354] The scheme considers four types of proposals for funding support. The proposal should either be a significant upgradation of or improve upon existing military systems; it should demonstrate a pathway from TRL 3 to a finished product for the armed forces; focus on the development of new and future-oriented products for defence applications and finally, import substitution of components for technologies not available in India.[355] The IP generated will be shared between DRDO and the selected startup, and the startup can sell to user agencies, but only as a sub-contractor for DRDO. In addition to TDF, a Dare to Dream competition has been launched, which invites individuals and startups to create and provide radical solutions in certain emerging technologies identified by DRDO.[356] One of the major issues with TDF is that initially all projects under TDF required a service sponsor. Till early 2020, only the three Services could sponsor. Then the Indian Coast Guard (ICG) was added. In late 2020, the Chairman DRDO also added the organisation itself as a sponsor. Now a significant chunk of the projects under TDF are DRDO sponsored.[357]

The third route of iDEX has already been discussed in detail before. The fourth route is that of Make. There are three categories of Make that promote Make in India products. Make I is government funded, which involves the D&D of equipment, systems and major platforms by the industry. Under this category, MoD provides up to 70 per cent of funding support for prototype development or up to Rs 250 crores per development agency (DA). Make II and III concern the D&D of 'equipment/system/platform or their upgrades or their subsystems/sub-assembly/assemblies/components/materials/ammunition/software, primarily for import substitution'. While Make II is industry funded and looks at innovative solutions by Indian vendors without government funding, Make III encourages firms to enter into a joint venture (JV) or transfer of technology (ToT) with foreign OEMs for technologies and products that can be manufactured as import substitutions for 'product support of weapon systems/equipment held in the inventory of the Services'.[358] The final route is direct commercial sales.[359] For catering to all these categories, ADB has five dedicated officers of colonel level. Colonel ADB (Industry) looks at proposals by firms, new technologies and products and also facilitates firing ranges and equipment for development. Colonel ADB (Field Formation) coordinates with arms and DIO for iDEX projects while also facilitating capability demonstration of equipment and technologies in field areas. Colonel ADB (Make) looks at Make II projects and resolves queries of firms. Colonel ADB (Academia) vets research proposals from academia while Colonel ADB (DRDO) coordinates with DRDO for TDF projects.[360]

NOTES

[1] Summer Myatt, "How DOD's Strategic Capabilities Office Is Taking a New Approach to Defense Innovation", Govcon Wire, February 8, 2024, at https://www.govconwire.com/2024/02/how-dods-strategic-capabilities-office-is-taking-a-new-approach-to-defense-innovation/, (Accessed March 1, 2024)

[2] Major Roye Locklear, Jr, "The Army of 2040: An Extension of the 2030 Goals", Land Warfare Paper 154, Association of the United States Army Publication, March 2023, at https://www.ausa.org/sites/default/files/publications/LWP-154-The-Army-of-2040-An-Extension-of-the-2030-Goals_0.pdf, (Accessed March 1, 2024).

[3] "National Security Strategy of the United States of America" at https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, (Accessed March 1, 2024).

[4] "National Security Strategy October 2022" at https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf, (Accessed March 2, 2024).

[5] "Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge" at https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, (Accessed March 2, 2024).

[6] "U.S. Department of Defense National Defense Strategy of The United States of America Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review" at https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF, (Accessed March 2, 2024).

[7] Cheryl Pellerin, "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence", *DOD News*, October 31, 2016, at https://www.defense.gov/News/News-Stories/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence, (Accessed March 1, 2024).

[8] Eric P Hillner, "The Third Offset Strategy and the Army Modernization Priorities", Director's Action Group Report, Centre for Army Lessons Learned (CALL), May 2019, at https://usacac.army.mil/sites/default/files/publications/17855.pdf, (Accessed March 3, 2024).

[9] Benjamin Jensen, "Think Bigger: The Third Offset and Extending the Battlefield", War on the Rocks, December 12, 2016, at https://warontherocks.com/2016/12/think-bigger-the-

third-offset-and-extending-the-battlefield, (Accessed March 3, 2024).

10 Sean Carberry and Stew Magnuson, “SPECIAL REPORT: A Snapshot of 24 Programs the Army Promised to Expedite”, National Defense, October 3, 2023, at https://www.nationaldefensemagazine.org/articles/2023/10/3/a-snapshot-of-24-programs-the-army-promised-to-expedite#:~:text=Its%20focus%20was%20on%20six,years%20stuck%20to%20this%20list, (Accessed March 3, 2024).

11 Guy Snodgrass, “Episode 7 - Third Offset Strategy (Part I)”, Podcast, April 24, 2020, at https://podcast.app/third-offset-strategy-part-i-e94081309, (Accessed March 4, 2024).

12 Robert M Gates, *Duty: Memoirs of a Secretary at War*, Alfred A. Knopf, New York, 2014, p. 528.

13 US Army Training and Doctrine Command (TRADOC) G-2, “Operational Environments to 2028: The Strategic Environment for Unified Land Operations”, August 20, 2012, at https://www.moore.army.mil/mssp/security%20topics/Potential%20Adversaries/content/pdf/OE%20to%202028%20final%20signed.pdf, (Accessed March 4, 2024).

14 Dmitri Trenin, “True Partners? How Russia and China See Each Other”, Centre for European Reform, at https://carnegieendowment.org/files/Trenin_CER_Eng.pdf, (Accessed March 4, 2024).

15 Kyle Mizokami, “The U.S. Could Soon Lose Air Superiority”, *Popular Mechanics*, March 6, 2024, at https://www.popularmechanics.com/military/aviation/a60030380/us-could-soon-lose-air-superiority, (Accessed March 7, 2024).

16 Brad Stapleton, “The Problem with the Light Footprint: Shifting Tactics in Lieu of Strategy”, Cato Institute, Policy Analysis No 792, June 7, 2016, at https://www.cato.org/policy-analysis/problem-light-footprint-shifting-tactics-lieu-strategy, (Accessed March 4, 2024).

17 Marcos A. Melendez III, Michael E. O’Hanlon and Jason Wolff, “America Can’T Afford to Ignore the Logistics Triad”, Brookings, July 2023, at https://www.brookings.edu/articles/america-cant-afford-to-ignore-the-logistics-triad, (Accessed March 4, 2024).

18 US Army Training and Doctrine Command (TRADOC) G-2, “The Operational Environment (2021-2030): Great Power Competition, Crisis, and Conflict”, April 2021, at https://apps.dtic.mil/sti/trecms/pdf/AD1156584.pdf, (Accessed March 5, 2024).

19 Javier Jordan, “International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict”, *Journal of Security Studies*, 14(1), 2020, pp. 1–24.

20 Robert O. Work and Shawn Brimley, “20YY: Preparing for War in the Robotic Age”, Centre for New American Security Research Report, January 1, 2014, p. 44, at https://www.jstor.org/stable/resrep06442, (Accessed March 5, 2024).

21 Ibid.

22 Cheryl Pellerin, “DoD Tech Transformation Holds Surprises for U.S. Adversaries”, *DOD News*, April 12, 2016, at https://www.defense.gov/News/News-Stories/Article/Article/719222/dod-tech-transformation-holds-surprises-for-us-adversaries, (Accessed March 5, 2024).

23 Col. Gabriel W. Pryor, “Logistics in the Indo-Pacific: Setting the Theater for a Conflict over Taiwan”, *Army Sustainment Journal*, February 1, 2024, at https://www.army.mil/article/272919/logistics_in_the_indo_pacific_setting_the_theater_for_a_conflict_over_taiwan#:~:text=To%20forestall%20intervention%20by%20external,threaten %20China%20in%20a%20conflict, (Accessed March 5, 2024).

24 Hal Brands and Zack Cooper, “Dilemmas of Deterrence: The United States’ Smart New Strategy Has Six Daunting Trade-offs”, The Marshall Papers, Centre for Strategic and International Studies (CSIS), March 12, 2024, at https://www.csis.org/analysis/dilemmas-deterrence-united-states-smart-new-strategy-has-six-daunting-trade-offs, (Accessed March 17,

2024).

25 Gian Gentile, Michael Shurkin, Alexandra T Evans, Michelle Grise, Mark Hvizda and Rebecca Jensen, "A History of the Third Offset, 2014-2018", RAND Report, March 31, 2021, p. 35, at https://www.rand.org/pubs/research_reports/RRA454-1.html, (Accessed March 6, 2024).

26 Ibid., p. 42–4.

27 Daniel Flott, "America First, Third Offset Second?", *The RUSI Journal*, 163(4), October 17, 2018, pp. 40–8.

28 Gian Gentile, Michael Shurkin, Alexandra T Evans, Michelle Grise, Mark Hvizda and Rebecca Jensen, no. 149, p. 25.

29 "Remarks by Deputy Secretary Work on Third Offset Strategy" at https://www.defense.gov/News/Speeches/Speech/Article/753482/remarks-by-deputy-secretary-work-on-third-offset-strategy, (Accessed March 6, 2024).

30 Ellen Grover, "What is AI Winter?", Built In, April 21, 2023, at https://builtin.com/artificial-intelligence/ai-winter, (Accessed March 6, 2024).

31 "The Third U.S. Offset Strategy and its Implications for Partners and Allies" at https://www.defense.gov/News/Speeches/Speech/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies, (Accessed March 6, 2024).

32 Gian Gentile, Michael Shurkin, Alexandra T Evans, Michelle Grise, Mark Hvizda and Rebecca Jensen, no. 149, p. 3.

33 "Defense Science Board Summer Study on Autonomy" at https://dsb.cto.mil/reports/2010s/DSBSS15.pdf, (Accessed March 6, 2024).

34 "Innovative Solutions for National Security" at https://dsb.cto.mil/index.htm, (Accessed March 6, 2024).

35 "Defense Science Board Summer Study on Autonomy", p. iii, at https://dsb.cto.mil/reports/2010s/DSBSS15.pdf, (Accessed March 6, 2024).

36 Ibid.

37 Ibid., p. 98.

38 Ibid., p. iii.

39 Gian Gentile, Michael Shurkin, Alexandra T Evans, Michelle Grise, Mark Hvizda and Rebecca Jensen, no. 149, p. 42.

40 Ibid.

41 NSWCDD Corporate Communications, "Milestones to Medals: NSWC Dahlgren Division Computer Scientist Earns the Navy Civilian Service Commendation Medal", Naval Sea Systems Command News, Dahlgren, Virginia, December 23, 2022, at https://www.navsea.navy.mil/Media/News/Article/3254249/milestones-to-medals-nswc-dahlgren-division-computer-scientist-earns-the-navy-c, (Accessed March 6, 2024).

42 "New Joint Interagency Combined Space Operations Center to Be Established" at https://www.defense.gov/News/Releases/Release/Article/616969/new-joint-interagency-combined-space-operations-center-to-be-established, (Accessed March 6, 2024).

43 Nathan Strout, "Intelligence Agency Takes Over Project Maven, the Pentagon's Signature AI Scheme", C4ISRNet, April 27, 2022, at https://www.c4isrnet.com/intel-geoint/2022/04/27/intelligence-agency-takes-over-project-maven-the-pentagons-signature-ai-scheme, (Accessed March 6, 2024).

44 Mark Pomerleau, "DepSecDef: JICSpOC Is First Organizational Construct of the Third Offset," C4ISRNet, September 21, 2016, at https://www.c4isrnet.com/c2-comms/2016/09/21/depsecdef-jicspoc-is-first-organizational-construct-of-the-third-offset, (Accessed March 7, 2024).

[45] “DoD to Set Up New Centre for Interagency Information Sharing” at https://thesimonscenter.org/ia-news/new-center-for-ia-info-sharing, (Accessed March 7, 2024).

[46] “US Space Forces - Space” at https://www.jtf-spacedefense.mil/About-Us/Fact-Sheets/Display/Article/3071003/national-space-defense-center, (Accessed March 7, 2024).

[47] Scott Shane and Daisuke Wakabayashi, “‘The Business of War’: Google Employees Protest Work for the Pentagon”, *The New York Times*, New York, April 4, 2018, at https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html, (Accessed March 7, 2024).

[48] Marcus Weisgerber, “The Pentagon’s New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS”, Defense One, May 14, 2017, at https://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833, (Accessed March 7, 2024).

[49] Jaspreet Gill, “Now That Maven Is a Program of Record, NGA Looks At LLMs, Data Labeling”, Breaking Defense, November 16, 2023, at https://breakingdefense.com/2023/11/now-that-maven-is-a-program-of-record-nga-looks-at-llms-data-labeling/ , (Accessed March 7, 2024)

[50] Nathan Strout, no. 167.

[51] Gian Gentile, Michael Shurkin, Alexandra T Evans, Michelle Grise, Mark Hvizda and Rebecca Jensen, no. 149, pp. 42–8.

[52] James Hasik, “Beyond the Third Offset: Matching Plans for Innovation to a Theory of Victory”, *Joint Force Quarterly 91*, October 30, 2018, at https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1676275/beyond-the-third-offset-matching-plans-for-innovation-to-a-theory-of-victory, (Accessed March 7, 2024).

[53] William T Eliason, “An Interview with Robert O. Work”, *Joint Force Quarterly 84*, January 26, 2017, at https://ndupress.ndu.edu/Media/News/Article/1038783/an-interview-with-robert-o-work, (Accessed March 8, 2024).

[54] “Innovation on a Mission” at https://www.iqt.org, (Accessed March 8, 2024).

[55] Ibid.

[56] “An Open Source Capabilities Shop” at https://www.iqt.org/labs, (Accessed March 8, 2024).

[57] “Projects: What’s on the IQT Labs Work Bench?” at https://iqtlabs.org/projects, (Accessed March 8, 2024).

[58] “DIU to Expand Efforts to Midwest to Identify Broader Commercial Solutions for Department of Defense Needs” at https://www.diu.mil/latest/dius-new-regional-focus, (Accessed March 8, 2024).

[59] “Work with Us” at https://www.diu.mil/work-with-us, (Accessed March 8, 2024).

[60] “Commercial Solutions Catalog” at https://www.diu.mil/solutions/portfolio/catalog, (Accessed March 8, 2024).

[61] “Doug Beck” at https://www.diu.mil/team/doug-beck, (Accessed March 8, 2024).

[62] “Our Team” at https://www.diu.mil/team, (Accessed March 8, 2024).

[63] Ibid.

[64] “We Work with Top Companies to Solve Today’s National Security Problems” at https://www.diu.mil/solutions/portfolio, (Accessed March 8, 2024).

[65] No. 184.

[66] “What is an Other Transaction Agreement (OTA)?” at https://www.osp.pitt.edu/news/what-other-transaction-agreement-ota#:~:text=An%20Other%20Transaction%20Agreement%2FAuthority,projects%20with%2 0nonprofit%20research%20institutions, (Accessed March 8, 2024).

[67] “Contract Comparison: Why Use Another Transaction Authority (OTA) Contract Vs. Federal

Acquisition Regulation (FAR) Based Contract?" at https://www.defenseacq.com/ota-contract-vs-far-based-contract, (Accessed March 8, 2024).

68 Gian Gentile, Michael Shurkin, Alexandra T Evans, Michelle Grise, Mark Hvizda and Rebecca Jensen, no. 149, p. iii.

69 Ibid., p. 62.

70 Alex Vershinin, "The Challenge of Dis-Integrating A2/AD Zone: How Emerging Technologies Are Shifting the Balance Back to the Defense", *Joint Force Quarterly 97*, March 31, 2020, at https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106488/the-challenge-of-dis-integrating-a2ad-zone-how-emerging-technologies-are-shifti, (Accessed March 8, 2024).

71 US Army Training and Doctrine Command (TRADOC), "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040", Version 1.0, December 2017, at https://www.tradoc.army.mil/wp-content/uploads/2020/10/MDB_Evolutionfor21st.pdf, (Accessed March 9, 2024).

72 Ibid., p. i.

73 Ibid., p. 2.

74 "Defense Primer: Army Multi-Domain Operations (MDO)" at https://sgp.fas.org/crs/natsec/IF11409.pdf, (Accessed March 9, 2024).

75 US Army Training and Doctrine Command (TRADOC), no. 195, p. 3.

76 Ibid., pp. 52–67.

77 Ibid., no. 195, p. 12.

78 Ibid., p. 16.

79 Ibid.

80 Ibid., p. 3.

81 Ibid., p. 25.

82 Ibid., p. 16.

83 Ibid., pp. 52–67.

84 Ibid., p. 16.

85 US Army Training and Doctrine Command (TRADOC), "The U.S. Army in Multi Domain Operations 2028", Pamphlet 525-3-1, December 6, 2018, p. iii, at https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf, (Accessed March 9, 2024).

86 Ibid.

87 Ibid., p. vii.

88 Ibid., p. E-2.

89 US Army Training and Doctrine Command (TRADOC), "FM 3-0 Operations," October 2022, at https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf, (Accessed March 9, 2024).

90 "The US Army's Multi-Domain-Operations Doctrine" at https://www.iiss.org/en/publications/strategic-comments/2022/the-us-armys-multi-domain-operations-doctrine/#:~:text=The%20doctrine%20focuses%20on%20limiting,defeated%20using%20long%2Drange%20firepower, (Accessed March 9, 2024).

91 "2019 Army Modernization Strategy: Investing in the Future" at https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf, (Accessed March 9, 2024).

92 "What We Do" at https://devcom.army.mil/what-we-do, (Accessed March 10, 2024).

93 "DoD Releases National Defense Science and Technology Strategy" at https://www.defense.gov/News/Releases/Release/Article/3389118/dod-releases-national-defense-science-and-technology-strategy, (Accessed March 10, 2024).

94 "National Defense Science and Technology Strategy 2023", p. 4, at https://www.cto.mil/

wp-content/uploads/2023/05/2023-NDSTS.pdf, (Accessed March 10, 2024).

95 Brandi Vincent, “Defense Department Previews New Future-Facing Technology Aims”, *Defense One*, February 3, 2022, at https://www.nextgov.com/emerging-tech/2022/02/defense-department-previews-new-future-facing-technology-aims/361578, (Accessed March 10, 2023).

96 “National Security Innovation Network” at https://nsin.mil, (Accessed March 10, 2024).

97 “Defense Innovation Unit” at https://www.diu.mil, (Accessed March 10, 2024).

98 “Defensewerx” at https://defensewerx.org, (Accessed March 10, 2024).

99 “Sofwerx” at https://sofwerx.org, (Accessed March 10, 2024).

100 “Afwerx: Unleashing American Ingenuity” at https://afwerx.com, (Accessed March 10, 2024).

101 “NavalX: Work at the Speed of Relevance” at https://www.secnav.navy.mil/agility/Pages/newhome.aspx, (Accessed March 10, 2024).

102 “Army Applications Laboratory” at https://aal.army, (Accessed March 10, 2024).

103 “XTech” at https://www.xtech.army.mil, (Accessed March 10, 2024).

104 Jennifer-Leigh Oprihory, “ARCWERX Will Leverage ANG, Reserve Innovation to Enhance Total Force,” *Air & Space Forces Magazine*, May 13, 2020, at https://www.airandspaceforces.com/arcwerx-will-leverage-ang-reserve-innovation-to-enhance-total-force, (Accessed March 10, 2024).

105 “Joint Rapid Acquisition Cell” at https://www.acq.osd.mil/asda/jrac/index.html, (Accessed March 10, 2024).

106 “Kessel Run” at https://kesselrun.af.mil, (Accessed March 10, 2024).

107 Brodi Kotila, Jeffrey A Drezner, Elizabeth M Bartels, Devon Hill, Quentin E Hodgson, Shreya S Huilgol, Shane Manuel, Michael Simpson and Jonathan P Wong, “Strengthening the Defense Innovation Ecosystem”, RAND Research Report, 2023, p. 10, at https://www.rand.org/pubs/research_reports/RRA1352-1.html, (Accessed March 10, 2024).

108 Ibid., p. xiii.

109 Ibid.

110 “Acquisition Process” at https://acqnotes.com/acqnote/acquisitions/milestone-b, (Accessed March 10, 2024).

111 Ibid.

112 “What is the purpose of SBIR & STTR programs?” at https://www.sbir.gov/tutorials/program-basics/tutorial-1, (Accessed March 10, 2024).

113 “The Three Phases of SBIR/STTR” at https://www.sbir.gov/about, (Accessed March 10, 2024).

114 “How Do I Develop a Relationship with a Defense Prime Contractor?” at https://www.sbir.gov/tutorials/finding-partners/tutorial-2, (Accessed March 11, 2024).

115 “Army Futures Command” at https://www.army.mil/futures, (Accessed March 11, 2024).

116 Jen Judson, “US Army to Stand Up Cross-Functional Team for Deep Sensing”, *Defense News*, March 7, 2024, at https://www.defensenews.com/land/2024/03/07/us-army-to-stand-up-cross-functional-team-for-deep-sensing, (Accessed March 11, 2024).

117 “Cross Functional Teams” at https://www.army.mil/futures#org-who-we-are, (Accessed March 11, 2024).

118 “Supporting Commands” at https://www.army.mil/futures#org-who-we-are, (Accessed March 11, 2024).

119 Ibid.

120 “Who We Are” at https://devcom.army.mil/who-we-are, (Accessed March 11, 2024).

121 “What We Do” at https://devcom.army.mil/what-we-do, (Accessed March 11, 2024).

122 No. 245.

123 "DEVCOM ARL" at https://devcom.army.mil/centerslabs/arl, (Accessed March 11, 2024).

124 "ARO 2022 Year in Review" at https://arl.devcom.army.mil/wp-content/uploads/sites/3/2023/06/ARO-YEAR-IN-REVIEW-2022-WEB-FINAL.pdf, (Accessed March 11, 2024).

125 "ARL Broad Agency Announcement (BAA)" at https://arl.devcom.army.mil/collaborate-with-us/opportunity/arl-baa, (Accessed March 11, 2024).

126 "Federally Funded Research and Development Centers and University Affiliated Research Centers" at https://defenseinnovationmarketplace.dtic.mil/ffrdcs-uarcs, (Accessed March 11, 2024).

127 "Department of Defense Multidisciplinary University Research Initiative (MURI)" at https://arl.devcom.army.mil/collaborate-with-us/opportunity/muri, (Accessed March 11, 2024).

128 "Small Business Innovation Research/ Small Business Technology Transfer" at https://arl.devcom.army.mil/collaborate-with-us/opportunity/sbir-sttr, (Accessed March 11, 2024).

129 Ibid.

130 No. 246.

131 "Artificial Intelligence of Maneuver and Mobility (AIMM)" at https://arl.devcom.army.mil/what-we-do/aimm, (Accessed March 11, 2024).

132 "Emerging Overmatch Technologies (EOT)" at https://arl.devcom.army.mil/what-we-do/eot, (Accessed March 11, 2024).

133 "Foundational Research for Electronic Warfare in MDO (FREEDOM)" at https://arl.devcom.army.mil/what-we-do/freedom, (Accessed March 11, 2024).

134 "Human Autonomy Teaming (HAT)" at https://arl.devcom.army.mil/what-we-do/hat, (Accessed March 11, 2024).

135 "Long Range Distributed and Collaborative Engagements (LRDCE)" at https://arl.devcom.army.mil/what-we-do/lrdce, (Accessed March 11, 2024).

136 "Physics of Soldier Protection to Defeat Evolving Threats (PSPDET)" at https://arl.devcom.army.mil/what-we-do/pspdet/#:~:text=The%20PSPDET%20ERP%20is%20developing,and%20research %20in%20computational%20mechanics, (Accessed March 11, 2024).

137 "Quantum Information Sciences - Position, Navigation and Timing (QIS-PNT)" at https://arl.devcom.army.mil/what-we-do/qis-pnt/#:~:text=The%20QIS%2DPNT%20ERP%20is,communication%20across%20all%20combat%20environments, (Accessed March 11, 2024).

138 "Transformational Synbio for Military Environments (TRANFORME)" at https://arl.devcom.army.mil/what-we-do/transforme, (Accessed March 11, 2024).

139 "Versatile Tactical Power and Propulsion (VICTOR)" at https://arl.devcom.army.mil/what-we-do/victor, (Accessed March 11, 2024).

140 "Futures and Concepts Center" at https://www.army.mil/futuresandconceptscenter#org-organizations, (Accessed March 11, 2024).

141 Ibid.

142 Ibid.

143 James M. Richardson, "Project Convergence: A Venue for Joint All-Domain Command and Control Experimentation", *Joint Force Quarterly 107*, October 25, 2022, at https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3197270/project-convergence-a-venue-for-joint-all-domain-command-and-control-experiment, (Accessed March 11, 2024).

144 US Naval Institute Staff, "Report to Congress on Army's 'Project Convergence'", *USNI News*, June 3, 2022, at https://news.usni.org/2022/06/03/report-to-congress-on-armys-project-convergence, (Accessed March 11, 2024).

145 Andrew Feickert, "The Army's Project Convergence", Congressional Research Service (CRS), June 2, 202, at. https://sgp.fas.org/crs/weapons/IF11654.pdf, (Accessed March 12, 2024).

146 Ibid.

147 Colin Demarest and Jen Judson, "What Project Convergence Will Look Like After Bucking Its Yearly Rhythm," C4ISRNet, October 11, 2023, at https://www.c4isrnet.com/battlefield-tech/c2-comms/2023/10/11/what-project-convergence-will-look-like-after-bucking-its-yearly-rhythm, (Accessed March 12, 2024).

148 Colin Demarest, "Project Convergence Shows JADC2 Alignment, Leaders from 3 Services Say," C4ISRNet, October 21, 2022, at https://www.c4isrnet.com/battlefield-tech/it-networks/2022/10/21/project-convergence-shows-jadc2-alignment-leaders-from-3-services-say, (Accessed March 12, 2024).

149 "What is the Army Software Factory?" at https://soldiersolutions.swf.army.mil/about, (Accessed March 12, 2024).

150 "U.S. Army Futures Command Army Software Factory Catalog FY2023" at https://api.army.mil/e2/c/downloads/2023/05/01/0778888d/aswf-catalog-fy-2023.pdf, (Accessed March 12, 2024).

151 "Our Focus Areas" at https://aal.army, (Accessed March 11, 2024).

152 "This is SPARTN" at https://aal.army/spartn, (Accessed March 12, 2024).

153 "Infosheet: This is SPARTN" at https://aal.army/assets/files/pdf/infosheet-spartn.pdf, (Accessed March 12, 2024).

154 "Who We Are" at https://cftste.experience.crmforce.mil/ai2c/s/who-we-are, (Accessed March 11, 2024).

155 "Army's Pittsburgh-based Center Accelerates Development of AI Applications" at https://www.army.mil/article/251079/armys_pittsburgh_based_center_accelerates_develop ment_of_ai_applications, (Accessed March 12, 2024).

156 "ARM – Advanced Robotics for Manufacturing Institute" at https://www.dodmantech.mil/About-Us/Manufacturing-Innovation-Institutes-MIIs/ARM-Institute, (Accessed March 12, 2024).

157 "Campus Design and Facility Development" at https://www.cmu.edu/cdfd/buildings/ric/index.html, (Accessed March 12, 2024).

158 Byron Spice, "Carnegie Mellon AI Collaborates with Pentagon to Improve Helicopter Reliability", Carnegie Mellon University School of Computer Science, February 3, 2021, at https://www.cs.cmu.edu/news/2021/carnegie-mellon-ai-collaborates-pentagon-improve-helicopter-reliability, (Accessed March 12, 2024).

159 US Army Media Services, "04-Understanding the US Army As a Customer", Introduction to U.S. Army Futures Command's AI Integration Center (AI2C), AI2C Research Portfolio & AI2C Project Highlights, Video, at https://mediaservices.cmu.edu/media/04-Understanding+the+US+Army+as+a+customer/1_bs1kmzg, (Accessed March 12, 2024).

160 Akshat Upadhyay, "Do-It-Yourself (DIY) Warfare: A New Warfighting Paradigm", *Strategic Analysis*, March 19, 2024.

161 Akshat Upadhyay, "Do-It-Yourself (DIY) Warfare: A New Warfighting Paradigm", *Strategic Analysis*, March 19, 2024.

162 Brandi Vincent, "Switchblade 600 Kamikaze Drones in the Running for Replicator Mass Production", *Defense Scoop,* February 2, 2024, at https://defensescoop.com/2024/02/02/switchblade-600-kamikaze-drones-replicator-mass-production, (Accessed March 12, 2024).

163 Ibid.

164 Courtney Albon and Noah Robertson, "Pentagon Says $1 Billion Planned for First Two Years of Replicator", *Defense News*, March 12, 2024, at https://www.defensenews.com/pentagon/2024/03/11/pentagon-says-1-billion-planned-for-first-two-years-of-replicator, (Accessed March 12, 2024).

165 Ashley Roque, "Army's $186B Budget Request Shuffles Artillery, Aviation Plans," *Breaking Defense*, March 11, 2024, at https://breakingdefense.com/2024/03/army-budget-request-2025-biden-pentagon-how-much-does-the-army-spend, (Accessed March 12, 2024).

166 Jackson Barnett, "The Army Is Trying to Jump-Start Its Venture Capital Arm", *Fedscoop*, February 11, 2022, at https://fedscoop.com/army-venture-capital-corporation, (Accessed March 13, 2024).

167 "Marque Ventures" at https://www.marque.vc/about, (Accessed March 13, 2024).

168 Heather Somerville, "Investors Are Betting on Defense Startups. The Pentagon Isn't.", *The Wall Street Journal*, January 25, 2024, at https://www.wsj.com/tech/defense-startups-risk-becoming-failed-experiment-without-more-pentagon-dollars-dc9e663a, (Accessed March 13, 2024).

169 "Military Talent Exchange for America" at https://www.shift.org, (Accessed March 13, 2024).

170 Jake Chapman, "American Military-Civil Fusion at Risk with the Loss of the Shift Fellowship", War on the Rocks, March 22, 2024, at https://warontherocks.com/2024/03/american-military-civil-fusion-at-risk-with-the-loss-of-the-shift-fellowship, (Accessed March 25, 2024).

171 Ariel Levite, "How Was Israel Caught Off-Guard?", War on the Rocks, February 22, 2024, (Accessed March 13, 2024).

172 Edward Luttwak and Eitan Shamir, no. 101, pp. 3–14.

173 "U.S. Security Cooperation with Israel" at https://www.state.gov/u-s-security-cooperation-with-israel, (Accessed March 14, 2024).

174 Edward Luttwak and Eitan Shamir, no. 101, pp. 23–8.

175 Ibid., p. 9.

176 Ibid., p. 12.

177 Yonat Rein-Sapir and Eyal Ben-Ari, "The Israel Reserve Law: The Duality of Reservists and Transformed Military Autonomy", *Armed Forces & Society*, 47(4), April 23, 2020.

178 Jordan Chandler Hirsch, "U.S. Soldiers Impressed by Informal IDF", Tablet, November 17, 2009, at https://www.tabletmag.com/sections/news/articles/us-soldiers-impressed-by-informal-idf, (Accessed March 14, 2024).

179 Shyam Sankar and Joab Rosenberg, "The U.S. Can'T Afford to Wait to Fully Embrace the World'S Most Effective Weapon", *The Washington Post*, March 4, 2024, at https://www.washingtonpost.com/opinions/2024/03/04/tech-reservists-israel-us, (Accessed March 14, 2024).

180 Edward Luttwak and Eitan Shamir, no. 101, pp. 3–7.

181 Ibid., pp. 149–52.

182 Ibid., p. 4.

183 Geoffrey Ingersoll, "The Best Tech School On Earth Is Israeli Army Unit 8200", *Business Insider India*, August 14, 2023, at https://www.businessinsider.in/defense/the-best-tech-school-on-earth-is-israeli-army-unit-8200/articleshow/21813110.cms, (Accessed March 14, 2024).

184 Seth Adler, "Inside the Elite Israeli Military Unit 8200", Cyber Security Hub, June 11, 2020, at https://www.cshub.com/threat-defense/articles/inside-the-elite-israeli-military-unit-8200, (Accessed March 14, 2024).

185 Edward Luttwak and Eitan Shamir, no. 101, pp. 215–24.

186 Bruce Rogers, "Former Israeli Intelligence Officers Found Sentra To Provide Cloud Security", *Forbes*, March 1, 2023, at https://www.forbes.com/sites/brucerogers/2023/03/01/former-israeli-intelligence-officers-found-sentra-to-provide-cloud-security/?sh=14ace2bb61fa, (Accessed March 14, 2024).

187 Edward Luttwak and Eitan Shamir, no. 101, p. 65.

188 "Military Research and Development" at https://english.mod.gov.il/About/Innovative_Strength/Pages/Military_Research_and_Development.aspx, (Accessed March 14, 2024).

189 "Unit for Research & Technological Infrastructure" at https://english.mod.gov.il/About/Innovative_Strength/Pages/Unit_for_Research_%26_Technological_Infrastructure.aspx, (Accessed March 14, 2024).

190 "IMDO- Israel Missile Defense Organization" at https://english.mod.gov.il/About/Innovative_Strength/Pages/IMDO_Israel_Missile_Defense_Organization.aspx, (Accessed March 14, 2024).

191 Ibid.

192 "Unmanned Aerial Vehicle (UAV) Administration" at https://english.mod.gov.il/About/Innovative_Strength/Pages/Unmanned_Aerial_Vehicle_Administration.aspx, (Accessed March 14, 2024).

193 "Space and Satellite Administration" at https://english.mod.gov.il/About/Innovative_Strength/Pages/Space_and_Satellite_Administration.aspx, (Accessed March 14, 2024).

194 Jason Gewirtz, *Israel's Edge: The Story of The IDF's Most Elite Unit - Talpiot*, Gefen Publishing, Jerusalem, 2015, pp. 1–10.

195 "Nurturing Future Generations" at https://english.mod.gov.il/About/Innovative_Strength/Pages/Nurturing_Future_Generations.aspx, (Accessed March 14, 2024).

196 "Iron Dome in Action: A Preliminary Evaluation" at https://defense-update.com/20111024_iron-dome-performance-analysis.html, (Accessed March 15, 2024).

197 Edward Luttwak and Eitan Shamir, no. 101, pp. 205–7.

198 Seth J Frantzman, "How Israel's Military is Prioritizing Dual-Use Start-Ups to Accelerate Defense Tech", *Breaking Defense*, July 28, 2023, at https://breakingdefense.com/2023/07/how-israels-military-is-prioritizing-dual-use-start-ups-to-accelerate-defense-tech, (Accessed March 15, 2024).

199 "The Future of Bioconvergence-Design" at https://biodesignisrael.org/bioconvergence-design, (Accessed March 15, 2024).

200 Seth J Frantzman, no. 323.

201 "U.S.-Israel Operations Technology Working Group (OTWG)" at https://www.jewishvirtuallibrary.org/u-s-israel-operations-technology-working-group-otwg, (Accessed March 15, 2024).

202 Bradley Bowman, "The U.S.-Israel Operations-Technology Working Group Gets Busy", Foundation for Defense of Democracies, December 20, 2022, at https://www.fdd.org/analysis/2022/12/20/the-u-s-israel-operations-technology-working-group-gets-busy, (Accessed March 15, 2024).

203 "The IDF Innovation Strategy", International Military Innovation Conference (IMIC) 2022, September 13–5, 2022, at https://military-imic2022.com/wp-content/uploads/2022/09/The-IDF-Innovation-Strategy_CMI_IMIC_September2022-1.pdf, (Accessed March 15, 2024).

204 Ibid.

205 no. 328.

206 Ibid.

207 Ibid.

208 "Vol. 28-30: Military Superiority and the Momentum Multi-Year Plan", Dado Center, October 1, 2020, at https://www.idf.il/en/mini-sites/dado-center/vol-28-30-military-superiority-and-the-momentum-multi-year-plan/vol-28-30-military-superiority-and-the-momentum-multi-year-plan, (Accessed March 15, 2024).

209 Jean-Loup Samaan, "'Decisive Victory' and Israel's Quest for a New Military Strategy", Middle East Policy Council, No 3, 2023.

210 Edward Luttwak and Eitan Shamir, no. 101, pp. 169–70.

211 Eran Ortal, "Going on the Attack: The Theoretical Foundation of the Israel Defense Forces' Momentum Plan", Dado Center, October 1, 2020, at https://www.idf.il/en/mini-sites/dado-center/vol-28-30-military-superiority-and-the-momentum-multi-year-plan/going-on-the-attack-the-theoretical-foundation-of-the-israel-defense-forces-momentum-plan-1, (Accessed March 15, 2024).

212 Ibid.

213 Yaakov Lappin, "Ma'alot (Ascent): The IDF Will Need to Drastically Update Its Multi-Year Program", Begin-Sadat Center for Strategic Studies, November 1, 2023, at https://besacenter.org/maalot-ascent-the-idf-will-need-to-drastically-update-its-multi-year-program, (Accessed March 15, 2024).

214 Seth J Frantzman, "How Israel's Military is Prioritizing Dual-Use Start-Ups to Accelerate Defense Tech", Breaking Defense, July 28, 2023, at https://breakingdefense.com/2023/07/how-israels-military-is-prioritizing-dual-use-start-ups-to-accelerate-defense-tech, (Accessed March 15, 2024).

215 Anthony Capaccio, "US Gives First Iron Dome Interceptors to Israel", Bloomberg, October 12, 2023, at https://www.bloomberg.com/news/articles/2023-10-12/pentagon-owned-stocks-in-israel-transfered-to-defense-forces, (Accessed March 15, 2024).

216 Seth J Frantzman, "Rafael Expects Iron Beam Laser to Be Active in 2025: Exec," Breaking Defense, March 08, 2024, at https://breakingdefense.com/2024/03/rafael-expects-iron-beam-laser-to-be-active-in-2025-exec, (Accessed March 15, 2024).

217 David Hambling, "Israel Rolls Out Legion-X Drone Swarm for the Urban Battlefield", *Forbes*, October 24, 2022, at https://www.forbes.com/sites/davidhambling/2022/10/24/israel-rolls-out-legion-x-drone-swarm-for-the-urban-battlefield/?sh=68a0a9ce4f49, (Accessed March 15, 2024).

218 "About Us" at https://aerorozvidka.ngo, (Accessed March 16, 2024).

219 Oleg Danylov, "The Unique Ukrainian Situational Awareness System Delta Was Presented at the Annual NATO Event", Mezha Media, October 28, 2022, at https://mezha.media/en/2022/10/28/the-unique-ukrainian-situational-awareness-system-delta-was-presented-at-the-annual-nato-event, (Accessed March 16, 2024).

220 "NATO's Support of Ukraine's C4 Capabilities" at https://www.afcea.org/signal-media/defense-operations/natos-support-ukraines-c4-capabilities, (Accessed March 16, 2024).

221 "NATO'S Practical Support to Ukraine", NATO Fact Sheet, February 2015, at https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_02/20150203_1502-Factsheet_PracticalSupport.pdf, (Accessed March 16, 2024).

222 " 'Aerorozvidka' NGO Annual Report", at https://aerorozvidka.ngo/wp-content/uploads/2024/03/ZVIT_Aerorozvidka_EN_2023.pdf, (Accessed March 16, 2024).

223 "TIDE Sprint 2024: Advancing Interoperability", at https://www.act.nato.int/article/tide-sprint-2024-advancing-interoperability/#:~:text=TIDE%20Sprint%20forms%20part%20of,communicate%2C%20cooperate%2C%20and%20collaborate, (Accessed March 16, 2024).

224 "Coalition Warrior Interoperability Exercise", at https://www.act.nato.int/our-work/exercises/coalition-warrior-interoperability-exercise, (Accessed March 16, 2024).

225 "Multinational Interoperability for C2IS" at https://systematic.com/en-gb/industries/defence/products/domains/interoperability/mip, (Accessed March 16, 2024).

226 Liza Brovko, "Ukraine Joined the FMN – Will Increase Interoperability with NATO Countries", Babel News, February 26, 2024, at https://babel.ua/en/news/104316-ukraine-joined-the-fmn-will-increase-interoperability-with-nato-countries, (Accessed March 16, 2024).

227 No. 347.

228 Katerina Sergatskova, “What Wedding Drones over Ukraine Can Tell Us about the War”, Focus Ukraine, Blog of Kennan Institute, October 2, 2023, at https://ukraine.wilsoncenter.org/blog-post/what-wedding-drones-over-ukraine-can-tell-us-about-war, (Accessed March 16, 2024).

229 347. No.

230 Ibid.

231 “Situational Centers” at https://aerorozvidka.ngo/situational-centers, (Accessed March 16, 2024).

232 “Trainings” at https://aerorozvidka.ngo/course, (Accessed March 16, 2024).

233 “Situational Awareness Is the Key to Our Victory” at https://aerorozvidka.ngo/situational-awareness, (Accessed March 16, 2024).

234 “The Year of Unbreakability: Aerorozvidka Chronicles” at https://aerorozvidka.ngo/the-year-of-unbreakability, (Accessed March 16, 2024).

235 “Ministry of Digital Transformation Calls to Use the eVorog Through the Diia App” at https://www.kmu.gov.ua/en/news/mincifri-zaklikaye-koristuvatisya-yevorogom-cherez-zastosunok-diya, (Accessed March 16, 2024).

236 No. 358.

237 Orysia Hrudka, “Meet the R18, Ukraine’s Formidable Night Strike Drone Transforming the Battlefield”, Euromaidan Press, May 24, 2023, at https://euromaidanpress.com/2023/05/24/meet-the-r18-ukraines-formidable-night-strike-drone-transforming-the-battlefield, (Accessed March 16, 2024).

238 “Cyber Resilience Is a New Challenge of Network-Centric Warfare”, at https://aerorozvidka.ngo/cyber-resilience, (Accessed March 16, 2024).

239 No. 357.

240 No. 347.

241 Hanna Arhirova, “Ukraine Launches ‘BRAVE12 Tech Cluster to Boost Military Capability”, C4ISRNet, April 26, 2023, at https://www.c4isrnet.com/unmanned/2023/04/26/ukraine-launches-brave1-tech-cluster-to-boost-military-capability, (Accessed March 17, 2024).

242 “Defense Mapping Software” at https://armysos.com.ua/defense-mapping-software, (Accessed March 17, 2024).

243 Mykhalo Lopatin, “Bind Ukraine’s Military-Technology Revolution to Rapid Capability Development”, War on the Rocks, January 23, 2024, at https://warontherocks.com/2024/01/bind-ukraines-military-technology-revolution-to-rapid-capability-development, (Accessed March 17, 2024).

244 David Zikusoka, “How Ukraine’s “Uber for Artillery” is Leading the Software War Against Russia”, New America, Blog Post, March 17, 2024 at https://www.newamerica.org/future-frontlines/blogs/how-ukraines-uber-for-artillery-is-leading-the-software-war-against-russia/, (Accessed March 18, 2024).

245 “Defense Mapping Software” at https://armysos.com.ua/defense-mapping-software, (Accessed March 17, 2024).

246 “Help Army” at https://prytulafoundation.org/en/help-army, (Accessed March 17, 2024).

247 “These Are the Drones You’re Looking for: Join Mark Hamill and the Army of Drones” at https://u24.gov.ua/dronation, (Accessed March 17, 2024).

248 “Frequently Asked Questions” at https://u24.gov.ua/about, (Accessed March 17, 2024).

249 “About United24” at https://u24.gov.ua/about, (Accessed March 17, 2024).

250 No. 372.

251 Ibid.

252 "NAFO Drone Part III: Operation Sea Baby" at https://u24.gov.ua/nafodrone_seababy, (Accessed March 17, 2024).

253 "Safe Skies" at https://u24.gov.ua/safeskies, (Accessed March 17, 2024).

254 "About the Accelerator" at https://mil-tech.gov.ua/en/about-accelerator, (Accessed March 18, 2024).

255 Vera Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab", *Time Magazine*, February 8, 2024, at https://time.com/6691662/ai-ukraine-war-palantir, (Accessed March 18, 2024).

256 No. 379.

257 Ibid.

258 "Implementing Solutions for the Victory" at https://mil-tech.gov.ua/en, (Accessed March 18, 2024).

259 Ibid.

260 "NATO Codification System (NCS)" at https://www.dla.mil/Working-With-DLA/Federal-and-International-Cataloging/NATO, (Accessed March 18, 2024).

261 No. 379.

262 No. 366.

263 "Ukrainian Defense Innovations" at https://brave1.gov.ua/en, (Accessed March 18, 2024).

264 Ibid.

265 Interfax-Ukraine News Agency, "BRAVE1 Defense Cluster Registers More Than 820 Developments in Seven Months – Minister Fedorov", Interfax-Ukraine News Agency, December 13, 2023, at https://en.interfax.com.ua/news/economic/953853.html, (Accessed March 18, 2024).

266 Mariia Denysiuk, "Ukraine's BRAVE1 Allocates $3M for Defense Innovation", AIN Tech, March 4, 2024, at https://ain.capital/2024/03/04/brave1-allocates-3m-for-defense-innovation, (Accessed March 18, 2024).

267 No. 388.

268 No. 391.

269 Elisabeth Gosselin-Malo, "How Ukraine's Defense Companies Have Adapted to Two Years of War", Defense News, February 22, 2024, at https://www.defensenews.com/global/europe/2024/02/22/how-ukraines-defense-companies-have-adapted-to-two-years-or-war, (Accessed March 18, 2024).

270 No. 391.

271 "European Innovation Council: Launch of the First Call to Support the Ukrainian Start-Up Community" at https://eic.ec.europa.eu/news/european-innovation-council-launch-first-call-support-ukrainian-start-community-2023-12-20_en, (Accessed March 18, 2024).

272 "Commission Announces Partners in European Innovation Council Action to Support the Ukrainian Deep Tech Community" at https://eic.ec.europa.eu/news/commission-announces-partners-european-innovation-council-action-support-ukrainian-deep-tech-2023-05-10_en, (Accessed March 18, 2024).

273 Dan Sabbagh, "Ukraine Says It Could Make 2m Drones a Year with Financial Help from West", *The Guardian*, March 20, 2024, at https://www.theguardian.com/world/2024/mar/20/ukraine-says-it-could-make-2m-drones-a-year-with-financial-help-from-west#:~:text=The%20minister% 20said%20 there%20were,drones%20are%20manufactured%20in%20 Ukraine%E2%80%9D, (Accessed March 29, 2024).

274 Kyiv Post, "Ukraine Poised to Produce 2 Million Drones in 2024", Kyiv Post, March 6, 2024, at https://www.kyivpost.com/post/29064#:~:text=The%20drone%20sector%20 in%20 Ukraine,currently%20available%20for%20its%20support, (Accessed March 18,

2024).

275 David Ingram, "Ukraine Creates a Branch of Its Armed Forces Specific to Drone Warfare", *NBC News*, February 7, 2024, at https://www.nbcnews.com/news/world/ukraine-creates-branch-armed-forces-specific-drone-warfare-rcna137634, (Accessed March 18, 2024).

276 Mykhalo Lopatin, "Bind Ukraine's Military-Technology Revolution to Rapid Capability Development", War on the Rocks, January 23, 2024, at https://warontherocks.com/2024/01/bind-ukraines-military-technology-revolution-to-rapid-capability-development, (Accessed March 17, 2024).

277 Bryan Clark and Dan Patt, "Unalone and Unafraid: A Plan for Integrating Uncrewed and Other Emerging Technologies into US Military Force", Hudson Institute Report, Hudson Institute, August 2023.

278 "Office of the Principal Scientific Advisor to the Government of India" at https://www.psa.gov.in, (Accessed March 20, 2024).

279 "The Prime Minister's Science, Technology and Innovation Advisory Council (PM-STIAC)" at https://www.psa.gov.in/pm-stiac, (Accessed March 20, 2024).

280 India Today, "Narendra Modi's First Independence Day Speech: Full Text", *India Today*, September 17, 2016, https://www.indiatoday.in/india/story/narendra-modi-independence-day-speech-full-text-red-fort-204216-2014-08-1,. (Accessed March 20, 2024).

281 Author Interview.

282 "Skill India Digital Hub" at https://www.skillindiadigital.gov.in/home, (Accessed March 18, 2024).

283 "About Us" at https://nsdcindia.org/about-us, (Accessed March 18, 2024).

284 "Startup India Seed Fund Scheme" at https://seedfund.startupindia.gov.in, (Accessed March 18, 2024).

285 Ibid.

286 "Portfolio of Incubators Approved Under the Startup India Seed Fund Scheme" at https://seedfund.startupindia.gov.in/portfolio, (Accessed March 18, 2024).

287 "#startupindia" at https://www.investindia.gov.in/startup-india-hub, (Accessed March 18, 2024).

288 "Accelerating Growth of New India's Innovations" at https://www.investindia.gov.in/agnii, (Accessed March 20, 2024).

289 "About AIM" at https://aim.gov.in, (Accessed March 20, 2024).

290 Ibid.

291 Ibid.

292 "About AIM" at https://aim.gov.in, (Accessed March 20, 2024).

293 "Draft National Deep Tech Startup Policy (NDTSP) 2023" at https://psa.gov.in/CMS/web/sites/default/files/process/NDTSP.pdf, (Accessed March 20, 2024).

294 Ibid.

295 Ibid.

296 Ibid.

297 No. 418.

298 Ibid.

299 Ibid.

300 Ibid.

301 Ibid.

302 "About DRDO" at https://www.drdo.gov.in/drdo/about-drdo#:~:text=DRDO%20was%20formed %20in%20 1958,Defence%20Science%20Organisation%20(DSO), (Accessed March 21, 2024).

303 Laxman Kumar Behera, “Examining India’s Defence Innovation Performance”, *Journal of Strategic Studies*, 44(6), December 14, 2021, pp. 830–53.

304 “Dr Samir V Kamat” at https://www.drdo.gov.in/drdo/dr-samir-v-kamat#:~:text=Samir%20V%20Kamat%20has%20taken,DRDO)%20on%2026th%20Aug%202022, (Accessed March 22, 2024).

305 “Technology Cluster” at https://www.drdo.gov.in/drdo/technical-clusters, (Accessed March 22, 2024).

306 No 427.

307 A Review of the Working of the Defence Research and Development Organisation (DRDO), Forty-Second Report, Lok Sabha Secretariat, Standing Committee on Science (2023-24), December 2023, at https://sansad.in/getFile/lsscommittee/Defence/17_Defence_42.pdf?source=loksabhadocs (Accessed March 18, 2024).

308 Sandeep Unnithan, “The ATV Project Was Atmanirbhar Since Its Inception: Vice Admiral PC Bhasin (Retd) | India Today Insight”, *India Today*, August 24, 2020.

309 “ADA” at https://www.ada.gov.in, (Accessed March 24, 2024).

310 “BrahMos” at https://www.drdo.gov.in/drdo/brahmos-0, (Accessed March 23, 2024).

311 No. 428.

312 “Report of the Group of Ministers on National Security” at https://www.vifindia.org/sites/default/files/GoM%20Report%20on%20National%20Security.pdf, (Accessed March 24, 2024).

313 Ibid.

314 Ibid.

315 Ibid.

316 Ibid.

317 Team LHI, “India’s Software Revolution: Rooted in Y2K”, Peepul Tree Stories, August 14, 2022, at https://www.peepultree.world/livehistoryindia/story/eras/india-software-revolution-rooted-in-y2k, (Accessed March 24, 2024).

318 No. 437.

319 Ibid.

320 Ibid.

321 Ibid.

322 Ibid.

323 Ibid.

324 Author Interview with Ex ADG ADB.

325 “WHAT IS iDEX?” at https://idex.gov.in, (Accessed March 24, 2024).

326 Ibid.

327 “Partners” at https://idex.gov.in/partners, (Accessed March 24, 2024).

328 “Written Answers to Starred Questions” at https://rsdebate.nic.in/bitstream/123456789/708917/1/IQ_251_10022020_S86_p21_p22.pdf, (Accessed March 24, 2024).

329 No. 452.

330 Ibid.

331 “Defence Acceleration Internship” at https://idex.gov.in/sites/default/files/2021-05/i4D-Guidelines%20-%202021.pdf, (Accessed March 24, 2024).

332 Vish Sahasranaman, “Guidelines: iDEX Technology & Product Management”, iDEX, at https://idex.gov.in/sites/default/files/2020-11/PMA_Guidelines_IDEX.pdf, (Accessed March 24, 2024).

333 Ibid.

334 Ibid.

335 Ibid.

336 Author Interview with ex DIO Member.

337 “Defence India Startup Challenges” at https://idex.gov.in/challenge-categories, (Accessed March 25, 2024).

338 “iDEX PRIME” at https://idex.gov.in/disc-category/24, (Accessed March 25, 2024).

339 “ADITI #1” at https://idex.gov.in/disc-category/41, (Accessed March 25, 2024).

340 “Open Challenge” at https://idex.gov.in/disc-category/5, (Accessed March 25, 2024).

341 Author Interview with Ex DIO Member.

342 Vish Sahasranaman, “Guidelines: iDEX Technology & Product Management,” iDEX. https://idex.gov.in/sites/default/files/2020-11/PMA_Guidelines_IDEX.pdf.

343 Author Interview.

344 “Introduction to Army Design Bureau” at https://indianarmy.nic.in/content2/adb/introduction-adb, (Accessed March 25, 2024).

345 “Make in India” at https://indianarmy.nic.in/content2/adb/make-in-india-adb, (Accessed March 25, 2024).

346 “Delegation of Financial Powers to Defence Services - 2021”, Government of India, Ministry of Defence, p.22.

347 Ibid.

348 Ibid.

349 Author Interview.

350 No. 471.

351 “Compendium of Problem Definition Systems 2023: Indigenise to Modernise” at https://indianarmy.nic.in/writereaddata/adb-documents/Compendium%20of%20Problem%20Definition%20Statement%202023.pdf, (Accessed March 25, 2024).

352 “The Scheme” at https://tdf.drdo.gov.in/scheme, (Accessed March 25, 2024).

353 “TDF Technical Consultative Workshop for Cycle 3 Projects” at https://www.gita.org.in/ActivityDetails.aspx?GITA=MPABgB8IwekTs+/OvIMVICK8qO7VzKsSu21gw4sRnk8=, (Accessed March 25, 2024).

354 No. 477.

355 Ibid.

356 “Dare to Dream” at https://tdf.drdo.gov.in, (Accessed March 25, 2024).

357 Author Interview.

358 “Defence Procurement Procedure 2016: Capital Procurement”, Government of India, Ministry of Defence, at https://mod.gov.in/sites/default/files/dppm.pdf_0.pdf#:~:text=Hence%20the%20Ministry%20of%20 Defence%20(MoD)%20is,%E2%80%9E Make%20in%20India%E2%80%9F%20in%20the%20defence%20sector, (Accessed March 25, 2024).

359 No. 470.

360 No. 471.

Chapter Three

Observations from Recent Conflicts

In Chapter 3, we embark on an analytical journey through the lenses of recent conflicts, delineating the intersection of emerging technologies with modern warfare's evolving dynamics. Our focus pivots to the Armenia–Azerbaijan War, the ongoing Russia–Ukraine Conflict, and the Israel–Hamas Conflict, each selected for their distinct technological and strategic profiles that underscore the multifaceted impact of technological advancements on the battlefield. These case studies have been meticulously chosen to bridge the theoretical discussions of Chapter 1 – centring around the philosophies of leading tech thinkers, entrepreneurs and scholars – with the practical manifestations observed in the innovation ecosystems of the United States, Ukraine and Israel discussed in Chapter 2. This approach allows us to distil critical tenets of the Adaptive Integrative Framework for Technology Absorption in the Armed Forces (AIF-TAF), setting the stage for a deeper exploration of how nations can leverage emerging technologies to forge a new paradigm in military strategy and operational art.

One needs to distinguish between observations and lessons when learning from a war in the third person. A second-hand perspective, though offering one of the most important advantages of not participating directly in a conflict, hampers the learning process of a non-participating military or security apparatus. Observing incidents, tactics, procedures and use of technologies and platforms from far away induces a mistaken sense of relevance of every technology and every tactic used in every battle. Without filtering for political context, geography, economy, leadership, training or other factors, absorbing vicarious observations may lead to an erroneous appreciation of own strength and weakness. For this the lessons learnt part is generally considered to be sequential and based on a nine-step process grouped broadly into observation, analysis and generation.

The first is observation. This has three steps: Open-source intelligence (OSINT) data collection, leveraging strategic partnerships and study of technology and weapons platforms. One resorts to use of OSINT tools to observe the peculiarities of battles, including force structures, types of platforms, arms and ammunition being used, losses and wins on the battleground and similar attributes. This is supplemented by news reports and academic publications. Next is a relatively confidential process of intelligence sharing between partners and allies to get a nuanced perspective on the conflict. The final component of observation is the study of weapons and technology to gain insights into the use of tactics, innovative techniques and technology exploitation by adversaries. The second phase is the process of contextualisation. This is an analytical phase, which again has three steps: simulation and wargaming, consultations with subject matter experts (SMEs) and diplomatic/political analysis. Simulation and wargaming allows non-participating countries to contextualise the studied and observed data, analyse it with respect to own doctrines and concepts and finally forecast potential applications for their forces and war-fighting strategies. After simulation, the results are discussed with academics and experts who provide a nuanced perspective on the conflict as well as suggest improvements and modifications for own forces. Finally, political and diplomatic analysis will frame the conflict in a broader geopolitical lens, enabling the study of how military and politics impact each other. Then comes the final stage, which is that of generation. This has three components: review of doctrine and training pedagogies, exercises both with own troops as well as joint ones and finally, feedback and iterating cycles. Based on stage two analysis and consideration of own contextual factors, decisions are made to modify tactics, techniques and procedures (TTPs) of the organisation, along with necessary modifications in procurement channels.

Obviously, this is not the only process through which military priorities are set, a grouping of the various wars and conflicts being fought in contemporary times also provides a snapshot of the technological milieu. However, witnessing certain aspects of contemporary wars, especially use of commercial technologies is critical from the perspective of this book. The succeeding sections will attempt to encapsulate important observations from three different conflicts, some ongoing and some recently concluded. The ongoing ones include the conflict between Russia–Ukraine and Israel–Hamas while the one between Armenia and Azerbaijan has just concluded, though with a significant chance of being reignited in the near future. These observations will be ahistorical and will not describe the chronology of the wider conflict but will only focus on military innovations and the use of emerging and disruptive technologies on the battlefield.

Armenia–Azerbaijan War

The conflict between the two countries was over the disputed region of Nagorno–Karabakh and lasted for 44 days between September 27, 2020 and November 10, 2020. It came to a close through a Russia-brokered ceasefire and resulted in Armenia ceding control over vast swathes of land to Azerbaijan.[1] The conflict witnessed an overwhelming use of drones, missiles, rocket artillery and automated C2 systems. The conflict also featured multiple countries siding up with the two antagonists with strange bedfellows. Israel and Turkey grouped up with Azerbaijan while Russia supported Armenia.[2] This section will focus on the use of two important technologies by both sides – drones and sensors.

Drones

The one platform or technology that defines this war is the drone. Drones were at the centre of a web of localised meshes used by Azerbaijan where the ISTAR and kinetic capabilities of drones were integrated with legacy platforms such as rockets, artillery batteries and long-range precision fires. Manned-unmanned teaming (MUM-T), in the form of special forces teams functioning in the depths of Nagorno–Karabakh and using laser designators for target acquisition, followed by strikes by UAVs, is also a practice that was first witnessed during this conflict.[3] Aerial drones and loitering munitions (LMs) were used extensively by both sides, though media reports were skewed in the favour of the Azeris. In terms of the types of unmanned aerial vehicles (UAVs) used, Armenia used mostly indigenously designed and developed ones at the beginning of the conflict and transitioned to using Russian platforms such as

Orlan 10s later. The major UAVs used by Armenia were X-55/ Kh-55 (recce), HRESH (LM), Krunk (recce) and the Russian Orlan 10 (recce).[4] On the other hand, Azerbaijan invested heavily in procuring foreign, especially Turkish UAVs and Israeli LMs, and copied heavily from the Turkish concept of operations (CONOPS) regarding use of robotic systems in war fighting.

The Turkish forces, as part of their Operation Spring Shield, used a combination of massed rocket artillery strikes in conjunction with ISTAR roles of drones against the Syrian Arab Army in early 2020. This CONOPS was meant to compensate for the lack of major Turkish manoeuvre elements and manned aircraft in the area. A similar concept was followed by the Azeris with the added actions of searching and taking out Armenian mobile surface-to-air missile (SAM) batteries. This allowed the Azeri UAVs comparative command of the control of air space in the battlefield.[5] Targeting assembly areas, command posts, logistics and manoeuvre elements of the Armenian forces, the Azerbaijan military used a combination of UAVs and artillery strikes to decimate the forces moving up to contact their own forces. Next, rocket artillery salvos were connected to drone feeds for ISTAR roles, converting regular conventional area salvos into precision strikes. This was done in addition to using Turkish Bayraktar TB-2s and Israeli LMs for targeted strikes against armoured platforms and personnel. TB-2, in fact, acted as an intelligence, surveillance and reconnaissance (ISR) platform for other UAVs and LMs too.[6] For example, TB-2 UAVs identified Armenian forces in a designated strike zone, where LMs circled autonomously to verify and then attack the identified targets in a kamikaze style attack.[7]

The TB-2s were equipped with indigenous MAM micro-guided munitions for targeted strikes as well as high-definition (HD) cameras for taking videos that could be later used for propaganda and information warfare (IW).[8] The major UAVs used by Azeris include TB-2 Bayraktar (strike and ISR), Anka-S (strike), Hermes 900 (MALE ISR), Heron (MALE ISR), Aerostar (ISR), Searcher (ISR) and Orbiter 1K, Orbiter-3, SkyStriker and Harop LMs.[9] Azerbaijan used its special operations forces, also called 'saboteur groups', mirroring US Special Forces operating against the Taliban post 9/ 11, by sending them into depth areas and using laser markers to 'light up' multiple weapons systems and fortifications to be targeted by UAVs. Repurposed An-2 biplanes were dressed up in camouflage and flown at low altitudes to act as decoys. When fired upon by Armenian AD systems, these systems were then targeted by UAVs flying at more than the interception altitude. Overhead observation through persistent presence of UAVs allowed Azeri military commanders to target Armenian military formations down to the level of platoons and sections. This was achieved in a terrain that was mountainous and therefore, presumed to offer a defensive advantage to the Armenian forces. However, the UAVs acted as the great leveller by targeting dismounted troops, air defence (AD) positions and vehicle convoys[10] using an 'eye in the sky' God-view mode.

One of the most obvious observations in this conflict especially with respect to drone operations is the mismatch between drone capabilities and existing legacy AD systems. While the Armenians mostly used Soviet and early Russian era AD systems, such as the 2K11 Krug, 9K33 Osa, 2K12 Kub and 9K35 Strela-10s, drones such as TB-2s flew much higher than their interception altitudes. Also, most AD systems, even till today, are not equipped to detect drones and UAVs.[11] Furthermore, Russian-supplied Polye 21 EW systems adversely affected the operation of Azeri drones, but these were corrected in a matter of days. In totality, the Armenians lacked the modern senses that make up technological superiority on the battlefield, that is, sensors, electronic warfare (EW) and counter unmanned aerial systems (C-UAS) systems. The later deployment of Buk and Tor mobile AD systems did lead to the downing of Azeri drones but these were deployed by the Armenians at a stage when the course of the conflict had already been decided in Azerbaijan's favour.[12] The use of hi-tech drones in this fashion by Azerbaijan forces and their vulnerabilities were observed very closely by both the Russians and Ukrainians who would turn the entire paradigm of drones not being able to change the outcome of a war on its head. The Ukrainians would pioneer the use of drones literally as cannon fodder, in the millions, to achieve tactical parity and superiority against a technologically advanced adversary.

Sensors

The Armenia–Azerbaijan conflict witnessed a proliferation of sensors across the length and breadth of the battlefield, especially in their use by the Azeri forces. Electro-optical sensors on drones were supplemented by infrared (IR) and HD TV ones supporting full motion videos (FMV), which were used for a number of purposes including IW, post-strike damage assessment (PSDA) and enabling LMs to identify and home on to individuals in a top-attack mode.[13] The Armenians suffered close to 250 tanks destroyed on their side. Most casualties of these tanks occurred without any contact battle.[14] One of the biggest reasons behind this is the use of thermal/IR and HD TV sensors and linking them with the strike capabilities of UAVs, which then destroyed these tanks before giving they could move out. This is the first modern war where sensors and shooters were amalgamated into a single platform.

Russia–Ukraine Conflict

The ongoing Russia–Ukraine conflict, now having crossed more than two years since the beginning of Russia's special military operation on February 24, 2022, has generated reams of literature on the use of disruptive technologies on the battlefield. The section will focus on the use of UAVs in the conflict.

Use of UAVs by Russia

UAVs have been extensively employed by Russia for real-time intelligence fusion, swift target identification and the destruction of Ukrainian military and civilian targets.[15] They play crucial roles in artillery spotting, vertical reconnaissance at the platoon level and gathering intelligence, including targeting Ukrainian electricity grid infrastructure such as sub-stations. Additionally, UAVs are utilised for dogfighting drones within counter-drone systems, enhancing missile system accuracy and reducing the sensor-to-shooter time window for mobile targets.[16] Moreover, they function as LMs, contribute to the suppression/destruction of enemy air defences (SEAD/DEAD) and, most importantly, compel Ukraine to exhaust valuable AD ammunition.[17] Furthermore, UAVs serve as vital components of a unified information space, providing detailed battlefield understanding distributed across relevant units. As an example, Russian military tactics integrate UAVs with artillery systems, missiles and tanks, extending the latter's range using indirect observation and creating a pseudo-beyond visual range mode reaching up to 12 km.[18] Russia's utilisation of UAVs has remained conventional to a large extent, serving as integral components within existing command and control (C2) structures.

While innovations have emerged, particularly in replacing human operators in tactical roles, the fundamental roles themselves have remained fixed. Notably, UAVs have replaced human operators in listening and observation posts (LPs and OPs), positioned ahead of the Russian defensive line. Specifically, UAV models such as the Orlan-10 and Orlan-30, boasting maximum ranges of 120–300 km respectively, have been instrumental in target designation for Krasnopol 152 mm laser-guided rounds.[19] While the original range of Krasnopol ammunition stands at 20 km, extendable up to 43 km, the limited range of initial laser designators necessitated alternative solutions.[20] These UAVs, equipped with off-the-shelf Canon cameras, including the OS 750 D version and laser designators, extend the reach of Russian artillery beyond conventional limits.[21] Within Russia's Armed Forces, UAVs are strategically organised into brigades, with all UAVs within a brigade consolidated into a single company. This company is subsequently segmented into platoons based on the UAVs' size and range capabilities. For instance, the mini platoon oversees operations of hand-launched Granat-1 UAVs, while the short-range platoon manages Orlan-10 and Granat-4 UAVs. Notably, training for UAV operations is conducted at the Inter Branch Center for Training of Specialists for Ground Troops in Kolomna, where exclusively contract non-commissioned officers (NCOs) are tasked with UAV operation, while conscripts undertake auxiliary duties. Additionally, officers across all three Services are undergoing UAV training at the Russian Air Force Academy, with artillery officers given preference.[22] The utilisation of Iranian-made Shahed-131 and Shahed-136 drones, categorised as LMs, was observed in tandem with cruise and ballistic missile strikes, aimed at Ukrainian civilian areas to coerce Kiev into capitulation.[23] Operating alongside these are Mohajer-6 drones, tasked with SEAD/DEAD operations, facilitating the Shahed series' deeper penetration to target Ukrainian assets.[24]

Despite ongoing efforts by volunteer groups within Russia to develop high-speed drones with first person view (FPV) capabilities using imported components, the Russian military faces a shortage of domestically manufactured Unmanned Combat Aerial Vehicles (UCAVs). Moreover, the integration of commercial quadcopters and drones into the Russian military's C2 structure has been a slow and challenging process, leading to significant operational gaps and casualties. Frontline soldiers have voiced demands for increased quadcopter deployment, highlighting the domestic industry's inability to rapidly scale UAV production down to the company and platoon levels.[25] While some praise has been directed towards junior- and mid-level Russian officers for their understanding and utilisation of these emerging platforms, criticisms persist regarding senior leadership's competence in appreciating their operational utility.

Use of UAVs by Ukraine

Ukraine's adoption of UAVs marks a significant tactical innovation within its armed forces. Ukraine has swiftly integrated UAVs into its military operations, leveraging private volunteers and niche technologies to compensate for limited defence budgets and delayed conventional military aid from the West. A notable achievement of the Ukrainian Armed Forces lies in effectively weaponizing the air littoral – the airspace between the infantry and fighter planes – where the bulk of engagements occur and UAV innovation flourishes. Facing initial budget constraints and delayed military aid, Ukrainian officers and soldiers, particularly the younger ones, quickly adapted to niche technologies, often driven by private militias, civilian volunteers and mid- to junior-level officers. However, senior leadership, akin to Russian counterparts, struggles to fully grasp the potential of emerging technologies. Complementing the military efforts, the Ukrainian government aims to position Ukraine as a digital powerhouse post-war and employs social media platforms for influence operations, garnering sympathy, maintaining Western support,[26] and countering Russian propaganda.[27] Notably, Ukraine's focus on unmanned systems, including UAVs and Unmanned Surface Vehicles (USVs), has yielded significant rewards.

Entrepreneurship and grassroots military innovation have led to the development of compatible payloads and modular systems capable of multifaceted roles, leveraging international standards in software and hardware integration. Since 2014, Ukraine has harnessed crowdfunding platforms such as the People's Project to raise funds for procuring commercial drones, initially utilised for ISR purposes.[28] Over time, these drones have evolved to conduct tactical harassment attacks, targeting individual Russian gun positions, infantry sections, tanks and mechanised vehicles. Many of these drones have been adapted to carry strap-on grenades and anti-personnel mines, serving as crude variants of LMs. A surge of companies emerged in late 2014, such as Ukrspecsystems, Athlone Air and Kiev Polytechnic, producing privately funded and designed drones supplied directly to soldiers or militias. Some drones are exclusively piloted by civilian volunteers, blurring the lines of combatant categorisation under International Humanitarian Law (IHL).

In July 2016, the US supplied limited quantities of RQ-11 Raven drones to Ukraine, but their effectiveness was quickly countered by Russian EW capabilities.[29] Domestic efforts by Ukrainian defence conglomerates, such as UkrOboronProm's AN-BK-1 unmanned aerial 'complex'[30] and Luch's Sokil-300 long-range UAV, have faced production challenges. To address gaps in drone capabilities, Ukraine initiated an 'Army of Drones' program, aiming to produce approximately 200,000 drones by 2023, led by Minister for Digital Transformation Mykhailo Federov.[31] The initiative fostered studies, competitions and expedited frontline drone delivery. Ukraine's drone ecosystem includes multiple startups, emerging in a rapid time frame. Notable attacks inside Russia, including strikes on Engels air base, Moscow, and an oil refinery in Krasnodar, utilised drones such as UJ-22, Tu-141 and 'Beaver'.[32] Despite high-profile successes, estimating the total number of attacks and their impact remains challenging due to conflicting reports and limited quantifiable data on casualties. The tactical use of drones in Ukraine includes several innovations, including civilian reliance on 3D printing for drone parts and makeshift drone assembly using foam plastic and Chinese spare parts.[33] The rapid expenditure of drones, viewed as 'flying ammunition', underscores their expendability. While initially Turkish-supplied Bayraktar TB-2s targeted Russian convoys, their susceptibility to Russian EW and SAM systems led to their phased-out use, primarily serving as propaganda tools.[34] The deployment of longer-range drones with potent weapon systems remains a challenge, despite ongoing projects such as the BRAVE1 technology cluster, integrating military, defence sector and private startups.

For the Ukrainians, challenges persist in integrating UAVs into the Ukrainian military structure, with a focus on augmenting artillery targeting and supporting special operations forces (SOFs), volunteer reconnaissance battalions and militias in resistance efforts. These include UAV use in tank-hunting, ISR and as improvised LMs targeting Russian bunkers. While social media platforms showcase Ukrainian military successes, the prolonged stalemate at Bakhmut underscores the complexity of the conflict,[35] highlighting both Ukrainian resilience and strategic challenges. Another persistent issue is the scaling up of technologies at the rapidity and mass required for the frontline.

Use of AI Systems on Both Sides

The implications of the use of AI systems in the Russia–Ukraine conflict are being studied in great depth due to the nature of the technology. On both sides, the technology has assisted military commanders, both on ground and in C2 centres, to speed up decision making, make sense of a plethora of disparate data from multiple sensors and conduct IW against each other. On the Ukrainian side, most of the technology has been given by Western tech companies such as Palantir and Clearview. Uses include integration of target and object recognition with satellite imagery by startups and companies such as Planet Labs, Maxar and BlackSky Technology. Among other applications, AI is being used for geolocating and analysing open-source data such as social media content for identification of Russian soldiers, weapons, systems, units or their movements; combining ground-level photos, video footage from numerous drones and UAVs and satellite imagery to provide faster intelligence analysis; understanding troop movements; and conducting battlefield damage assessments. Facial recognition and AI neural networks are being used to identify Russian soldiers, create an inventory and use the same for conducting IW. Primer, a US company, has used AI systems, especially natural language processing (NLP), to understand the specific ways Russian soldiers use to communicate, while Microsoft has been especially helpful in assisting Ukrainian cyber defence teams in using AI for enhanced threat intelligence against Russian cyberattacks. There have also been reports of the Ukrainian forces using fully autonomous UAVs, fitted with onboard AI, targeting Russian troops on ground.[36]

On the other hand, Russia is using AI for data analysis and enhancing the decision-making capacity of the Russian soldier. One of the more unique aspects of the Russian use of AI is its integration with robotics. Unmanned ground vehicles (UGVs) such as the Marker and UAVs are being field tested and deployed in combat zones in heavily mined and urban areas, while at the same time attempting to replace soldiers in more dangerous areas. The Russian Lancet-3 LM has reportedly been augmented with convolutional neural nets (CNN) for collecting, classifying and analysing imagery and video content collected by the LM in flight. AI is also being employed by Russia in IW though public proof of the same remains scant.[37]

Israel–Hamas Conflict

The use of emerging technologies in Israel's ongoing war with Hamas has been constantly in news due to the Israeli Defence Forces' (IDF's) use of AI-based targeting programs called 'The Gospel' (Habsora in Hebrew) and 'Lavender' to seek, identify and destroy targets in the Gaza Strip.[38] Some commentators have called this current conflict the 'first AI war' where the use of AI and ML algorithms to continuously keep generating targets has been compared to the workings of a factory.[39] The AI program generates targeting recommendations based on intelligence inputs and a list of close to 40,000 suspected militants whose names and details such as locations of homes etc are searched and matched dynamically with continuously updated intelligence and information to generate matches, which are then sent to the air force or artillery batteries for immediate destruction. Habsora was also activated and used in IDF's 11-day war against Hamas in May 2021, where it developed the capability to generate up to a 100-targets a day in the Gaza Strip.[40] Compared to IDF's capability of producing a maximum of 50 targets in a year, this capability represents an exponential leap. The data sets used include 'drone footage, intercepted communications, surveillance data and information drawn from monitoring the movements and behaviour patterns of individuals and large groups'.[41] However, there have been criticisms about the way over reliance on AI leads to automation bias where even having a human in the loop does not lead to a qualitative advantage, since the human only presses a button when prompted by the AI.

Ironically, one of the reasons why this war has generated a lot of brickbats for the IDF despite their technological superiority is their over-reliance on technology, at times, negating the human factor. One of the most visible artefacts of this failure is the 'smart wall', which stretched along the 64-kilometre stretch of the Gaza Strip, reportedly built at a cost of $1.1 billion. The smart fence comprised an integrated framework of cameras, motion and various other types of sensors, autonomous weapon systems, radars, aerostats – all manned 24/7 and serving as data repositories and observation hubs.[42] This was supplemented by the Iron Dome system and the Jaguar semiautonomous UGV replete with advanced sensors, automated driving system and advanced targeting and firing options.[43] The Hamas attack dismantled the entire system in a matter of minutes by focusing on segregating and isolating the 23 observation posts rising over the fence, forcing IDF soldiers to get behind fortified defences and keep their head down, by launching massive Qassam rocket attacks and finally using commercial drones to drop small bombs on cellular communication towers to prevent passage of messages.[44] Then they just used hand gliders to simply glide over the fences and demolished them at more than 30 places using bulldozers and wire-cutting tools. Once inside mainland Israel, Hamas operatives used UAVs in top-attack profiles against Merkava Mk 4 tanks, combined Al Zawari one way attack (OWA) UAVs with rocket barrages to create a defender's dilemma within IDF ranks and finally, employed cyber and EW capabilities.[45]

However, in their response, apart from use of air strikes, IDF Ground Forces are using a number of technological platforms to counter the challenges of Hamas tunnels and hit-and-run raids by Hamas squads. One such innovation on the battlefield is the Smash fire control system that is used both for counter-UAV as well as anti-personnel tasks, releasing bullet from the Smartshooter rifle only when the target is in sight. This technology is primarily a miniaturised processor that sits atop a standard issue rifle sight and improves the accuracy of a hit.[46] Apart from this, the IDF is also using indigenously made the Iron Sting precision mortar system[47] and the Maoz or Spike FireFly LM. The IDF has also deployed the Ghost Unit, also known as the Multidimension Unit or Unit 888, in combat in Gaza. The unit, part of the 'multi-arena infantry division' or the 99th Division, integrates soldiers and capabilities from all physical domains of land, air and maritime with cyber, space and UAV expertise.[48] The unit, operating on a tactical level, uses advanced drones and a combination of precision mortars and anti-tank weapons to target Hamas cells. IDF is using these units for a two-fold purpose: pushing advanced capabilities to the level of companies and platoons and increasing the cognitive load on IDF soldiers; and field testing new technologies on an actual battlefield in a manner of spiral development.

NOTES

[1] Michael Ertl, “Nagorno-Karabakh: Conflict between Azerbaijan and Armenians explained”, *BBC News*, September 28, 2023, at https://www.bbc.com/news/world-europe-66852070, (Accessed March 26, 2024).

[2] Isabel Debre, “Israeli Arms Quietly Helped Azerbaijan Retake Nagorno-Karabakh, to the Dismay of Region’S Armenians”, *Associated Press News*, October 5, 2023, at https://apnews.com/article/armenia-azerbaijan-nagorno-karabakh-weapons-israel-6814437bcd744acc1c4df0409a74406c.

[3] Shaan Shaikh and Wes Rumbaugh, “The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense”, Critical Questions, Center for Strategic and International Studies, December 8, 2020, at https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense, (Accessed March 24, 2024).

[4] Ibid.

[5] Can Kasapoglu, “Turkey Transfers Drone Warfare Capacity to Its Ally Azerbaijan”, *Eurasia Daily Monitor*, The Jamestown Foundation, October 15, 2020, at https://jamestown.org/program/turkey-transfers-drone-warfare-capacity-to-its-ally-azerbaijan, (Accessed March 24, 2024).

[6] Eado Hecht, “Drones in the Nagorno-Karabakh War: Analyzing the Data”, *Military Strategy Magazine*, 7(4), Winter 2022, pp. 31–7, (Accessed March 24, 2024).

[7] No. 488.

[8] Vahe Sarukhanyan, “Azerbaijan’s Possible Purchase of New Turkish Attack Drones”, hetq, August 15, 2023, at https://hetq.am/en/article/159020, (Accessed March 24, 2024).

[9] No. 488.

[10] No. 490.

[11] Robyn Dixon, “Azerbaijan’s Drones Owned the Battlefield in Nagorno-Karabakh – and Showed Future of Warfare”, *The Washington Post*, November 11, 2020, at https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html, (Accessed March 24, 2024).

[12] “Azerbaijan Captures Armenian Tor-M2KM and OSA Air Defense Systems”, at https://www.armyrecognition.com/defense_news_september_2023_global_security_army_industry/azerbaijan_captures_armenian_tor-m2km_and_osa_air_defense_systems.html, (Accessed March 25, 2024).

[13] No. 488.

[14] Jakub Janovsky, Dan, Stijn Mitzer, Joost Oliemans and Kemal, “The Fight For Nagorno-Karabakh: Documenting Losses On The Sides Of Armenia And Azerbaijan”, Oryx, September 27, 2020 at https://www.oryxspioenkop.com/2020/09/the-fight-for-nagorno-karabakh.html, (Accessed March 24, 2024).

[15] Samuel Bendett and Jeffrey Edmonds, “Russia’s Use of Uncrewed Systems in Ukraine”, Center for Naval Analyses (CNA), March 31, 2023, at https://www.cna.org/reports/2023/05/russias-use-of-drones-in-ukraine, (Accessed March 24, 2024).

[16] “How Drones Dogfight Above Ukraine” at https://www.economist.com/the-economist-explains/2023/02/07/how-drones-dogfight-above-ukraine, (Accessed March 24, 2024).

[17] No. 500.

[18] Charles Bartles and Lester Grau, “The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces”, Foreign Military Studies Office (FMSO), Fort Leavenworth, at https://www.armyupress.army.mil/portals/7/hot%20spots/documents/russia/2017-07-the-russian-way-of-war-grau-bartles.pdf, (Accessed March 24, 2024).

19 Walter Williams, "Threat Update Krasnopol—A Laser-Guided Projectile for Tube Artillery", Rest of World Combat Systems, Threat Support Directorate, at https://man.fas.org/dod-101/sys/land/row/krasnopol.htm, (Accessed March 24, 2024).

20 Stephen Bryen, "US-made Parts Keep Russia's Artillery Firing in Ukraine", *Asia Times*, June 3, 2022, at https://asiatimes.com/2022/06/us-made-parts-keep-russias-artillery-firing-in-ukraine, (Accessed March 24, 2024).

21 David Hambling, "Russia's Deadly Artillery Drones Have a Strange Secret (Updated)", *Forbes*, April 11, 2022, at https://www.forbes.com/sites/davidhambling/2022/04/11/russias-deadly-artillery-drones-have-a-strange-secret/?sh=3c188869779d, (Accessed March 24, 2024).

22 Charles Bartles and Lester Grau, "The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces", Foreign Military Studies Office (FMSO), Fort Leavenworth. https://www.armyupress.army.mil/portals/7/hot%20spots/documents/russia/2017-07-the-russian-way-of-war-grau-bartles.pdf, (Accessed March 24, 2024).

23 Roger McDermott and Tor Bukkvoll, "Russia in the Precision-Strike Regime – Military Theory, Procurement and Operational Impact", Norwegian Defence Research Establishment (FFI), August 1, 2017, at https://www.academia.edu/33924504/Russia_in_the_Precision_Strike_Regime_ Military_theory_Procurement_and_Operational_Impact, (Accessed March 24, 2024).

24 Mohammad Eslami, "Iran's Drone Supply to Russia and Changing Dynamics of the Ukraine War", *Journal for Peace and Nuclear Disarmament*, 5(2), pp. 507–18.

25 No. 500.

26 Kelsey D. Atherton, "How Drones in Ukraine Help Fuel Propaganda and Shape Perception", The Center for Public Integrity, March 26, 2022, at https://publicintegrity.org/national-security/ukraine-in-crisis/how-drones-in-ukraine-help-fuel-propaganda-and-shape-perception, (Accessed March 24, 2024).

27 Gillian Tett, "Ukraine Is Already Looking to a Postwar Digital Future", *Financial Times*, May 25, 2023, at https://www.ft.com/content/2c73dfbc-a25f-420b-bf2b-41fbb17e5ddb, (Accessed March 24, 2024).

28 "People's Project" at https://www.peoplesproject.com/en, (Accessed April 4, 2024).

29 Phil Stewart, "Exclusive: U.S.-supplied drones disappoint Ukraine at the front lines", *Reuters*, December 22, 2016, at https://www.reuters.com/article/us-usa-ukraine-drones-exclusive-idUSKBN14A26D, (Accessed March 24, 2024).

30 David Hambling, "Ukraine's Drone Army Was Born in a Crucible of Conflict", *Popular Mechanics*, February 20, 2017, at https://www.popularmechanics.com/flight/drones/a25281/ukraine-makeshift-drones, (Accessed March 24, 2024).

31 No 372.

32 Ibid.

33 David Hambling, "Bargain Basement Bombers: Ukraine's Homemade Drones Hit Russian Forces (Updated)", *Forbes*, January 24, 2023, at https://www.forbes.com/sites/davidhambling/2023/01/24/bargain-basement-bombers--ukraines-homemade-drones-hit-russian-forces, (Accessed March 24, 2024).

34 Sakshi Tiwari, "Russia 'Shot Down' Over 100 Bayraktar TB2 Drones in The Ukraine War & Kicked Them Out Of Action – Moscow", *Eurasian Times*, April 11, 2023, at https://www.eurasiantimes.com/russia-shot-down-over-100-bayraktar-tb2-drones-in-the-ukraine, (Accessed March 24, 2024).

35 Stephanie Sy and Teresa Cebrian Aranda, "Longest Battle of Ukraine War Leaves City of Bakhmut in Ruins", *PBS News Hour*, May 22, 2023, at https://www.pbs.org/newshour/

show/longest-battle-of-ukraine-war-leaves-city-of-bakhmut-in-ruins, (Accessed March 24, 2024).

[36] https://www.russiamatters.org/analysis/roles-and-implications-ai-russian-ukrainian-conflict

[37] Ibid.

[38] Gaby Del Valle, "Report: Israel Used AI to Identify Bombing Targets in Gaza", *The Verge*, April 5, 2024, at https://www.theverge.com/2024/4/4/24120352/israel-lavender-artificial-intelligence-gaza-ai, (Accessed April 8, 2024).

[39] David Meyer, "Israel's Reported Use of AI in Its Gaza War May Explain Thousands of Civilian Deaths", *Fortune*, April 5, 2024, at https://fortune.com/2024/04/04/israel-idf-ai-warfare-gaza-palestinian-hamas-lavender-972, (Accessed April 8, 2024).

[40] Yuval Abraham, "'A Mass Assassination Factory': Inside Israel's Calculated Bombing of Gaza", *+972 Magazine*, November 30, 2023, at https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza, (Accessed April 8, 2024).

[41] Ibid.

[42] David H Freedman, "Israel's High-Tech Border Failure Could Happen in the U.S., Experts Say", *Newsweek*, November 15, 2023, at https://www.newsweek.com/2023/11/24/israels-high-tech-border-failure-could-happen-us-experts-say-1843772.html, (Accessed March 23, 2024).

[43] Sebastien Roblin, "Israel's Newest High-Tech Border Guard: The Jaguar Robot", The National Interest, August 21, 2021, at https://nationalinterest.org/blog/reboot/israel%E2%80%99s-newest-high-tech-border-guard-jaguar-robot-192061, (Accessed April 1, 2024).

[44] Reuters, "Hamas Deployed Specialised Units to Attack Israel, Says Source", *Reuters*, October 9, 2023, at https://www.reuters.com/world/middle-east/hamas-deployed-specialised-units-attack-israel-says-source-2023-10-09, (Accessed April 2, 2024).

[45] "465. Learning from LSCO: Applying Lessons to Irregular Conflict", at https://madsciblog.tradoc.army.mil/465-learning-from-lsco-applying-lessons-to-irregular-conflict, (Accessed April 3, 2024).

[46] Eyal Boguslavsky, "Smash Sights Used by IDF Infantry Units Fighting in Gaza", Israel Defense, November 27, 2023, at https://www.israeldefense.co.il/en/node/60419, (Accessed March 24, 2024).

[47] Aleks Phillips, "How Israel's Iron Sting Is Taking On Hamas", *Newsweek*, October 3, 2023, at https://www.newsweek.com/israel-iron-sting-mortar-hamas-1836874, (Accessed March 24, 2024).

[48] Seth J Frantzman, "Gaza Conflict is Proving Ground for Israel's New High-Tech Multidimensional Unit", Breaking Defense, January 22, 2024, at https://breakingdefense.com/2024/01/gaza-conflict-is-proving-ground-for-israels-new-high-tech-multidimensional-unit, (Accessed March 24, 2024).

Chapter Four

Challenges and Recommendations

This chapter lists certain recommendations and suggestions for improving the absorption of disruptive technologies in the Indian Army. Having looked at the various innovation structures and organisations responsible for promoting innovation and pushing down the products in the hands of the warfighter, there are certain critical issues that need to be addressed, both to increase the quality and the speed of technology absorption at the headquarter (HQ) and the unit level.

Challenges and Recommendations

There are multiple challenges related to defence and military innovation in India. This section will list out all the challenges and then focus on certain broad guidelines for recommendations:

(a) **Unpredictability of Modern Warfare**: Modern warfare is unpredictable in its unfolding. Though there have been similarities in the use of emerging technologies in the conflicts discussed above, it is also clear from the outcome (or lack of it) that victory on the battlefield is not certain with the use of these new technologies. A number of countries, short of outright invasion, have resorted to the use of grey zone warfare – a type of coercion that employs non-kinetic means or sub-conventional kinetic means to affect a change in the military or political posture of the adversary, forcing it to either react conventionally and risk a wider conflagration or do nothing. Increasingly, emerging and disruptive technologies are being used in this type of warfare and a deep relook is required in a military's approach towards warfighting to cater for conflicts across a wide spectrum of coercion.

(b) **Absence of Overarching Absorption Strategy**: The conflict in Ukraine has shown that despite the initial asymmetry provided by the sudden use of a new and disruptive technology on the battlefield, lack of absorption in the form of doctrinal change and establishment of new structures or modification of the old ones, the countermeasure holiday, as envisaged by the Israelis, is only brief, before the adversary devises offsetting measures. Absorption of disruptive technologies can be successful only if embedded into an overarching strategy that takes into account the external threat actors, the likely trajectory of technological growth, careful vetting of the technologies required by the forces and the likely end point after the use of these new platforms and technologies. Currently, the absorption of disruptive technologies needs a major overhaul since it is based on a conventional warfare scenario. The approach being taken is that of incremental innovation where the focus is on solving the existing issues and challenges in available platforms and trying to fit new technologies and platforms into existing concepts. Utilising the models of strategic, military and defence innovation as given by Cheung,[1] the absorption of technologies needs to start at the very top. There is a major concern that traditional military organisations are too wedded to the precepts of industrial age warfare with its neat segregation of platform-based capabilities, that unless a radical approach to modernisation is not undertaken, the new technologies and platforms will be made to conform to existing doctrines and structures rather than moulding existing ones or creating new ones from scratch. The issues of technology 'flattening' and 'spreading'[2] need to be looked at in detail.

(c) **Research & Development (R&D) Vertical within the Indian Army**: As mentioned earlier, the military innovation ecosystem of the Indian Army centres around the Army Design Bureau (ADB). But the ADB is not a design bureau in the literal sense of the word. For example, post the 1971 war and subsequently the 1974 Pokharan nuclear blasts, the Indian Navy (IN) created the Weapon and Electronic Systems Engineering Establishment (WESEE) in 1978 and posted personnel to indigenise products. The creation of this establishment was the recognition of the fact that while indigenous shipbuilding in the navy had started in the mid-1960s with the creation of the Naval Design Bureau (NDB) in 1965, the sensors and weapons continued to be imported from other countries.[3] All design bureaus, whether in India or abroad, are platform based. The 'design' component is to evaluate the potential for optimising the various sub-components obtained from various vendors so that the platform as a whole works as per envisaged capabilities. These design bureaus can be thought of as designers to large-scale integrators, which in the case of IN were the various shipyards cropping up in India. The organisation has a mix of PhDs and scientists. NDB and WESEE organically support IN.

In the case of the Indian Army, it hasn't had any organisation like this. An Army Facilitation Cell was created under then Director General Perspective Planning (DG PP now Director General Strategic Planning or DG SP), which was later renamed as ADB.[4] The organisation was totally focused on the innovation part, which was looking at gaps in capability requirements of various arms or line directorates and then looking at the industry and academia for solutions. The role of ADB was to look at the industry, requirements of the army, technological thresholds and suggest areas where there might be technology infusion.[5] The funds used were Innovation for Defence Excellence (iDEX), Technology Development Fund (TDF) and ATB, apart from Army Commanders' Special Powers Fund (ACFSP) and emergency procurement (EP). ADB looked at the respective arms' weapons, technology and capability profile and what technology infusion may be required over multiple time windows. The closer the time period, the clearer its suggestions were.

ADB was imagined as the Indian version of Defence Advanced Research Projects Agency (DARPA) and its motto was and still remains 'Connecting Capabilities'.[6] However, in the defence sector, since there was no gatekeeping, all startups started pushing their projects everywhere. This was one of the major reasons behind the creation of the Defence Innovation Organisation (DIO) to handle and channelise startups. Another issue is that ADB requires an infusion of technical manpower. Institutes such as the Army Institute of

Technology (AIT) should be leveraged for searching for technological proposals. Even within the Indian Institute of Technology (IITs), apart from a few professors, most are focused on prototypes and not products and therefore private universities outside this system need to be tapped. The second challenge is that ADB, even as envisaged in its original role, has been a facilitator organisation. This is a major gap since ADB can only vet and not create its own proposals.[8] Whatever it vets is the collection and collation of requirements by other arms and line directorates. This may help in aiding the incremental innovation part, where each arm and platform is getting evolutionary and there are gradual upgrades to similar weapon profiles, it hinders true defence innovation.

Secondly, looking at the linkages with actual innovation organisations: ADB routes its challenges and problem definition statements (PDS) to the DIO, under Department of Defence Production (DDP), which further hands them over to the partner incubators (PIs), whose responsibility is the identification of suitable startups and iDEX winners.[9] The ADB, therefore, remains two steps removed from the site of innovation. Additionally, there is relatively limited technical expertise within ADB to either create or vet proposals, which means that innovation does not happen within the army, nor can soldiers or officers co-develop or co-create with the startups and micro, small & medium enterprises (MSMEs), which is the need of the hour, both for optimising the time and the potential of the technological artefact. At the same time, the role of the ADB is in pushing indigenisation, especially in creating linkups between the requirements of the line directorates and indigenous startups and MSMEs.

(d) **Challenges of DIO, iDEX and PIs:** Most PIs have limited technological and institutional capacity to support the startups. Also, this indirect way of reaching out to startups dilutes the urgency and need for rapid prototyping and iterative development issues. Though the program director from DIO is supposed to supervise the PIs, the monitoring is procedural and may not cater to the technological output.[10] Since DIO doesn't have the technical capacity for issuing the utilisation certificate, which is a mandatory document stating that the startup has rationally spent the given tranche of the Support for Prototype and Research Kickstart (SPARK) grant, this job is handed to PIs. The process of issuing a utilisation certificate is that the nodal agency has a review through a committee, a nodal officer report is required for every milestone and startups have to show proof that they have commercial backing. As of now, individuals with technological skills have not been employed consistently as consultants to take care of techno-commercial activities. The recruitment of manpower for program directors (PDs) and deputy PDs (DPDs) does not cater for a minimum technical baseline. PDs and DPDs are supposed to assist the startups from top to bottom since these are not MSMEs with some financial power. They require help and guidance in materials, services, locations, labs and ranges and people. The entire startup selection and procurement process is centralised instead of being decentralised.[11] There are a lot of tech startups in India that are relevant for defence but they haven't heard of iDEX till date. Lack of common Indian design standards and quality control is also another issue.[12] If one looks at the recent conflicts, it is easy to grasp that commercial technology need not be converted to military grade for every case since a decent amount of ruggedness is built in even in commercial products. As a result, there is a need for a certain level of segregation where COTS platforms and technologies must be judged based on pre-existing international standards, preculding the need for long-winded and time consuming quality assurance (QA) processes.

(e) **Innovation Cycle Split into Two Mutually Antagonistic Processes:** If one looks at the entire innovation cycle – from an idea to the product – there is an obvious split in the middle. Most innovation organisations, either embedded within the military or catering to the needs of defence face this issue. The innovation cycle in itself and the support (financial, moral and institutional) provided to the startups is generally well-defined and the speed of bringing up a technology readiness level (TRL) 3 idea to a TRL 8 prototype, well tested in multiple conditions, is very good. However, this is the stage where the hand-off from the innovation organisation to the acquisition organisation takes place. While, for the former, rapidity in action and decision making is paramount, for the latter it is the exactly opposite. The main criteria for acquisition organisations is ensuring fair competition and preventing loss to the exchequer. This phase is marked by excessive, multi-year deliberations, which defeats the entire purpose of expediting an idea up the TRL chain.

Recommendations

Before starting with the recommendations, a new model of technology absorption is being presented. Many would argue that in order to introduce a new model, the lacunae in the older model should be identified. The most critical difference between industrial age absorption and the newer technologies is that of capabilities. The earlier model of technology absorption and the one still in vogue, looks at technology absorption from the point of view of a platform: better tanks, better rifles, better jets etc. This is robust in the sense that it locks technology development under the rubric of a known platform and only an incremental innovation needs to be looked at. However, emerging technologies such as AI, quantum technology, synthetic materials and others are much more expansive and encompassing. They are also cross disciplinary. As a result, the old model where capabilities are tied to platforms and therefore certain specialised arms, may not lead to optimal outcomes. It is for this reason that a new framework called the Adaptive Integrative Framework for Technological Absorption in the Armed Forces (AIF-TAF) is proposed. The pillars underpinning this model focus on *capabilities; open-source innovation; networking; talent management;* and *flexibility*.

AIF-TAF provides a higher-level and abstracted framework for technology absorption into the Indian Armed Forces in general and the Indian Army in particular. The need for a higher-level framework becomes important from the perspective of providing a structure and foundation for an understanding that can enable the army to look at future technologies and provide a broad guidance on how to create enabling policies for technologies and platforms to be tested and embedded within different components of the organisation. AIF-TAF takes inspiration from the tenets of complexity science – an interdisciplinary field that studies complex systems characterised by non-linear interactions, emergent properties and self-organisation. It seeks to understand how simple rules and behaviours at the individual level give rise to complex, often unpredictable phenomena at the system level. Complexity science applies mathematical modelling, computational simulations and empirical observation to explore the dynamics of various systems including biological, social and economic systems. Since the army is also a social system with its peculiar cultural and organisational characteristics, applying the tenets of complexity science to technology absorption gives rise to a sequenced and step-based pedagogy.

On a practical level, the first tenet or step of AIF-TAF is complexity assessment and systems mapping. Modern warfare needs to be understood in its totality. The process of military and defence innovation does not occur in a situational vacuum. It has to be adaptive enough to foresee both growth trajectories of technologies and their interaction with social systems, looking at vulnerabilities to avoid on the friendly side while exploiting the adversary's. Also, there is a need to map out the interactions and dependencies within the army's ecosystem, looking at linkages not only with other Services but also across the civilian sector. The military ecosystem contains not just technological artefacts or products used by the forces and developed for them by the public and private sectors, but also the supply chains, norms, institutions, ethics, cultural traits, intellectual capital, industrial strength, international partnerships and policy guidance, among others. These have to be mapped out in detail with important strengths and vulnerabilities chalked out and solutions for them ideated.

Once this is done, the second tenet is to identify the emergent needs of military technology through a bottoms-up approach. This can also be termed as *emergent needs identification*, where multiple disciplines and operational levels (units, formations and individuals) are engaged for identifying challenges specific to their functioning and areas of responsibility. These challenges should not be filtered through the prism of a particular arm or Service. Based on these challenges, solutions need to be thought of and forecasting for future challenges needs to be done. Disruptive technologies such as quantum computing and AI can help here.

The next step is the exploratory scouting of technologies where selected army personnel, in concert with academia and civilian counterparts in industry, bureaucracy and startups engage in a broad and dynamic search for potential technological solutions. The critical component of this stage is the ownership of the army as a whole for searching for and steering technological solutions for itself, rather than delegating it to other organisations. Next comes the rapid prototyping and iterative development, which will be monitored and led by uniformed project officers working with startups, academia, MSMEs, DRDO labs and system integrators. These projects will be owned by the army, based on its specific requirements. Feedback will be given and incorporated into the development process, with quick trials and testing.

After this comes the decentralised experimentation and learning phase. Here units and formations will test and validate the technology in varied conditions and observations and lessons will be shared on a common portal based on the Army Digital Network (ADN). This will facilitate cross-learning and information sharing within the organisation. The networked evaluation and feedback loop phase is next, where technological effectiveness will be vetted and consolidated based on a networked approach using the lessons culled from the common portal. Positive feedback loops will be used for continuous improvement and adaptation. The training and doctrinal amendments and modifications will start in parallel and not wait for a particular product. One also needs to start looking at setting broad pedagogies for training on scientific temperament and not just specific systems and drills. Flexibility and adaptability in training programs will be emphasised.

The next tenet focuses on scalable integration and resilient deployment and integration of technologies. Instead of products, one will need to focus on technologies and their enablers, that is, trained and tech-oriented officers and soldiers. This will prepare the force for rapid changes and unforeseen challenges in deployment. After this is the holistic operational feedback and system reassessment, where holistic feedback considering impacts across the entire system will be gathered and technology's role within the broader system will be regularly assessed. The last step is strategic adaptation and continuous evolution where strategies will be continuously assessed and adapted to align with evolving technology and warfare landscapes. An ongoing and evolutionary process of technology absorption will be resorted to.

We will now look at the E, B and G level analysis, which is a strategic framework typically used in intelligence and military contexts. It stands for 'Economic', 'Bureaucratic/Administrative', and 'Geopolitical' levels of analysis. Applying this framework to AIF-TAF involves examining how economic factors, bureaucratic or administrative structures and geopolitical considerations influence the framework's effectiveness and implementation.

E Level (Economic Analysis) of AIF-TAF

- **Budget and Funding**: Assess the economic feasibility of integrating emerging technologies. This includes evaluating the costs of acquisition, maintenance and required upgrades for emerging technologies such as AI, unmanned systems, big data, and others.
- **Resource Allocation**: Determine how resources are allocated for training, R&D and infrastructure upgrades essential for technology absorption.
- **Economic Impact**: Consider the broader economic impact of technology integration such as potential cost savings, efficiency improvements and the economic benefits of advanced technological capabilities.
- **Industry Partnerships**: Explore partnerships with private sector firms as well as the potential economic benefits of collaborations in developing and integrating new technologies.

B Level (Bureaucratic/Administrative Analysis) of AIF-TAF

- **Organisational Structure**: Evaluate how existing military organisational structures support or hinder the absorption of new technologies. If required, consider the need for restructuring to facilitate more agile and adaptable decision-making.
- **Policy and Regulation**: Assess the adequacy of current policies and regulations governing the use of emerging technologies in military operations, including ethical guidelines and rules of engagement.
- **Inter-Service Coordination**: Analyse the level of coordination and communication between different branches of the armed forces in the technology integration process.
- **Training and Development**: Focus on the administrative processes for training military personnel in new technologies, ensuring that they are adequately prepared to utilise these capabilities.

G Level (Geopolitical Analysis) of AIFTAF

- **Global Technological Landscape**: Examine the geopolitical implications of technological advancements globally. Assess how other nations' technological developments might impact military strategy and national security.

- **Alliances and Partnerships**: Consider the role of international alliances and partnerships in technology sharing, joint development programs and standard setting in military technologies.
- **Strategic Deterrence and Influence**: Evaluate how the integration of advanced technologies affects a nation's strategic deterrence capabilities and its influence in global affairs.
- **Ethical and International Norms**: Assess how the adoption of emerging technologies aligns with or challenges international norms and ethical standards in warfare.

The E, B and G level analysis of AIF-TAF allows for a comprehensive examination of the economic, bureaucratic and geopolitical dimensions of integrating emerging technologies in the armed forces. This approach ensures that strategic decisions are informed by a thorough understanding of the various external and internal factors that can impact the success and sustainability of technology absorption in military contexts. We will now look at a hypothetical example of AI with respect to the AIF-TAF framework and see how disruptive technologies can be effectively absorbed by the Indian Army.

Absorption of Artificial Intelligence (AI) in the Military

Complexity Assessment and Systems Mapping

- Understand AI's potential impact across various military domains such as intelligence, surveillance and reconnaissance (ISR) decision-making, pattern recognition and autonomous operations.
- Map out the AI ecosystem including data sources, processing capabilities and user interfaces.

Emergent Needs Identification

- Identify specific operational areas where AI can enhance decision-making, efficiency or tactical advantage.
- Gather inputs from intelligence assessments, field units and formation commanders and cybersecurity establishments.
- Nominate officers with specific educational qualifications and understanding for exploratory scouting.

Exploratory Scouting of Technologies

- Collaborate with AI research institutions and private sector innovators to explore cutting-edge AI applications.
- Attend technology expos and engage in defence-specific AI research.

Rapid Prototyping and Iterative Development

- Co-develop and/or co-create AI prototypes for specific applications such as predictive maintenance, threat analysis or unmanned vehicle navigation. Collate information and continuously monitor the progress of the project.
- Continuously refine AI algorithms based on real-world feedback.

Decentralised Experimentation and Learning

- Deploy AI prototypes in various geographical and functional settings: such as command HQ, lower formation HQ, units, individuals, army HQ branches and directorates.
- Utilise AI-based systems in real-time operations in Jammu and Kashmir (J&K).
- Encourage units to experiment with AI tools and share lessons learned.

Networked Evaluation and Feedback Loops

- Use a distributed network of analysts and operators to evaluate AI performance. Nominate nodal officers across commands (Service now and theatre later) who will monitor, collect, collate and analyse the observations and create positive feedback loops to route to the developer.
- Establish feedback mechanisms to inform ongoing AI development.
- Create an AIF-TAF portal on ADN to collect observations and lessons learned.

Adaptive Training and Doctrine Co-evolution

- Develop training programs that evolve with AI advancements, focusing on human-machine teaming (HMT).
- Update both the army and the HQ Integrated Defence Staff (IDS)' doctrine to include AI-enabled strategies and tactics.

Scalable Integration and Resilient Deployment

- Gradually integrate AI systems into broader military operations, ensuring scalability.

- Prepare for potential AI vulnerabilities and ensure systems are resilient to disruption.

Holistic Operational Feedback and System Reassessment

- Collect comprehensive feedback on AI's impact across different military domains.
- Reassess AI strategies and tools regularly to ensure they meet evolving military needs.

Strategic Adaptation and Continuous Evolution

- Adapt long-term military strategies to leverage AI's full potential.
- Continue investing in AI research and development for ongoing capability enhancement.

Coming to specific recommendations on the broader policy directives, some are given below:

(a) New National Defence Science, Technology and Innovation (NDSTI) Strategy

The Vijay Raghavan Committee, which was tasked with the restructuring of DRDO, has proposed significant reforms in defence technology management. Under the panel's recommendations, the Defence Technology Council (DTC), chaired by the prime minister and including the defence minister and national security advisor (NSA), will play a central role in identifying suitable partners for specific defence technologies. To bring together diverse perspectives, DTC would also include two members each from academia and industry. This move signifies the prime minister's office's (PMO) direct involvement in defence research and oversight over DRDO. Furthermore, the panel suggests the establishment of a separate department within the Ministry of Defence (MoD) – the Department of Defence Science, Technology and Innovation (DDSTI). This department would promote defence R&D within academic and startup ecosystems and also serve as the secretariat for the DTC. Additionally, an empowered committee under the DTC, co-chaired by the chief of defence staff (CDS) and the PSA, has been proposed. The panel also recommends bifurcating the post of secretary R&D in MoD currently held by the DRDO chairman.[13] Assuming this open domain news to be true and notwithstanding the fact that this may create another delinking layer within the already complicated and process-oriented bureaucracy of the MoD, there is a need for a National S&T and Innovation Strategy (NSTIS), which can be taken out now by DDSTI in concert with the National Security Council Secretariat (NSCS), Department of Science and Technology (DST), Department of BioTechnology, DRDO, Ministry of Electronics and IT (MeitY) and the Department of Space (DoS).

Based on this, DMA should devise the National Defence Science, Technology and Innovation Strategy (NDSTIS). The NDSTI should be able to recognise the geopolitical and strategic settings under which the technological requirements of the armed forces will need to be met and set down the parameters and critical technologies required for the forces on the short-, medium- and long-term horizon. This will provide a direction to the efforts of the startups and R&D setup across the country. The Military Science, Technology and Innovation Strategy (MSTIS) can then be taken out by the HQ IDS, with the operations branch being at the helm. Based on this, the theatre commanders or Service chiefs can create their own S&T and Innovation Plan (STIP). STIP should focus on mini offsets in the short term, capability enhancements in the medium term and deep-tech in the long run. Now that the geography and functionality of the theatre commands are set, the priorities in forecasting will be clear. Models that can be used for further studies include the May 2023 report by the Special Competitive Studies Project (SCSP) called 'Offset-X: Closing the Deterrence Gap and Building the Future Joint Force', which identified 10 key technologies that will provide an effective deterrence against adversaries in the future.[14] One has to remember that the effectiveness of certain disruptive technologies becomes very explicit in their application to grey zone warfare, which may be the predominant form of conflict that Indian forces may be engaged in and where conventional capabilities may prove relatively ineffectual.

It is therefore recommended that a new organisation be created under the Deputy Chief of Army Staff (Strategy) called the Innovation Directorate, headed by a DG. DG Innovation will have control over the Indigenisation, R&D (INRD) funds under a new ATB cell and a new corporate social responsibility (CSR) outreach cell headed by a civilian appointee with prior management experience in tech companies. This will have two branches, the pre-existing ADB responsible solely for incremental innovation and a new R&D Bureau (RDB) under a two-star additional director general (ADG).

The existing ADB should be made responsible for Defence India Startup Challenges (DISC) concerning the army and TDF. It should also have horizontal linkages with the navy and the air force for ensuring that common technological products and prototypes are shared across Services for scaling.

ADG RDB should have under him two brigadiers (Brigs): Brig Ideas and Innovation and Brig Operational Concepts (Op Concepts). Under Brig Ideas and Innovation, there should be three colonels (Cols). Col Civil Military Integration (CMI) will have under him three cells: standardisation cell, commercial technology quality assurance (QA) cell and intellectual property (IP) cell. Col Makerspace will be responsible for monitoring the progress of military officer and soldier innovators across newly established innovation floors at the level of the Command HQ. He will also have an Assistant Military Secretary (AMS) Innovation posted under him to liaise with the military secretary (MS) branch for ensuring officers with requisite educational and technical qualifications are selected and posted across these innovation floors. He will also be responsible for Project Army Talent Acquisition and Leverage (ATAL) cell. The ATAL cell will invite requirements and ideas directly from units and formations in field and pass them to startups. Finally, Col Deep-Tech and Startups, the third colonel under Brig Ideas and Innovation, will be responsible for drafting and creating policies and strategies for deep-tech and liaise with Project AGNII for inviting startups and organisations involved in deep-tech for consultations and demonstrations. Additionally, the colonel will also head a mixed team of civilians and military SMEs to scout for startups up to TRL 3, bring them up to prototype stage and then hand them over to the cross-functional teams (CFTs) for scaling them for deployment. Brig Op Concepts will head a team of four Cols heading four CFTs of sensors, shooters, processors and communication links. These teams will be a mix of all arms and Services and may feature civilian SMEs. The army currently functions on industrial era concept of arms and services, handled by various line directorates. The IN and Indian Air Force (IAF) do not face this challenge since all their various branches serve platforms. However, as the new technologies have a lot of overlap it becomes very difficult to designate a single directorate for innovating a particular technology. Since future warfare is likely to be fought by arms-agnostic platforms such as drones and autonomous systems, it is logical that formations are based on functionalities rather than Cold War era distinctions of specific platforms. Industrial age silos cannot fight modern age wars and there is a need to recast or reassemble existing line directorates.

A point on the concept of CFTs. CFTs are the physical manifestation of the desired shift from platforms to capabilities. For example, one needs to define the requirement of capabilities such as long-range firepower, precision effects, space-based C4ISR, cross-terrain mobility and individualised miniature aviation etc. This needs to be the foundation and will obviously be informed by the threat scenario and a national security and defence strategy, written or unwritten. The current CDS has called it 'tactics led modernisation'. In fact, one can go one step further and state that there is need of a 'capability based modernisation'. Once the requirements are clear, one can start finding, inventing and absorbing new technologies. The next step is to remove the silo-isation within the Services and arms. Traditional platform-based units have to be restructured radically if the aim of fighting multi-domain operations has to be fulfilled. IBG-isation (Integrated Battle Groups) and theaterisation are the correct step in this direction but they need to be made more expansive. New warfighting domains such as cyber, electromagnetic spectrum, cognition and near space have to be taken into account, with adequate intellectual space for incorporating new domains as and when they come into existence. In other words, the old adage of strategy equalling means and ends has to be reimagined. While ends are the effects that one intends on the adversary, capabilities are the means.

(b) Human Resource (HR) Management for the Army

For any technology-oriented organisation, the most important asset and capital is the intellectual capital. In order to ensure that technology absorption is effective and long lasting, it is necessary that the required intellectual capital be built up. A Talpiot like program can be imagined to be setup within the various army-run institutions such as the Military College of Telecommunication Engineering (MCTE), where a dedicated number of seats are reserved for such candidates. Within the existing force, there is a need to consolidate the number of officers and men from a science, technology, engineering and mathematics (STEM) background and post them accordingly. Identified innovators must be assured that their unique workloads and postings will not interfere with their promotions. Finally, the newly established RDB must have minimum posting criteria as a Master of Technology (M Tech) and/or a Doctor of Philosophy (PhD) in STEM subjects.

(c) Talent Management

Though it may seem counter-intuitive, given the stress on emerging technologies replacing humans, the single most important ingredient of this desired change is the human talent. The Indian Army needs to start matching appointments with qualifications and capabilities, with a stress on technical competence. The deployment period of these personnel also needs to be extended to match the fruition of a particular technology rather than being time bound. Startups and MSMEs are the cutting edge of technological development but there is latent potential within the army that needs to harness and leverage these technologies – in terms of training, education, usage, creation and R&D.

One can also think of modifying the short service commission to orient it to an Israeli-lite model, where young entrepreneurs or even willing CEOs of defence tech startups may be commissioned in the army on a five-year basis. This can be a win-win for the individual and the organisation, both on a short- and long-term basis. While the Indian Army will gain willing technology-savvy individuals whose commissioning period will be tied to a five-year cycle where they can access all the institutional resources of the army to develop their ideas from TRL 1/2/3 to 7/8, gain a deep understanding of the organisation and its peculiarities in the process and the at the end of the five-year period, offer the prototype to the army, with the intellectual property (IP) resting with the individual. This will create a core of technologists within the force. On the other hand, once the individual leaves the organisation, he can hone and sharpen the prototype, create a better product and even contribute to the defence export potential of the country.

(d) New Technologies Require New Acquisition Processes

The MoD's manual on the Defence Procurement Procedure (DPP) 2016 lists 12 steps for acquisition: request for information (RFI), service qualitative requirements (SQRs), acceptance of necessity (AoN), solicitation of offers, evaluation by the technical evaluation committee (TEC), field evaluation, staff evaluation, oversight by the technical oversight committee, commercial negotiations by the contract negotiation committee (CNC), approval by a competent financial authority (CFA), taking out the supply order (SO) and finally, post contract management details. This needs to be modified for startups. The RFI that informs the general environment about the capabilities required by the forces and also the tentative time schedule for the acquisition process or the request for proposal (RFP) does not need to be promulgated separately for requirements of the army already mentioned in the compendium of problem definition statements (CPDS); the CPDS itself should be treated as the RFI. Additionally, once the RDB is setup and innovators from the army are involved in the design and development (D&D) process along with the startups from the TRL 3 stage onwards, the TEC and Technical Oversight Committee (TOC) phase should also be done away with since the technical evaluation and oversight is happening concurrently. The DPP can also feature a separate category for technologies identified in the NDSTIS for expedited delivery processes. There has to be a recognition that the grants and aid given for the development of a particular prototype have to be taken forward, if vetted on ground, and allow the product to scale rather than limit its spread by channelling it into a conventional acquisition process.

Conclusion

The Indian Army stands at the precipice of a transformative era marked by the assimilation of disruptive technologies into its operational framework and as symbolised by the theme of 2024 for the Indian Army – the Year of Technology Absorption. Drawing insights from the defence innovation ecosystems of the US, Israel and Ukraine, as detailed in earlier chapters, India is poised to leverage these learnings to bolster its indigenous defence capabilities. This will, however, require a major turning away from years of entrenched silo-isation, not only between Services, but also within the army, which is still arms-focused. The latest spate of technologies, being platform agnostic, need a different development and acquisition process, as compared to the existing ones. This can only come from a top-down approach. Lessons gleaned from conflicts such as Israel–Hamas, Russia–Ukraine and Armenia–Azerbaijan underscore the imperative for the Indian Army to swiftly adapt to evolving threats and adopt a proactive stance towards innovation and technology absorption.

Within the Indian context, a comprehensive examination of the domestic innovation ecosystem, elucidated in preceding chapters, sheds light on the nation's burgeoning potential in defence innovation with the caveat that if the current rate and procedural bottlenecks continue, startups in the defence sector may pivot to other fields and domains, such is the nature of the commercial technology. The introduction of the AIF-TAF framework represents a paradigm shift, providing a structured approach to facilitate technology absorption and integration within the Indian Armed Forces. By fostering collaboration between academia, industry and defence establishments, this framework is poised to propel India towards self-reliance in defence technology.

In conclusion, the journey towards disruptive technology absorption in the Indian Army is marked by both challenges and opportunities. By embracing the principles of innovation, collaboration and adaptability, the Indian Army can navigate the complexities of modern warfare and emerge as a formidable force capable of safeguarding the nation's interests in the 21st century and beyond.

NOTES

[1] Tai Ming Cheung, "A Conceptual Framework of Defence Innovation", *Journal of Strategic Studies*, 44(6), June 22, 2021, pp. 775–801.

[2] Akshat Upadhyay, "Engagement or Estrangement: Gauging Indian Army's Relationship with the Emerging Technologies", Centre for Land Warfare Studies, Issue Brief No 272, February 11, 2021, (Accessed March 24, 2024).

[3] Smruti Deshpande, "45 Yrs Since Founding, Navy's Engineering Establishment WESEE Works on Next-Gen Combat System", *The Print,* July 24, 2023, at https://theprint.in/defence/45-yrs-since-founding-navys-engineering-establishment-wesee-works-on-next-gen-combat-system/1683133, (Accessed June 20, 2024).

[4] No. 499.

[5] Ibid.

[6] Ibid.

[7] Author interview with the Officer.

[8] No. 499.

[9] Author Interview with Ex iDEX-DIO member.

[10] Ibid.

[11] Ibid.

[12] Author Interview with CEO of a Mysore-based Defence Startup.

[13] Pradip Sagar, "Top Panel Recommends Shake-Up in DRDO, Bigger Role for Private Players In Defence Research", *India Today*, January 9, 2024, at https://www.indiatoday.in/india-today-insight/story/top-panel-recommends-shake-up-in-drdo-bigger-role-for-private-players-in-defence-research-2486516-2024-01-09, (Accessed June 13, 2024).

[14] Justin Lynch et al, "Offset - X: Closing the Deterrence Gap and Building the Future Joint Force", Special Competitive Studies Project (SCSP), Report, May 2023.

Index

₹ 995

PENTAGON
PRESS
www.pentagonpress.in

ISBN 978-81-98445-88-9
9 788198 445889