

Medals and Ribbons

Jan. - Mar. 2024 | Vol.4 | Issue 1 ■ Price Rs.200/- ■ Annual Subscription Rs.700/- (ENGLISH QUARTERLY)

A SALUTE TO OUR VALIANT WARRIORS

Unrestricted Future **WARFARE**

Multi Domain with Disruptive Technologies

**NAVIGATING THE
DIGITAL AGE**

The Digital Landscape Surrounds Us

**NUANCED USE OF FORCE
IN INDIAN STATECRAFT**

The First 15 Years after Independence

**MILITARIZATION AND
WEAPONIZATION OF SPACE**

Implications for India

DEDICATED TO

The Valiant Warriors of 19 RR, 63 RR, 9 PARA (SF) and J&K Police
who were killed in action in Kokernag and Kalakote on
13 September 23 and 22 November 23 respectively

Operation Garol, Kokernag, 13 September 23



IC-67028M
Colonel Manpreet Singh,
SM, 19 RR
(Parent unit 12 SIKH LI)



IC-78151L
Major Aashish Dhonchak,
SM, 19 RR
(Parent Unit 15 SIKH LI)



4494574P
Sepoy Pardeep Singh,
19 RR
(Parent Unit 18 SIKH LI)



185686
DySP Himayun Muzzammil Bhat,
Kashmir Police Service,
District Police Office, Anantnag

Operation Solki, Kalakote, 22 November 23



IC83609N
Captain MV Pranjal,
63 RR
(Corps of Signals)



IC 84541K
Captain Shubham Gupta,
9 Para SF



9114288Y
Havildar Abdul Majid,
9 Para SF



4207184P
Lance Naik Sanjay Bisht,
9 Para SF



16032927X
Paratrooper Sachin Laur,
2 Para SF

Col David Devasahayam



In the last few issues, we have largely been bringing to our readers historical narrations and reports of actions and operations done by our Armed Forces since Independence. There are many stories yet to be narrated but I realise that we also need to look ahead. Contemporary conflicts and future warfare will be vastly different from what we have seen in the past. Modern warfare has many dimensions, described as **“Multi Domain Operations”** in military parlance.

Being involved with capital markets and investments on a daily basis, I consistently witness the power wielded by the global financial cartels. Attempts to dismantle or weaken the existing financial order are being made by the emerging powers, alternative currency trade is being propounded and structural changes are being suggested in the global governing bodies. Today, Economy is the strongest pillar in the National Power of a country, and economic warfare is thus an important dimension in modern conflicts. It is operationalized through sanctions, trade monopolies, resources denial, grants, loans and denial of loans too. The Russo –

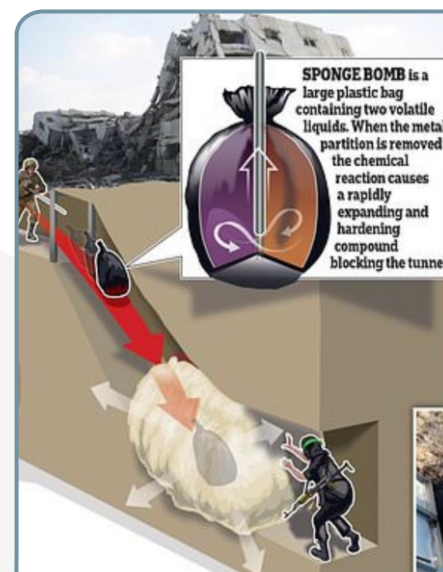
Ukraine War has seen curbs being put on Russian oil and gas, and strong attempts to reduce the flow of dollars into Russia.

Technological advances have been the **‘drivers of change’** in warfighting doctrines and capabilities. In this generation, technological leaps are more rapid than what was witnessed in previous centuries. Our young leaders have to keep pace with these technological trends, and the Armed Forces have to remain equipped and ready for these new *‘game changing demons of war’*.

To quote an example, I recently viewed a video showing the **“sponge bomb”** innovated by Israel to counter the Hamas in the Gazan tunnels - An ingenious answer to the extremely difficult infantryman’s battle of fighting through the narrow, dark passages and a maze of tunnels. Such quickly innovated disruptive technologies will profoundly influence future battles.

In this issue, we have thus focused on such innovative inventions in the fields of computing, communications, analytics, and also discussed threats in the biological warfare dimension. Space warfare, drones, biometric profiling, influence

operations are some of the other themes that we have deliberated upon. Since the theme of this issue is looking into the future, readers will miss the personal accounts and action stories, which were a part and parcel of our previous issues. Nevertheless, I know that it would be worthwhile for readers to dwell upon the changing trends and technologies which will shape our military readiness in the coming decades.



The Sponge Bomb

CONTENTS

Vol.04 • Issue 01 • Jan '24 - Mar '24

Nuanced Use of Force in Indian Statecraft 09

by Maj Gen H Dharmarajan

A perspective covering the military's role while subtly influencing decision-making from a recessed backdrop in the first 15 years post attaining independence in 1947.

Navigating the Digital Age 16

by Adm Karambir Singh (Retd)

Our former Naval Chief elaborates that digital technology has become the backbone in modern warfare, offering precision and sophistication previously unimaginable.

Space Militarization and Weaponization 20

by Lt Gen Anil Bhatt (Retd)

Space has rightfully been identified as the fourth dimension of warfare after land, sea and air. This overview brings out the evolving dynamics of space militarization and weaponization.

Pathogens and Viruses - A Likely Biological Warfare – Bioterror Threat? 28

by Lt Gen R S Grewal (Retd)

Dangerous pathogens can be developed and used to target an inimical country, people, group or enterprise as world power politics becomes more immoral – as highlighted in this commentary.

Private Military Contractors – The Dogs of War 36

by Maj Gen A K Bardalai (Retd)

Private Military Contractors will continue in future conflicts as they meet the clandestine requirements of different nations, and provide lack of accountability too – an insightful analysis.

Trends in Maritime Warfare 40

by Rear Adm S Y Shrikhande (Retd)

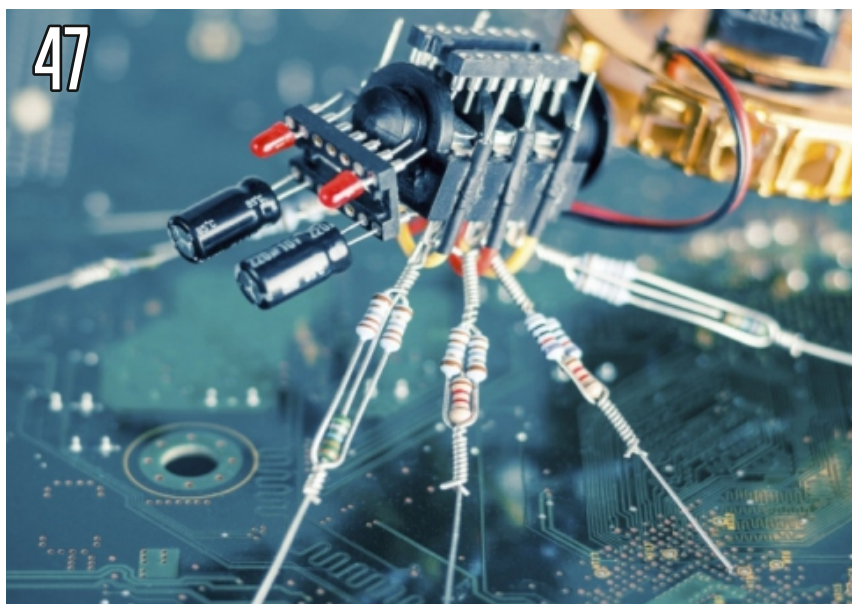
With increasing accuracy and longer ranges, anti-ship missiles, unmanned boat swarms and drones are potent threats to ships at sea. Trends in the maritime dimension are discussed in this analysis.

Drones - Shaping Combat Space in the Russia-Ukraine Conflict 44

by Air Marshal Harpal Singh (Retd)

Drones or unmanned aerial vehicles are proving to be potent, effective and economic in conflict. This article discusses their employment in the Russia-Ukraine Conflict.





56 **Edge Computing** *by Brig Subhash Katoch (Retd)*

Edge Computing provides one of the possible ways to handle the large amount of data from sensors, shooters and computing power as well as reliable networks required to handle contemporary warfighting.

60 **Quantum Technology and Military Operations** *by Capt Vishwas Sharma*

The disruptive power of quantum technology and how it stands to reshape the battlefield, from secure communication channels and unbreakable codes to ultra-precise navigation and intelligence gathering is discussed in this paper.

65 **5G Technology** *by Lt Col Tony Joseph and Capt Pooja Sharma*

A scan of 5G technology and how it benefits the Armed Forces, and how it differs from 4G, 3G, etc.

68 **Moving to 6G – The Next Tech Race** *by Col Dinesh Sharma (Retd)*

A new paradigm of wireless communication, the sixth-generation system, is expected to be implemented between 2027 and 2030 with full support of Artificial Intelligence. This review highlights the technological blueprint.

72 **Evolving Weapons and Systems – Transient Nature of Disruptive Technologies** *by Col Manish Sarin (Retd)*

Ongoing conflicts have propelled new tactics and weapon systems onto the battlefield. Innovations too have been made, but counter-measures are also fielded rapidly.



47 **Nanotechnology** *by Lt Col Rahul Hermon*

Nanotechnology applications in defence include small and micro drones, mosquito drones, nano satellites for military communications and surveillance and such other innovations. A report on this future technology.

52 **Striking Shadows – The Biometric Danger** *by Col VKT Mishra (Retd)*

This article discusses how biometric profiles are built up and transparency about leader's behaviour, attitudes, location and so on is used to target them.



Navy's Innovation Impetus – Converting 'SPRINT' to a Marathon 76

by Cdr Ishant Panwar

SPRINT is an initiative from the Navy which succeeded in launching 75 viable innovations in the first year. This article critically examines SPRINT with an aim to recommend long term policy and organisational changes.

North Tech Symposium 80

by Lt Gen J S Sandhu (Retd)

To match the operational requirements with advances in weaponry and new technologies, the users, the developers, the manufacturers and the researchers are brought together on a single platform. A report on this symposium.

Tiranga Atop 28 Highest Points / Peaks 82

by Col R S Jammal

'Har Shikhar Tiranga', an audacious and patriotic expedition, hoisted the Indian national flag on the highest peak or point of every state across India in the last one year.



Smarter Ways to Invest in Real Estate 84

by Babu Krishnamoorthy

In this article, investing in commercial property to generate regular returns is examined.

9 Takeaways for 2024 from India's Top Wellness Experts 88

by Dr. Renuka David

The Radiant Wellness Conclave, held in September 2023 in Chennai brought forth a treasure trove of ideas to transform not just your health, but also your life. This summary highlights nine key takeaways from nine experts – each on a different dimension of wellness.

Battle of Narratives – Impact of Influence Operations 92

by Lt Gen J S Sandhu (Retd)

Influence Operations are tailored actions to shape perceptions of targeted people to achieve larger political, economic, social, military or a combination of these objectives. These reflections point out the effect of dominant narratives on warfighting and national governance.

Medals and Ribbons

A SALUTE TO OUR VALIANT WARRIORS (ENGLISH QUARTERLY)

Founder and Publisher

COL DAVID DEVASAHAYAM (Retd)

Editorial Team

Chief Editor

Lt Gen J S SANDHU (Retd)

Consulting Editors

Lt Gen D ANBU (Retd)

Air Marshal HARPAL SINGH (Retd)

Rear Adm S SHRIKHANDE (Retd)

Creative Editor

Dr. RENUKA DAVID

Vice President Design and Contents

Ms NEETI JAYCHANDER

Admin & Production

Capt R G PRAKASAM (Retd)

Marketing & Subscriptions

CHANDRAVEL KANTHASAMI

Art and Designing

SARAVANAN

SHASHI BANDI

(Captions)

Photography

VIGNESH NARAYANAN

(3Leaf Studio)

Accounting Team

GIRISH SHENOY

Despatch

SUB RAJAN PODUVAL K (Retd)

ANIL KUMAR

Published By

Col David Devasahayam (Retd),

Radiant Villa,

VGP Golden Beach Phase 1,

Injambakkam,

Chennai - 600041.

Printed At

Vasan Print Mfg Co

29, Dr. Besant Road, Ice House,

Chennai - 600014.

Operations Office

Radiant Building, #28, Vijayaraghava Road,

T. Nagar, Chennai - 600017.



Lt Gen J S Sandhu, (Retd).

About three decades ago in the late nineties, I had read some of the acclaimed books of Alvin Toffler, namely **Future Shock**, **The Third Wave** and **Powershift**, wherein he spoke about the changing nature of warfare, about non-lethal weapons, and how the world was transiting from the *Industrial Age* to *The Information Age*. Undoubtedly, this is the **Digital Age**; and Admiral Karambir Singh, our former Navy Chief elaborates on “*Navigating in The Digital Age*” in his insightful article in this issue.

Taking a cue from the visionary Alvin Toffler, we too have donned “*over the horizon*” goggles and tried to gaze at the new paradigms in warfare. Shrikhande, our erudite Navy Editor looked at the trends in maritime warfare and interestingly points out that there is a continuum in warfighting doctrines and precepts - echoes and practices from the past will be visible in

the years ahead. Information warfare and influence operations are a major facet in modern war, and in my **Reflections** article I too bring out that such operations have been around in the last century too, albeit termed differently.

Notwithstanding this continuum in principles, current technologies have amplified the effects of war in several dimensions. Notably, the internet, social media, a multitude of electronic and print media have magnified the information war to effectively alter perceptions much more than the propaganda of yesteryears. Social media and Artificial Intelligence (AI) have facilitated biometric profiling and ‘*deep fakes*’ with indistinguishably similar voice, inflections, gestures, visuals and other biometric signatures. Precision targeting and computerised fire control systems coupled with better munitions have enhanced the destruction caused by bombs and missiles phenomenally. Precision targeting of Russian Commanders has also been possible due to AI-detected biometric signatures and electronic eavesdropping.

Like tigers who fight to the end to retain control over their forest turf, global powers are using all their resources to protect their wealth, while the emerging powers are using similar means to change the power equations. The result is **Unrestricted Warfare**, using all means, all dimensions. In ancient times, Chanakya too had advocated using all tools by

the King to retain and expand his kingdom – “*Sam, Daam, Dand, Bhed*”. But, in future the ‘**Unrestricted**’ philosophy would cause far more death, destruction, mayhem and violence to the human race than the ancient era. New unregulated threats like bio-terror, space assets denial, use of irregular “*Private Military Contractors*” would result in humanitarian anguish – akin to barbarism. We have seen a trailer of sorts in the Israel-Hamas conflict. We have discussed these dangers in this issue.

Technology has a tremendous impact on warfare. The massed phalanx of Roman Armies had to disperse under the onslaught of firearms and artillery. In future, drone swarms can annihilate an infantry attack, just as sea drone swarms can damage destroyers, cruisers and carriers. So it is imperative for the Young Officers and leadership of our Armed Forces to absorb the technological threats unfolding. Computing, communications, situational awareness, decision disruption, personal protection are some of the features being impacted, as brought out in some of the articles hereafter.

The translation of the ‘*disruptive technology*’ to a usable product is a key imperative. The Navy has worked on this roadmap in the last couple of years, setting up an effective organisation called Naval Innovation and Integration Organisation

EDITOR'S NOTE



(NIIO), created a project with acronym SPRINT, and delivered the *'technology to product and procurement'* baby on a fast track. While we have profiled this initiative in this magazine, I must also state that similar ventures are taking place in the other two Services too. The North Tech Symposium is one such platform where usable products are showcased, and procurement is initiated. I have included a short report on this Symposium.

The Chinese have followed the dictum *"winning without fighting"* for centuries. Visionary leaders realise that **Force** has unwanted repercussions, without any assurance of victory. Major General H Dharmarajan deliberates on the *Nuanced Use of Force in Indian Statecraft* in the decade plus after our

independence; he indicates that the stick was used sparingly, but effectively in the princely states and in Goa too. He also elucidates that diplomacy without a matching **Force** presence may not be adequate to protect the national soil.

In future, non-kinetic means to achieve policy objectives would be preferred, vis-à-vis the use of force. **"This is not the era of war"** was the wise counsel of our Prime Minister to President Putin. Alternative non-kinetic methods may have given Russia better dividends in Ukraine. Yet kinetic conflicts are not a thing of the past. Wars have been a part of history and will occur in times to come; the Israel - Hamas conflict is a case in point, and Palestinian - Israeli wars are likely to repeat. But powerful nations tend to achieve their national interests without going to war, while remaining ready for war. Our Armed Forces likewise must remain battle ready.

On 16 September 2023, we had a lively day in Chennai during the Radiant Wellness Conclave. Dr Renuka David, who helms the Conclave has covered the splendid interactions with eminent persons that day in our Wellness Section. Also, while in service,

we generally invest in residential property, but our financial guide points out in the Money Matters column that investment in commercial real estate is far more lucrative. Our readers should consider such an option seriously when planning to buy property.

A friend sent me a photo of our **Medals and Ribbons** magazine on the magazine rack at RIMC, Dehradun (see image alongside). I was glad to see that the next generation is getting a positive insight into the Armed Forces, and we have been sending complimentary copies of the magazine to many schools. Like RIMC, several schools are subscribing to the magazine too; and we look forward to more subscriptions.

In the next April 24 Issue, we plan to focus on contemporary conflicts like the Russo – Ukraine War, the Israel – Hamas conflict, the Yemen War, civil strife in Sudan, the internal violence in Myanmar and such current confrontations. We look forward to interesting reports on these operations; the articles may be sent to chiefeditor@medalsandribbons.com by 05 February 2024.

Many of us are not tech wizards and may not gel with the professional and technical orientation in this Issue. We have however tried to put across the content in layman terms, and hopefully the readers will find them interesting enough – remember these articles will give you an insight into what the future may throw up. If we face a technological gap, we would find ourselves at a loss in battle. **So, let us be ready for the next war, and not think like the last war!**

We look forward to your earnest feedback. The Editorial Team thanks all the readers for your valuable support and your positive kudos, which has enabled us to record and enhance the glory and pride of the Indian Armed Forces.





The Indian Tricolour flutters over The Citadel in Panjim, Goa for the first time in December 1961.

NUANCED USE OF FORCE IN

INDIAN STATECRAFT

(The First 15 Years Post-Independence)

Much has been analysed in recent times of the evolution of India's foreign policy over the last seven-and-a-half decades. Notwithstanding, in the practice of statecraft, only a few have covered the role that the instrument of **"the military"** may have played, especially when only subtly influencing decision-making from a recessed backdrop. This article covers the first 15 years after India stepped into the comity of Nations, post attaining independence in 1947.

Buttressing diplomatic dealings with the capability of the Armed Forces, be it either as a comforting asset or as a looming threat in the shadows, has been witnessed many a time, but seldom spoken of. There are instances too where force as an instrument of statecraft has had unintended consequences on foreign affairs.

There are as many as 202 Indian Diplomatic Missions¹ all over the globe today, and most practitioners of foreign policy would agree that a resident defence attaché (DA) in the mission adds considerable heft in multiple ways. But with much less than half that number of Indian DAs all over the world today, it is probably the absence of a DA, or leaving it only to a distant accredited attaché from elsewhere that leaves an Ambassador feeling less empowered. Yet such a statistic cannot throw much light on the connect between latent force and Indian foreign policy, and one can do better by going back 75 years to chart the course of this relationship.

¹ "Admiration at Home Respected Internationally," *New India Samachar*, Vol 2, Issue 24, Jun 16-30, 2022, p.21.



His Highness the 14th Dalai Lama (third from right) during his escape from Lhasa, after entering the Tawang Region in Arunachal Pradesh, 31 March 1959 (photo courtesy dalailama.com/pictures/escape-into-exile)

The Prelude

At its inception in 1947, India emerged onto the global stage as a champion of non-violence. This is not in any way to state that the power of the Indian military had not been felt anywhere around the world. On the contrary, by mid-1945, a humongous strength of more than 2.6 million² Indian soldiers had contributed to the Allied cause during World War-II through the British Indian Army, as the largest-ever volunteer force. There were glowing tributes for the stellar acts of Indian gallantry flowing from all over. Not just the handful of Victoria Crosses, George Crosses or Military Crosses, the “**unknown Indian soldier**” had proven that fearsome warrior within the Indian spirit far more than those formally recognised by the British Raj. While a lot may be attributed to the strategy of non-violence, one can incisively discern the unseen pressure of force behind many a tactic of “*silently suffering*” that was presumed to achieve the desired ends. Numerous protests that

eschewed violence were not taken seriously at all, especially in the inter-war years. When payoffs of adopting only passive resistance were negligible, it appeared unviable for followers to undergo extreme hardships under the oppressors.³ An unseen hand of “*force*” seemed to emerge from the background.

A case in point is that not long after the end of the World War-II, what blew up within India was the Royal Indian Naval Mutiny and that of the Royal Indian Air Force uprising, both of which erupted in 1946. Though not quite actively supported by the Indian political leadership then, these appear to have contributed in substantial measure in shaking the British confidence to continue to rule India.⁴

The possibility of another large mutinous 1857-like situation seems to have caused a catalytic acceleration towards a negotiated settlement. The shadow of force silently precipitated what was achieved by the political leadership thereafter. **Force as an instrument, though not in the political forefront (more downplayed by the British themselves) had already played a role in London’s decision to exit from India.**

The situation in the context of force and military affairs was rather complex in the run-up to 1947. Defence matters at the time of Partition⁵ continued to be controlled largely by the British. While General Cariappa took over as Army Chief only in January 1949, the Navy and Air Force continued to be led by British officers for several years later. The partitioning of the British Indian Army with the apportionment of the various regiments, the armament as well as the ordnance between India and Pakistan was subjected to innumerable pulls and pressures.⁶ The endeavour to acquire more military force by both the newly formed states was pronounced.

In September 1947, Indian diplomats were lobbying hard for a non-permanent seat for India on the UN Security Council.⁷ While the

² “Indian Army Website, History: World War-II, <https://indianarmy@nic.in>.

³ Freedman, Lawrence, “Strategy: Chapter 23: The Power of Nonviolence”, Oxford University Press, New York, 2013, ISBN 978-0-19-932515-3, pp.354-364.

⁴ Malhotra, Iqbal, “Dark Secrets”, Bloomsbury India, 2022, p.122-123.

⁵ Bhagwati, Jaimini, “The Promise of India”, Penguin Random House India, 2019, p.xxviii.

⁶ Rao, P.V.R., “Defence without Drift”, Bombay Popular Prakashan, 1970, p.6-7.

⁷ Memorandum of Conversation, by Mr. Theodore C. Achilles of the United States Delegation Staff of Advisers, Office of the Historian, accessed at <https://history.state.gov/historicaldocuments/frus1947v01/d84>.

West was voting for Canada, and the Arabs for India, yet Ukraine was considered a 'safer option' by many of the 57 voting nations in the UN General Assembly at that time. In eleven rounds of contestation, India lost to Ukraine in all of them and eventually had to withdraw its candidature for the UN Security Council in the twelfth round of voting.⁸ Soft power alone at that nascent stage had little weight.⁹ There was considerable uncertainty too as to how India would chart its course, and it was not until the next election that India joined the UN Security Council in 1950.

The vesting of one single Supreme Commander for both India and Pakistan under General Auchinleck, ensured that every effort was made to restrain the use of force. British officers in the two post-partition armies were given stand-down orders to prevent getting embroiled into the calls of the nationalists who were seeking to use force against each other on either side of the Radcliffe Line. While the combat ratios of the partitioned military weighed heavily in favour of India in 1947, force which could have tipped the decision, was partly withheld. Governor General Mountbatten at this stage played a substantial role in urging India to take the Kashmir issue to the UN, leading eventually to a UN-brokered ceasefire. There were attempts made by India in 1948-49 to acquire Sherman tanks of World War-II vintage from the USA during the Kashmir operations, which did not materialise till 1950.¹⁰ Influence from the international environment to rein in the Indian use of force eventually resulted in the unfinished agenda of partition.

Contours of 'Force' during Consolidation

In the context of the princely states that had been given an option to merge or to remain as an independent nation, the

Nawab of Junagadh had initially decided to join Pakistan. While disregarding the contiguity principle, the Nawab also attempted to force the smaller border principalities like Babariawad and Mangrol to renounce their accession to India. This provoked a call by Sardar Patel to order the Indian Army to secure Babariawad, after legally obtaining clarity regarding its Accession. With the heightened tensions that followed, including the Indian Navy ferrying troops and securing the coast, the Nawab fled with his family to Pakistan in October 1947. The plausibility of use of force evidently facilitated a breakthrough.

During the September 1948 annexation of the princely state of Hyderabad, despite the intransigence of the Nizam, and his weak force levels, India's first Defence Minister Mr Baldev Singh was given explicit instructions not to let the mobilisation of the Indian armoured brigade be misconstrued as an indicator of aggression. While there were other considerations to portray it a law-and-order police action (particularly to preclude another communal mayhem), the aim of Operation Polo was eventually achieved, albeit with limited use of the Army over a week-long duration of fighting.

These instances were significant pointers of how the blunt instrument of

a mobilised military was employed. But the decade that followed saw such abrasive employment recede into oblivion, with direct military power becoming more latent and benign in its form. This was the phase when India was making a conscious effort in the post-colonial era to downplay the use of force in external affairs. The focus was to ensure that democracy got well embedded,¹¹ with the Indian Armed Forces being kept at as much as an arm's length, as was feasible (*so as not to follow the path of what happened across the international boundary in Pakistan*). The stated objectives were to nurture peace through a non-expansionist approach, using moral reasoning to influence adversarial stakeholders. Therefore, to employ Chanakya's sutras of clout and influence did not come to the fore prominently.

Post the stalemate in UN over Kashmir, India's adoption of non-alignment achieved considerable traction, and the need for adoption of any coercive measures appeared to recede. The Army's strength was targeted to be reduced towards 200000 after the 1948 Territorial Army Act attempted to retain only a nucleus instead of full fighting units. Despite the concerted efforts at military downsizing, Indian foreign policy was

⁸ *Securing between 22 to 29 votes, India lost eleven consecutive rounds of voting to Ukraine for a place in the UN Security Council in 1947 as a non-permanent member. Accessed at the UN Security Council website <https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Elections%20Table%201946-2018.pdf>.*

⁹ Bhagwati Jaimini, *The Promise of India*, Penguin Random House India, 2019, p.29.

¹⁰ Subrahmanyam, K., "Arms and Politics," *Strategic Analysis*, Jan 2005, Volume 29, Issue 1, Manohar Parikkar Institute of Defence Studies and Analysis. The Indian Defence Attaché sought Shermans from the US Secretary of Defense. Accessed at https://www.idsa.in/strategicanalysis/ArmsandPolitics_ksubrahmanyam_0305.

¹¹ Das, Gurcharan, "A Story of Private Success and Public Failure," *The Times of India*, Delhi Aug 20, 2022, p.20.



Panchsheel Agreement signed in Beijing between India and China in April 1954 (photo credit organiser.org)

catapulted to the global centre-stage in the early 1950s even as the Cold War competition began to immerse the international arena. Be it its prominent role of chairmanship of the Neutral Nations Repatriation Commission in Korea, the Geneva Conference on Indo-China after the French defeat, participation in UN peacekeeping operations or as the founding member of NAM, India came to the fore with its idealism, without much reflection of its military power. Eschewing force in statecraft seemed to gain considerable traction at that time.

Diplomacy Diluted by Minimised Muscle

With non-alignment and retaining strategic autonomy as a cornerstone of India's foreign policy,¹² the Cold War development of Pakistan joining SEATO and CENTO in 1954-1955 nudged Indian defence entities to seek technology and capability. An offer from the Soviet Union in 1954 for providing military equipment to India (even before it was offered to

AN-12 transport aircraft from the Soviet Union.¹⁶ Endeavours by the Indian industry to develop its own fighter aircraft which began in 1957 in concert with the German aviation engineer Kurt Tank¹⁷ got little traction from abroad. On the other hand, acquisition of 54 British-origin Canberra bombers (including photo-reconnaissance) concluded in the same year, continuing Indian dependency on the UK defence industry.

The decline in the overall defence allocations, alongside the peace overtures of Panch Sheel let China take an upper hand, be it its assertion in Tibet, or its cartographic aggression by continued publication of distorted maps of disputed areas. India had referred to these maps as early as in October 1954 and later again during Zhou Enlai's visit to India in 1956.¹⁸ Even as China announced the completion of Sinkiang-Tibet

Egypt) was turned down on the pretext of remaining non-aligned. At this time, India was extensively dependent on the UK for supplies of equipment and technology,¹³ while Pakistan had developed defence ties with both the UK as well as the US.¹⁴ It was not surprising that London snubbed a feeble Indian bid to acquire modern submarines, while the US turned down the request for expensive F-104 fighter jets, even on full payment.¹⁵ There were some limited but diversified procurements from different nations in this decade, be it aircraft like Mystere fighters, Alize, Alouette helicopters from France, 106mm Recoiless Guns and Fairchild Packet aircraft from the USA, and later Mi-4 helicopters and

¹² Shivshankar Menon, "Seventy Five Years of Indian Foreign Policy: Key Successes, and the Gaps That Still Remain," 15 August 2022, accessed at <https://thewire.in/diplomacy/seventy-five-years-of-indian-foreign-policy-key-successes-and-the-gaps-that-still-remain>.

¹³ Bhagwati Jaimini, "The Promise of India," Penguin Random House India, 2019, p.31. There were naval vessels, Hunters, Sea Hawks, Gnat aircraft (besides Canberra bombers), and Centurion tanks procured from UK, besides collaboration with public sector entities like Bharat Electronics Limited for licensed manufacture.

¹⁴ "Foreign Relations of the United States," Office of the Historian, Department of State, USA, accessed at <https://history.state.gov/historicaldocuments/frus1952-54r09p1/d107>

¹⁵ Bhagwati Jaimini, "The Promise of India," Penguin Random House India, 2019, p.41.

¹⁶ Subrahmanyam, K., "Arms and Politics," Strategic Analysis, Jan 2005, Volume 29, ibid.

¹⁷ Dr Kurt Tank, a German, was the chief designer of HF-24 supersonic fighter aircraft under the aegis of HAL. Accessed at https://archive.pib.gov.in/archive/ArchiveSecondPhase/DEFENCE/1961-JAN-DEC-DEFENCE/PDF/DEF-1961-06-24_322.pdf.

¹⁸ Banerjee, DK, "Sino-Indian Border Disputes," Intellectual Publishing House, New Delhi, 1985, p.10.

Road through Aksai Chin, increasing violent incidents on the border with China caused considerable embarrassment in the second half of the 1950s. Despite the prospect of escalation, the Indian defence spending was only 1.87% of the GDP with an average growth rate of only 2.8% in that period. From a lion's share for defence of more than 30% of the central government spending in 1950-51, the allocation had plummeted to 15% a decade later.¹⁹ Indian foreign policy in the latter half of this decade continued to hinge on idealistic foundations while lacking credible military backing to shift towards a realist outlook.

The downing of an Indian Canberra on a photo-reconnaissance mission over Pakistani territory by PAF's American-origin Sabre F-86F jets in April 1959²⁰ reflected the adversary's benefit with better state-of-the-art technology from a strategic alliance. A little more than a year later, Pakistan under General Ayub Khan, partnering with the US, secured for itself a generous share of the Indus Waters in September 1960. It was around this time that the India-US Atomic Energy Cooperation was gaining ground for development of the first nuclear power reactor (Tarapur) in India.²¹

Further in the domain of defence capability acquisitions, the contract for the first aircraft carrier INS Vikrant was concluded with the UK in 1957, albeit with reduced capabilities. It was not the best of major defence investments that could bolster security against a developing land threat from the Northern borders in that era. However, its delivery in 1961 did give a fillip to the image of the Indian Navy, and developed that element of confidence in the leadership to coerce the Salazar Regime in Goa to buckle under the threat of force.²² The apprehension that any NATO forces may come to the aid of the Portuguese in Goa was adequately put to rest (as being

out-of-area)²³ before action was initiated. While there was no direct participation of INS Vikrant in the sinking of the Portuguese frigate Afonso de Albuquerque, nor in the limited air strikes prior to the liberation of Goa in December 1961, assertive diplomacy had been strengthened by military muscle. While the USSR, Arabs and African nations supported the action, the US, the UK and a few others condemned the Indian action. China remained ambivalent, generically supporting the oppressed colonies against the imperialists. However, the Chinese Communist Party (CCP) did particularly note the Soviet veto of the West-sponsored UN Resolution that sought the withdrawal of the Indian forces from Goa.

India-China: Cooperation to Confrontation – Calibration of “Clout”

Along the Northern Borders, China appeared to tackle its “status rivalry” with India throughout the 1950s by adjusting its policies to keep India non-aligned, and to keep its mutual border disputes as bilateral.²⁴ India was one of the earliest countries to recognise the founding of the People's Republic of China in 1949, and in the mid-1950s an outlook prevailed at Delhi that China was closer to India than to either of the Super Powers. The 1954 India-China Agreement on Tibet appeared to resolve China's apprehensions regarding India's support to the US stirring trouble in Tibet. Numerous moves were made by the CCP leaders such as the Afro-Asian solidarity in the Bandung Conference (1955) to ensure that India neither got closer to the US nor to the Soviet Union.

Later, as bilateral issues including the Aksai Chin and Tibet came to the fore, China started taking note of the visits to India of Soviet leaders like Khrushchev in 1955, or of the US President Eisenhower to Delhi in December 1959, as well as the repeated visits of Indian leaders to the USA, slowly envisioning the formation of a strategic triangle against itself.²⁵ To counter this development, the CCP leadership deliberately extolled “China-India Friendship” in 1959, while conciliatory notes to New Delhi were sent out by Mao and later by Zhou Enlai during his visit in April

¹⁹ Rao, P.V.R., “Defence without Drift,” *Bombay Popular Prakashan*, 1970, p.5.

²⁰ Philip, Snehash Alex, “Untold story of an LAF Canberra & its crew, 60 years before Wing Commander Abhinandan's MiG,” 26 April 2019, *The Print*, accessed at <https://theprint.in/defence/untold-story-of-an-iaf-canberra-its-crew-60-years-before-wing-commander-abhinandan-mig/227141/>.

²¹ “Foreign Relations of the United States: 1958–1960, South and Southeast Asia, Volume XV,” Office of the Historian, Department of State, USA. Accessed at <https://history.state.gov/historicaldocuments/frus1958-60v15/d249>.

²² Mendes, Sushila Sawant, “Goa Remained a Portuguese Colony when India Became Independent,” *The Wire*, 17 Aug 2022, <https://thewire.in/history/goa-remained-a-portuguese-colony-when-india-became-independent>.

²³ Pöllath, Moritz, “Far away from the Atlantic: Goa, West New Guinea and NATO's out-of-area policy at Bandung 1955,” *Journal of Transatlantic Studies*, 11:4, Dec 2013, pp. 387-402.

²⁴ “India-China Bilateral Relations.” More high level visits were undertaken by China to India (by President Zhou Enlai) than by India to China. Accessed at <https://mea.gov.in/Portal/ForeignRelation/China-January-2012.pdf>.

²⁵ Gokhale, Vijay, “China's India Policy: Lessons for India-China Relations,” *Carnegie Endowment for International Peace*, Dec 2022, https://carnegieendowment.org/files/Gokhale_Chinas_India_Policy3.pdf. China was particularly concerned after the flare up by the US in the Taiwan Straits in 1958, Khrushchev's visit to Washington in Sept. 1959 (prior to the US President's visit to Delhi), and the spat between Khrushchev and Mao Zedong in Beijing in Oct. 1959. Later, even Brezhnev visited Delhi as the CPSU President in 1961.



The Portuguese Frigate Afonso de Albuquerque in 1961

1960. For China, any war-fighting ability for India, be it offered by the big powers, or that sought by India, was a matter of concern, considering the developing geopolitical milieu at this stage. The US President Eisenhower had offered to equip six divisions of the Indian Army, akin to what had already been given to Pakistan (this offer was turned down). Early in 1962, the Indian Air Force (IAF) was on the lookout for a supersonic fighter aircraft²⁶ and had shortlisted what was on offer, the British Electric Lightning, the US F-104A Starfighter, the French Mirage and the Soviet MiG-21. However, while the MiG-21 deal was sealed in 1962, the first aircraft were eventually inducted into the IAF only in 1963. Notwithstanding, some military material did start flowing prior, in 1961 itself. The CCP leadership at Zhongnanhai observed with concern that the Soviet supplied helicopters and transport aircraft were being used along the Sino-Indian border.²⁷

Going back to March 1959, when the Dalai Lama and his followers fled from Lhasa, and were granted asylum in India, the widespread sympathy for Tibet in India

enraged the Chinese,²⁸ further aggravating the boundary question. Resorting to military coercion, the PLA's (People's Liberation Army) response of escalating tension resulted in skirmishes between Indian troops and the PLA, be it at Longju (August) or Kongka Pass (October) in 1959. Chinese transgressions into Indian territory had already been occurring periodically even in the period 1954-58 at numerous places viz. Khurnak Fort, Hupsang Khad, Kurik, Barahoti, Laphthal, Walong etc.²⁹ Conversely, this appeared to bring forth more support at the politico-strategic level for India, both from the USSR as well as the USA.³⁰ Soviet leader Khrushchev's public admonishing of Mao Zedong at Beijing in October 1959 for these escalations,³¹ besides the positive overtures from the American quarters during the US President's visit to India afforded a comforting sense of complacency to the dispensation at Delhi. Misconstruing the success of these diplomatic initiatives, India's adoption of the **"Forward Policy"** in 1961,³² a seemingly unsustainable military posture, was a classic case of foreign policy dictating army's operations. Despite the lack of suitable

²⁶ Tiwari, Saksbi, "Battle Of Supersonic Warplanes – How IAF's 'Much Criticized' MiG-21 Fighters Destroyed US- Origin Jets In A Clash Over Indian Subcontinent," 03 April 2022, <https://www.eurasiantimes.com/iaf-mig-21-fighters-destroyed-us-origin-jets-used-by-pak-air-force/>.

²⁷ Cable from the Chinese Embassy in India, 'Overview of India's Foreign Relations in 1961,' 01 January 1962, Wilson Center Digital Archive, <https://digitalarchive.wilsoncenter.org/document/cable-chinese-embassy-india-overview-indias-foreign-relations-1961>.

²⁸ "Foreign Relations of the United States, 1958–1960, China, Volume XIX," Office of the Historian, Department of State, USA, accessed at <https://history.state.gov/historicaldocuments/frus1958-60v19/d382>.

²⁹ Arpi, Claude, "Chinese Incursions: 60 years ago," Indian Defence Review, 21 September 2015, accessed at <http://www.indiandefencereview.com/chinese-incursions-60-years-ago/>

³⁰ Zhefeng, Hu, "Mao and the Sino-Indian Counter-attack in Self Defence," Bai Nian Chao No. 3, 1999. Mao is reported to have himself observed the growing support for India from the USSR and the USA.

³¹ Gittings, John, "The day Khrushchev and Chairman Mao saw red," The Guardian, 27 November 2001, accessed at <https://www.theguardian.com/world/2001/nov/27/russia.internationaleducationnews>.

³² Daulet Singh, Zorawar, "Nehru's Forward Policy remains a puzzle. But he had confidence in strong allies, soft power," The Print, 28 October 2022, accessed at <https://theprint.in/opinion/nehrus-forward-policy-remains-a-puzzle-but-he-had-confidence-in-strong-allies-soft-power/1185054/>.

high-altitude equipment, insufficient acclimatisation for operations in the dizzy Himalayan heights,³³ inadequate infrastructure to accommodate soldiers, or the conspicuous absence of a credible capability to logistically support such a body of troops, orders to implement a coercive posture were passed. It was more the absence of force as a strategic tool while implementing such an assertive stance, the hollowness of which made it so pronounced.

Meanwhile, the developing Indo-US military relations were being closely monitored by China.³⁴ Cooperation for a communications satellite including sharing of military intelligence, besides American support to India for the manufacture of military materials was seen from Beijing as a signature of “collusion”. China responded cautiously (to prevent a rush of support from the US and UK) with calibrated use of nuanced gestures of force at the lowest level.³⁵ That the border patrols were being conducted by the Army instead of the armed police was one early signature.³⁶ From Mao himself reasserting “armed coexistence”³⁷ along the Indo-China boundary, to investing newly established Indian posts, conveying threats to induce withdrawal, blocking routes to advance, probing to occupy dominating positions, attempting to sever logistic lines, seeking to cut communications, sounding local and diplomatic warnings, till the subsequent breakout of hostilities, practically every step in the book seemed to be invoked to push towards a negotiated settlement. Quite the contrary happened, with each nuance of force being perceived as a bellicose provocation, deliberately intended to escalate. **The rest is history, for the war unfolded in October 1962, as a continuum of the force in statecraft spilling across the tipping point.**

Epilogue

In the Indian sphere of influence, the first fifteen years post-Independence witnessed many a subtle use of force by the statesmen at the helm. It was a formative phase, in which many different arrows in the quiver of the strategist were tested, albeit with varying outcomes. Much of the decision making at that time may be seen on the broader canvas of the goings-on in the neighbourhood where in analogies of success or failure could be inferred. Yet one aspect emerged poignantly, that the practitioner of foreign affairs was inextricably enmeshed with what the military contributes towards the larger interest. As Clausewitz put it, war (sic. Force) is more of a political instrument, and a continuation of the political intercourse by other means.

³³ Jba, Prem Shankar, “What China Means When It Says India Needs to ‘Remember the Lessons from History’,” *The Wire*, 06 July 2017, Accessed at <https://thewire.in/diplomacy/china-india-war-19>.

³⁴ Cable from the Chinese Embassy in India, ‘Overview of India’s Foreign Relations in 1961,’ 01 January 1962, Wilson Center Digital Archive, accessed at <https://digitalarchive.wilsoncenter.org/document/cable-chinese-embassy-india-overview-indias-foreign-relations-1961>.

³⁵ Maxwell, Neville, “China’s India War: How the Chinese Saw the Conflict,” May 2011, accessed at <https://chinaindiaborderdispute.files.wordpress.com/2010/07/neville-maxwell-chinas-india-war.pdf>

³⁶ Subramaniam, Arjun, “India’s Wars: A Military History Wars 1974-1971,” Harper Collins Publishers India, 2016, p.214.

³⁷ “You Wave A Gun, And I’ll Wave A Gun’: Mao.” *Outlook*, 05 Feb 2022, accessed at <https://www.outlookindia.com/magazine/story/you-wave-a-gun-and-ill-wave-a-gun-mao/282573>



Major General H Dharmarajan, an alumnus of the Rashtriya Indian Military College, Dehradun was commissioned into the Corps of Engineers in 1986. Renowned for his intellectual insights, Dharmarajan has written articles for many professional journals. Besides winning the COAS Gold Medal Essay Competition, he has also won awards while attending training courses at National Defence College, National War College, Washington DC, Defence Services Staff College, College of Military Engineering and National Defence Academy. He has commanded a division along the Line of Control in the Jammu Region, and is presently commanding Bengal Sub Area.



Maj Gen H Dharmarajan

NAVIGATING THE DIGITAL AGE

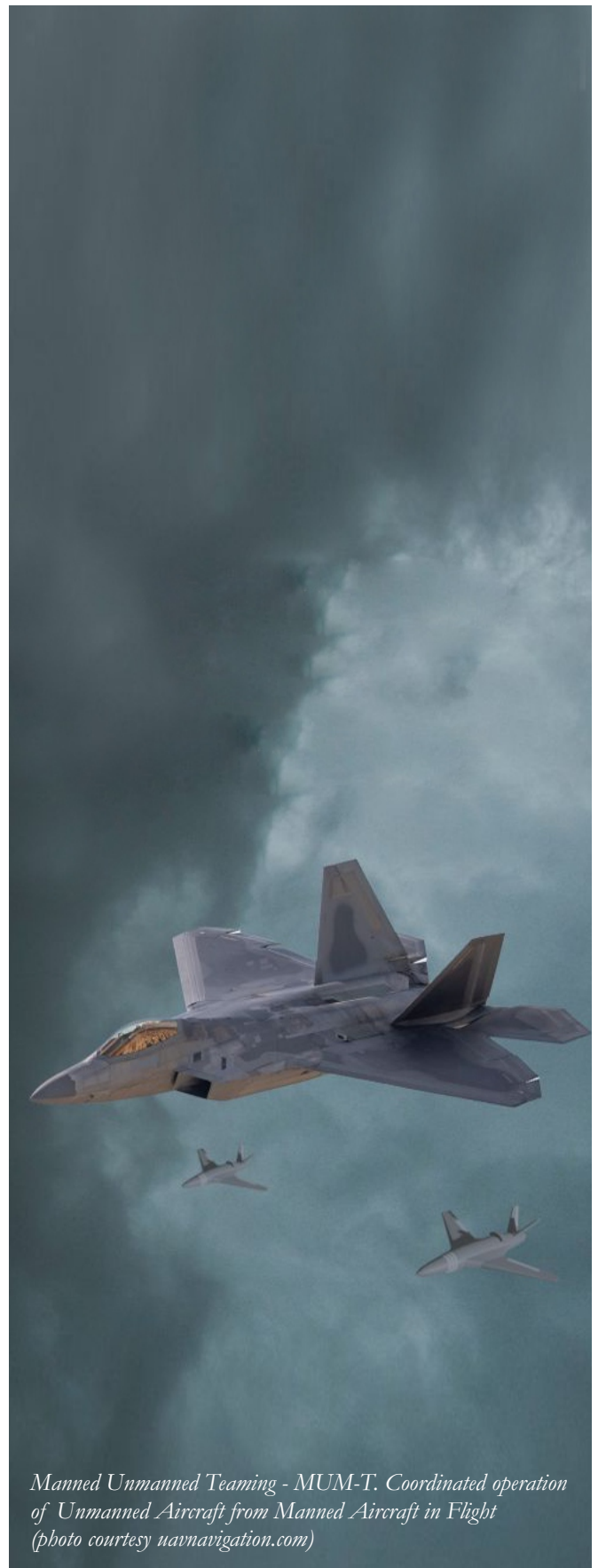
We stand at an inflection point between the Industrial Age and the Information Age. The transformation is profound and far-reaching.

Digital technology, once a mere aid in traditional warfare, has now become its backbone, offering precision and sophistication previously unimaginable. Our former Naval Chief elaborates.

Evolution of the Digital Landscape

The race in technological advancement is no longer led solely by defence technologies. Commercial technology has overtaken these, becoming a crucial asset to supplement, and sometimes replace, traditional defence mechanisms. This shift is not limited to the world's superpowers; it is accessible to the smallest of actors, levelling the playing field in unprecedented ways.

The conflict in Ukraine showcases this new era starkly. Drones, augmented by digital tools like Artificial Intelligence (AI), sensors, and space technology, have been used with striking effectiveness. A notable example is Elon Musk's Starlink satellites that played a pivotal role in the Ukraine conflict, showcasing how commercial digital technology can supplement traditional weapons systems. These off-grid, high-bandwidth internet connections, accessible via small dishes powered by car batteries, provided a crucial C3I (Command, Control, Communications, and Intelligence) network for Ukrainian forces. Starlink's low latency and resilience against jamming made it a game-changer in the conflict. Similarly, Israel's confrontation with Hamas in the Gaza Strip in 2021, labelled the "*world's first AI war*", represents another frontier of this evolution. AI technology, analysing radar detections, played a critical role in guiding the Iron Dome Air Defence system to intercept some 4000 rockets in 11 days. It's a different matter that Hamas managed to overwhelm this system on 07th October 23 by firing almost 5000 rockets in a span of 20 minutes. The solution for this too, however, would emanate from the realms of digital technology and is being fielded as we speak, in the form of the Laser Dome.



Manned Unmanned Teaming - MUM-T. Coordinated operation of Unmanned Aircraft from Manned Aircraft in Flight (photo courtesy uavnavigation.com)

In the digital age, information flows with the speed of thought, and its manipulation for strategic purposes has become a commonplace tactic, as observed in the Ukrainian conflict. Cyber warfare has emerged as the new battleground, with nations like China investing heavily in these technologies. Cyber-attacks originating from China, during Nancy Pelosi's visit to Taiwan, targeting the Taiwanese President's Office, Foreign Office, defence networks etc., highlight the profound impact of this new warfare domain. Interestingly these attacks primarily affected those networks that had Chinese origin software or devices.

Adapting to Digital Challenges : A Leadership Perspective

In this rapidly changing digital landscape, traditional military structures and strategies, rooted in the industrial age, are no longer sufficient. To outcompete adversaries, the Navy must be digitally adept, embracing innovative, swift, and decisive actions. This necessitates a new kind of leadership – one that is not only adept at navigating these changes but also capable of driving them, even if it means being disruptively innovative. Change, in this context, is not merely about seeking new answers to old questions. It's about altering the very nature of the questions we ask. It's a paradigm shift from conventional thinking to a mindset that embraces the potentials and challenges of the digital age.

In an era marked by rapid digital advancements, the strategies of naval leadership are evolving to meet new challenges and seize emerging opportunities. The question at hand is how to adapt and capitalise on these changes in the evolving digital landscape.

Rethinking Force Structuring : The Maritime Kill Web

Let us first consider Force Structuring.

Traditionally, naval force structuring has been viewed through a platform-centric lens, focusing on tangible assets like say a 200 ship, 450 aircraft navy. However, this perspective requires a fundamental shift. Imagine the digitally enabled Navy of the future as a complex maritime **'kill web'** - an intricate network seamlessly processing and acting on vast amounts of data through an interlinked system of data links and communication systems. In this envisioned future, ships, submarines, aircraft, space assets, cyber capabilities, unmanned systems, and weapons are not standalone entities. Instead, they are nodes or connectors in an ever-evolving, sophisticated network. This is the essence of network centrality, a concept now made possible by the digital revolution.

When acquiring new platforms, naval leadership must ask how these assets will augment the **'kill web.'** Platforms like P8 aircraft, High-Altitude Long Endurance (HALE) systems, or MH60R helicopters should not be seen merely as maritime reconnaissance or anti-submarine warfare tools. They must be integrated parts of a synergistic family of naval systems. For example, could these assets act as *'combat clouds'* to provide communication redundancy for satellites? This requires equipping and networking them from the outset, rather than attempting integration later.

The concept of Manned-Unmanned Teaming (MUM-T) is another critical aspect. It's not a choice between manned or unmanned systems, but a combination of both. This approach leverages the strengths and compensates for the weaknesses of each platform. To make MUM-T work effectively, expansion in the use of networks, AI, and rapid software upgradability is essential.

Long-range precision weapons too need to be data-linked to the **'kill web,'** possibly via airborne connectors like UAVs or pseudo-satellites. This implies that acquisition directorates should not focus solely on platform-specific requirements but on integrating these assets into the **kill web**, whether they are platforms or weapons.

What should the next generation **'kill web'** look like? Should the Navy retain its existing force mix, or should it consider a more agile, distributed, and digitally



Elon Musk and the Starlink communication service played a crucial role for Ukraine in the conflict against Russia (photo courtesy firstpost.com)



Yangshan Port in Shanghai (photo courtesy www.wikipedia.com)

enabled force? The effectiveness of small, technically and digitally enabled teams, as demonstrated in Ukraine against a larger Russian force, suggests that a balanced approach might be the answer. The challenge for today's naval leadership is to structure the next generation **kill web** effectively. This would involve a blend of surface, air, underwater, space, and cyber capabilities; and leveraging AI, Machine Learning, robotics, and networks. The goal should be to achieve a fully blended warfighting capability, essential for algorithmic and digital warfare. The acquisition processes for software-heavy systems of the future differ significantly from those for traditional hardware. The iterative design approach dominates software development, necessitating a shift in design and acquisition principles. Policy changes through the Ministry of Defence are required to adapt these principles for the digital age.

Redefining Operations

In today's digital age, the battlefield extends far beyond physical territories, encompassing the cyber realm where even a port can be immobilized not by

traditional blockades, but by cyber-attacks on its cargo handling software. Naval strategy and tactics are undergoing a profound transformation, adapting to these new realities. Consider the Yangshan Port Phase 4 of the bustling Shanghai port, which is fully automated and controlled by AI and robotics. A similar situation applies to the Colombo container transshipment port, a critical hub for India's maritime traffic. A cyber-attack on these could have devastating consequences, bringing operations to a grinding halt. The recent cyber-attacks on Australian ports are also a case in point.

The traditional concept of protective cover for task forces has evolved from conventional air and sub-surface defence to cyber defence also. The U.S. Navy's practices in the South China Sea demonstrate this shift, highlighting the importance of cyber capabilities in safeguarding naval operations. Today's digital landscape is marked by strategies focused on attacking from the inside-out, targeting networks, social media, and financial institutions. The paradigm has shifted from merely guarding physical borders to also having to secure cyber and information frontiers. In this context incidents like the afore-mentioned cyber-attacks following Nancy Pelosi's visit to Taiwan and the communication and power grid blackout in Ukraine in 2014 that preceded the invasion of Crimea underscore the importance of cyber defence. Ukraine's ability to shift its government cloud outside the country in 2022 demonstrates a proactive approach to protecting critical infrastructure denying the Russians a repeat of their success in this domain in 2014.

Ukraine's exploitation of AI algorithms for transcribing Russian communications and using facial recognition to identify targets on social media offers valuable lessons. This innovative use of technology not only aided in intelligence gathering but also played a vital role in targeting key Russian military figures in the early days of the war.

Maintenance and Logistics

The Navy's shift towards digitization, starting with going paperless, opens up new possibilities in maintenance and logistics. A centralized Data Analysis Centre, like those used by commercial shipping companies, based on real time performance monitoring of each platform, could enable reliability-based maintenance, and efficient inventory management. Whilst initiatives like the Rukmini Aided Software Services (RESS) and the AI Lab at INS Valsura are steps

towards this digital transformation, there is definitely scope for further advancement.

Training and Human Resources (HR)

In an era defined by digital transformation, the Indian Navy is not only keeping pace but also innovating to stay ahead. This journey involves a comprehensive strategy encompassing training, HR and embracing technological advancements.

Training of operators and maintainers is pivoting towards modern methods like simulators, emulators, virtual reality (VR), and augmented reality (AR). This approach is exemplified by the MH60R aircrew training, where 80% of the training is conducted on simulators. It bears mention that containerised F35 and MH60R simulators are used onboard US Navy Aircraft Carriers for crew training. Such advancements ensure that personnel remain current and combat ready. The prospect of integrating AI into naval strategy and training is no longer a matter of conjecture. The potential use of AI tools like ChatGPT in staff colleges and war colleges for refining staff solutions and operational plans is a tantalising possibility. AI could soon play a vital role in war games and strategic planning.

The evolving digital landscape necessitates a shift in leadership styles, favouring distributed leadership and flatter hierarchies. Despite technological advances, it's crucial to preserve the concept of Mission Command in maritime operations. The establishment of a Digital Corps within the Navy, comprising experts in digital warfare, data analysis, coding, and network administration, is a step that is necessary towards ensuring future readiness.

Innovation

The Indian Navy has always been

proactive in embracing technology, as seen in its early initiatives like the Directorate of Naval Construction and WESEE. Recognizing the potential in the digital sphere, the Navy quickly adapted, issuing unmanned and simulator roadmaps in 2020. The setting up of the Technology Development and Acceleration Council (TDAC) and the Naval Innovation and Indigenisation Organisation (NIIO) in the same year further bolstered this approach. These developments have helped the Navy, in partnering with academia and industry to push innovation. Under the current leadership, the SPRINT initiative has catalysed innovation within the Navy. Collaborating with the Defence Innovation Organisation (DIO), start-ups, and academia, the NIIO has signed contracts for over 100 innovative products, many focusing on AI applications such as autonomous systems with IMO level 4 autonomy, autonomous weaponised boat swarms,

AI-based weapon inspections, and advanced communication and radar technologies.

Looking Ahead with Optimism

Reflecting on the journey thus far, we can remain optimistic about the Navy's ability to navigate the digital revolution. The foundation laid by visionary leaders and on-going technological advancements are steering the Navy towards a future where naval forces are not just equipped but also intellectually prepared for the challenges of the digital age.

As the Navy sails through these transformative times, its success will hinge on its ability to integrate future digital advancements into its core strategy and operations. By doing so, it will not just navigate the present but will set a course for a future where technology and tradition sail in unison.



Admiral Karambir Singh, PVSM, AVSM (Retd) was the Chief of the Naval Staff (CNS) from 31 May 2019 to 30 November 2021. An alumnus of the National Defence Academy, Khadakwasla, the Defence Services Staff College, Wellington, and the College of Naval Warfare, Mumbai, the Admiral was commissioned into the Indian Navy in July 1980. A Naval aviator of repute, he earned his wings in 1981 as a helicopter pilot and has flown extensively on the Chetak (Alouette Mk III) and several variants of Kamov helicopters. Over the four decades of his sterling service, he has commanded the guided-missile corvette INS Vijaydurg, and two of the Indian Navy's frontline guided-missile destroyers, namely INS Rana and INS Delhi. As a Vice-Admiral, he was the Director-General Project Seabird, and oversaw all aspects of the development of the Indian Navy's expansive and modern base at Karwar in India's southern state of Karnataka. He has a rich store of senior command experience and was the Flag Officer Commanding-in-Chief, Eastern Naval Command prior to taking over as the CNS.



Admiral Karambir Singh

SPACE MILITARIZATION AND WEAPONIZATION

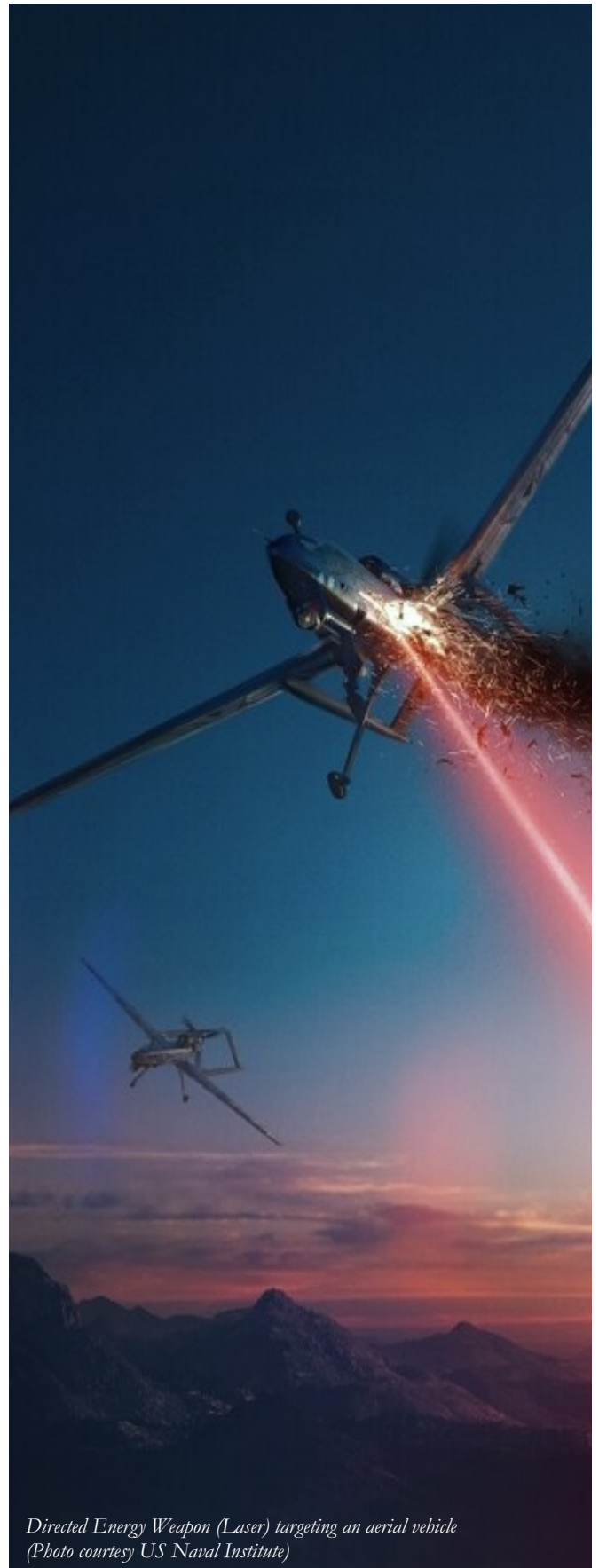
IMPLICATIONS FOR INDIA

Space has rightfully been identified as the fourth dimension of warfare after land, sea and air. As President Lyndon Johnson stated in the 1960s, **"Control of Space means Control of the World".**

The unique vantage point of space provides unmatched intelligence gathering opportunities and global communications that are pivotal in modern military operations. Understanding the evolving dynamics of space militarization and weaponization is thus critical.

The notion of utilizing the '*high ground*' of space for military advantage took root in the 1950s at the end of the Second World War when humans made their first foray into space with the Soviet Union's launch of the world's first artificial satellite **Sputnik-1**. This triggered the Space race between the two Cold War rivals, as space increasingly became the new frontier for missile technology and nuclear deterrence strategy. Subsequent decades saw both the Soviet Union and the United States make advances in spy satellites and anti-satellite (ASAT) weapons as they viewed supremacy in space as vital for security interests. This period saw the rise of the Strategic Defence Initiatives (SDI) or **"Star Wars"** by the USA, this was primarily a concept of Ballistic Missile Defence (BMD) to locate the launch sites of the Soviets and thereafter neutralize the missile with space-based or ground-based assets. This period also saw the development of early ASAT weapons by these two powers.

The military value of space in enabling precision strike capabilities was convincingly demonstrated during the first Gulf War in the early 1990s. America's Global Satellite Positioning



*Directed Energy Weapon (Laser) targeting an aerial vehicle
(Photo courtesy US Naval Institute)*

System (GPS) assisted precision-guided munitions while communication satellites enabled commanders to direct forces in real-time. Similar leverage of satellite assets was noted in NATO's war campaign in Kosovo, later that decade. This heralded an era where space-based force enhancement functions underpinned modern military doctrine.

Contemporary security challenges in the 21st century's Information Age necessitate even greater reliance on space for intelligence insights, navigation accuracy, robust communications and early missile warning. Currently over 90 countries have some presence in space, with private sector innovation also bolstering access. But this has raised concerns on the weaponization of space potentially fuelling arms races and being counterproductive for sustainable space presence. Assessing the likelihood, implications and mitigation avenues for space warfare threats is thus an imperative.

Space weaponization is the process of placement of weapons in outer space or on heavenly bodies. It also involves the creation of weapons that will transit outer space or simply travel from earth to attack or destroy targets in space. The weaponization of space is different from the militarization of space. Militarization of space includes the usage of space-based assets for command, control, communication, surveillance, and reconnaissance activities.

As national security priorities motivate fresh investments in defensive space control capabilities as well as potential offensive counter-space weapons, historical lessons underscore the need for international norms and risk mitigation protocols. So, let us examine the undercurrents, debates and future policy choices available as humanity stands at the threshold of weaponization of space.

Emerging Space Threats & Countermeasures

The Gulf War in 1991 marked a pivotal juncture demonstrating the force multiplier effect of leveraging space assets, which has subsequently become vital in modern military operations. America's GPS satellites provided precise geo-location enabling smart munitions like cruise missiles to strike Iraqi targets during Operation Desert Storm. Communication satellites like DSCS facilitated robust command and control links between dispersed coalition forces across the Middle East theatre.

Space support has remained crucial in post-Cold War era conflicts. Detailed satellite imagery assisted target identification and battle damage assessment for air strikes. More recently, the on-going Russia-Ukraine conflict has seen extensive use of commercial satellite services by Ukrainian forces. **SpaceX's** Starlink Low Earth Orbit (LEO) constellation is delivering broadband internet to augment wartime communications. High-resolution earth observation data from companies like Maxar has assisted intelligence analysis (locate, detect and neutralize), while geospatial intelligence firms like Planet Labs etc. provide daily satellite imagery aiding tactical decisions.

This war has clearly defined two factors-

- The next wars will start in space with both adversaries trying to neutralize each other's assets and capabilities. This was very apparent from the Russian attempt to target VSAT terminals in Central Europe just a day prior to the war.
- Secondly, private commercial players providing force enhancing capabilities such as Starlink and Maxar

or Hawkeye have become new players in the future wars and hence neutralizing of such civilian assets in future may become 'Kosher'. Russia did announce its intention of targeting Starlink assets, but possibly did not do so because of lack of capability or not wanting to escalate the war to another dimension. However, in future civilian space assets, which, by their dual nature, can be used by militaries may become acceptable military targets.

While satellites have become pivotal for military and economic functions, adversaries are developing capabilities to disrupt, degrade or destroy space assets. Counter-space weapons employ kinetic physical attacks as well as non-kinetic methods like electronic warfare and cyber intrusions to neutralize satellites.

Kinetic weapons directly damage or demolish satellites through impact, explosion or directed energy. Missile-launched interceptors, air-launched missiles as well as ground-based ASAT lasers come under this category. Co-orbital weapons like Russia's suspicious 'Kosmos' inspection satellite also introduce proximity threats that can channel kinetic attacks using robotic arms.

High-powered microwave beams and radiofrequency jammers are being tested by China to disrupt satellite electronics in a non-kinetic fashion. Similarly, spoofing trusted signals to misdirect satellite positioning, communication or data transmissions can achieve adversarial aims. The US reports instances of GPS signal spoofing disrupting ship navigation possibly by Russia. As satellite ground stations are also vital nodes, targeting associated cyber infrastructure can complement space-based attacks.



Schematic showing Space Wars (photo courtesy Dave Cutler Science Photo Library/Newscom)

A sophisticated combination of cyber intrusions, signal jamming and physical attacks termed '**Integrated Space Denial**' can systematically cripple an adversary's space assets. With satellites becoming prevalent, an opportunity exists for potentially cascading failures due to debris collisions as well as economic aftershocks. Extensive Chinese research output on satellite vulnerability studies betrays offensive intent despite an official stance favouring space arms control.

India has made advances indigenously across the space technology spectrum spanning launch vehicles, remote sensing satellites, missile defence programmes and Directed Energy Weapons (DEW). However, Space Situational Awareness (SSA) through an integrated Space Command facility remains a work-in-progress. Optimizing space asset redundancy, hardening electronics against radiation, addressing supply chain cyber flaws and camouflaging transponder signals are vital.

The US leads measures to enhance Space Domain Awareness (SDA)

Avoiding unilateral arms acceleration while also upholding the right to self-defence poses a policy dilemma. Investing in passive protection, redundant constellations and rapid replacement capabilities rather than purely offensive programmes may offer a balanced approach. Global consensus shaping behaviour norms and cushioning space commercialization shocks can aid sustainable security solutions.

Space Domain Warfare

What would a Space War entail? A space war may entail multi-frontier engagements spanning ground, air, space and cyber domains targeting various links of the space-service value chain. Key scenarios include defending friendly satellites, denying rivals their space support functions by degrading Intelligence, Surveillance and Reconnaissance (ISR), or communication abilities and threatening terrestrial nodes like tracking stations and associated infrastructure. Kinetic hit-to-kill vehicles, co-orbital weapons, directed energy capabilities complemented by cyber intrusions and electromagnetic warfare constitute the gamut of counter-space arms capabilities.

Modern space domain warfare encompasses two key objectives -

- Enabling and enhancing capabilities of conventional land, air and sea-based forces via ISR, global communications and precision navigation i.e. the force enablement and enhancement through Space.
- Space protection/ Space domination i.e. protecting one's own space assets from emerging threats while denying rivals their desired space support functions and use of Space.

leveraging partnerships with Australia and other spacefaring allies. Space situational radars and telescope networks tracking orbiting objects help build a holistic picture for defensive response coordination. China's array of ground and space-based sensors provides tremendous space surveillance capabilities. Combined with tested ASAT capacity constituting a credible threat, it limits adversaries' freedom of action in conflict. While international treaties like Outer Space Treaty prohibit Weapons of Mass Destruction (WMDs) in space, verification remains challenging. Russia too operates missile attack early warning satellites and maintains a counter-space weapons inventory since the Cold War.

Space a Force Enabler

Modern satellites and their sensor suites underpin some key military capabilities leveraging space-derived advantages:

- **ISR.** Space assets equipped with EO, IR, hyper-spectral, and radar imaging capabilities offer near-persistent surveillance. This continuous, real-time stream of data empowers ground forces with an unparalleled level of situational awareness, contributing to effective decision-making and battlefield visualization. The shift towards persistent surveillance providing military resolution and accuracy has reached 10 cm and 10 m, leverages smaller satellites across multiple orbital planes scanning earth more frequently with updated EO and Radar sensor data. Sub-metre image resolution and precise geo-location registration aids pinpoint targeting while on-board analytics promises actionable intelligence alerts.

- **Satellite Communications.** It emerges as a lynchpin in the enhancement of conventional capabilities. It provides global and seamless connectivity, acting as a force multiplier by facilitating swift information exchange between diverse military entities, including theatre units, higher formations, and political leadership. Global low-latency connectivity via LEO broadband constellations with end-to-end data encryption provides alternate network-centric warfare channels resilient to conventional network disruption.

- **Position Navigation and Timing.** The precision offered by space assets in navigation is instrumental in accurate geo-location, aiding in targeting, manoeuvres, and the coordination of weapon systems. Global and regional satellite navigation constellations ensure military operations benefit from enhanced accuracy, crucial for mission success. Indigenous navigation constellations like India's NAVIC reduces

reliance on GPS alone aiding location accuracy beyond borders while also assisting long-range missile guidance. Similarly, GLONASS, GALILEO and Beidou are satellite navigation systems developed by Russia, the European Union and China, respectively.

- **Missile Defence.** Detection and tracking of missile launches from space promises more reaction time while space-based lasers may emerge as directed energy interceptors.

- **Weather Monitoring.** Volumetric assessment of storm systems by radar satellites guides forecasts and cloud penetration enables satellite imagery for mission planning.

Space Domination/Control

Space Control essentially involves protecting space infrastructure and space-based assets from disruption or damage by an enemy or any other agency knowingly or otherwise. It comprises of space protection, space denial and SSA. While space protection involves protecting own space assets from disruption or damage, space denial means denying an enemy access to the space resources during the conflict. Space control or space supremacy together contributes towards space domination which will be crucial for any nation for achieving its national security objective.

Essentially the strategy for space control can be either defensive that is protecting your own space assets or offensive that is degrading or destroying the enemy's space assets. SSA would be a prerequisite for any space mission while space domination is an overwhelming superiority in space which offers unrestricted freedom of operation of space assets. Space control through

space protection and space denial will be limited in time in space and would be more practical in a multipolar space order. Space protection, space denial and SSA are the primary requirements towards Space Security.

SSA/SDA. The cornerstone of effective space protection lies in SSA, this imputes knowing the precise location of both friendly and adversary assets. It involves comprehensive tracking and surveillance of objects in earth orbit like satellites, space debris and potential threats. It encompasses detecting, cataloguing and monitoring man-made orbital objects using a network of radars, telescopes, satellites and sensors. SSA provides critical inputs for protecting own assets, safely launching new satellites and attributing any hostile action. With its two distinct features, SDA represents a strategic paradigm which involves enhanced capabilities in conventional domains and the imperative for safeguarding own assets in space. Future battle networks must seamlessly integrate land, aerospace and maritime units into unified webs augmented by space-based ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance) and guidance systems. Cross-domain adjudication, multi-sensor cueing and coordinated kinetic plus non-kinetic options require another order of doctrinal evolution enabled by SDA fusion. The future of warfare lies in cross-domain synergies across land, sea, air, space and cyber realms.

India faces limitations in this capability, underscoring the need for collaboration with strategic partners such as the United States and the QUAD alliance to enhance SDA capabilities. Participation in international partnerships and



Schematic showing possible Indian Missile Defence (photo courtesy clearias.com)

data pooling arrangements will aid collective security while optimizing resource costs.

Protection of Space Assets

Protecting military and commercial satellites underpinning the economy from kinetic and non-kinetic attacks is pivotal today for space-faring nations. While passive measures like hardening satellite electronics, low observational signatures, orbital manoeuvrability are prudent, credible deterrence also requires some active capacity to disable adversary space infrastructure threatening assets. Optimizing redundancy and rapid replacement capabilities for crucial satellites also contributes to resilient space posture.

Space Protection. Safeguarding space assets involves both passive and active measures. Passive protection includes redundancy and hardening strategies against interference and attacks. Rapid replacement strategies are pivotal, ensuring quick restoration of degraded capabilities, thereby minimizing the impact of potential threats. Hardening satellite electronics, disguising

encompasses the ability to neutralize potential kinetic and non-kinetic threats, establishing a proactive defence posture. Denial of adversaries' access to space and maritime commons during conflicts can achieve asymmetric effects when their forces lose satellite navigation, communication and live feeds from ISR platforms. India demonstrated its deterrence ability through the successful Mission Shakti ASAT missile interceptor test in 2019.

Categorisation of Space Weapons

Broadly all space weapons can be categorized either by their location of launch and delivery or method of neutralization, as outlined hereafter.

Location-Categorization of Space Weapons. This refers to segmenting space weapons into classes as per their launch point, target location and strike delivery path. The three key location variants encompass:

- **Earth-to-Space Weapons:** These include ground-based or airborne systems like ASAT missiles that are deployed from terrestrial or aerial platforms to attack adversary space assets in orbit. Examples would include the interceptor missiles demonstrated by India (2019), China (2007) and the US (1980s) to destroy target satellites.
- **Space-to-Space Weapons.** These space weapons are pre-positioned in orbit for on-demand activation, allowing force application within the space domain by engaging hostile satellites also traversing in orbit. Examples are the emerging generation of co-orbital weapons and proximity operation satellites carrying payloads to damage adversary satellites at close quarters.
- **Space-to-Earth Weapons.** This envisages strike systems

transponder signatures, deploying compact decoys and instituting rapid replacement capabilities can complicate rivals' counter-space plans. Alternate constellations, laser satellite links, autonomous orbit shifts and smart jam resistance aid resilience. Satellite longevity through onboard fuel and module replacement by servicing spacecraft will also emerge as a priority.

Space Deterrence. Beyond passive protection, the concept of space deterrence becomes imperative. This involves not only having the capacity to resist kinetic and non-kinetic threats but actively deterring adversaries through strategic means. Space deterrence

based in space which can direct force downwards towards ground or sea-based targets. While no openly declared space-to-earth programme exists today, past US SDI concepts leveraging orbiting strike platforms and Soviet Fractional Orbital Bombardment concepts hinted at this possibility. Advanced DEW if based in space can also deliver effects downwards.

Categorisation by Method of Neutralisation. The two primary classes here are kinetic and non-kinetic counter-space weapons:

- **Kinetic Weapons.** Examples here include direct ascent ASAT missiles, and co-orbital drones damaging target satellites via physical impact or proximity-detonation effects. They aim to achieve physical destruction of the satellite.

- **Non-Kinetic Weapons.** These encompass diverse systems like high-powered lasers, microwave emitters and cyber weapons that can disable satellite functionalities without needing to destroy the platform through advanced electronic warfare techniques, software attacks or directed energy systems. The temporary disruptions may be aimed at specific satellite sensors, communications links, or position/timing signals.

- **Proximity Space Weapons.** A new generation of threats is emerging in the form of satellites designed to manoeuvre close to adversarial assets already deployed in orbit. Known as co-orbital or proximity operation satellite weapons, their unique advantage lies in masked intent while closing in until the last mile. These can have dual use serving ostensibly legitimate aims like SSA, debris inspection etc. while also constituting on-orbit threats carrying payloads to damage adversary satellites when commanded. For example, Russia has the Nivelir satellite with a manoeuvrable robotic arm that can grapple with derelict objects as well as

tamper with or destroy manoeuvring satellites at close distances. Two variants of dedicated proximity weapons maybe loitered in orbit, namely Kamikaze Satellites that seek to inflict terminal direct impact damage to destroy targets and Spy Satellites meant to snoop, tap communications or interfere with enemy satellite electronics through malicious cyber or directed energy payloads. Both further complicate space security challenges.

India's Military Space Capabilities

India has slowly and systematically developed extensive space technologies bolstering both civilian and military needs over the past five decades since the first sounding rocket launch in 1963. The Indian Space Research Organization (ISRO) currently operates over 75 satellites leveraging launch vehicles like PSLV and GSLV along with the geosynchronous satellite launch vehicle (GSLV Mk III).

ISRO's remote sensing satellites with specialized sensors continuously expand earth observation capabilities aiding land and ocean surveillance. The RISAT series in particular carries Synthetic Aperture Radars (SAR) enabling all-weather, day-and-night imaging critical for security forces and disaster response agencies. High resolution Cartosat satellites also enhance land mapping and targeting detail.

The regional NaVIC satellite navigation system provides real-time position, timing and navigation services supplementing US GPS infrastructure across India and 1500+ km beyond borders. This assists Armed Forces by reducing reliance on foreign systems for accurate geo-location, targeting, timing and weapon triangulation leveraging

both networks. NaVIC usage in all weapon systems used by our Armed Forces will however require a more focussed and persistent effort.

The GSAT satellites constellation forms a crucial communication backbone connecting military command centres with land, air and sea via secure data links and voice channels. The latest GSAT 7A specifically serves larger Indian Air Force needs over extensive geographical areas using anti-jamming features. There are plans to launch GSAT 7 which is being called an Army satellite but will practically be used by all three Services.

The successful 2019 ASAT interceptor missile test dubbed **Mission Shakti** demonstrated India's capability to destroy hostile satellites in LEO. This deterrence ability coerces adversaries against attacking Indian space assets, apart from underlining indigenous expertise. On-going projects include early warning threat detection radars, DEW testing and electronic warfare suites.

The Defence Space Agency was constituted in 2019 as a tri-services Space Command for sharpening operational focus. Enhancing SSA via telescopes and radars to build precise space object catalogues amidst growing orbital congestion is vital. Identifying and rectifying defence satellite communication needs and gaps in coverage can aid forces modernization.

India actively champions international efforts to reinforce norms of responsible behaviour in space and curbing weaponization. It is party to treaties like PAROS (UN Treaty), has supported legally binding instruments on arms control and opposes militarization of LEO. Pursuing offensive space warfare



India's Mission Shakti anti satellite missile showcased in Republic Day Parade January 2020
(photo courtesy www.reddit.com)

systems remains unlikely but defensive space capabilities may be enhanced given the deteriorating geopolitical climate.

With one of the most advanced and diversified space programmes globally, India boasts indigenized end-to-end launch vehicle manufacture capability. Augmenting military satellites persistently through compact SCATSAT-class satellites, leapfrogging electronics miniaturization and propulsion systems can aid consolidation of the strategic high ground advantage. Faster satellite replacement, space debris clean-up solutions and strategic international partnerships will also be a key factor.

China's Space Warfare Capabilities

China views space dominance as critical to its regional military strategy, global influence and economy. It thus invests in advanced space infrastructure for intelligence, surveillance, communications, navigation and science missions. Concurrently, focus on denying adversaries unimpeded access to space in conflict underscores counter-space research spanning kinetic and non-kinetic domains.

Robust satellite tracking combines sensors, telescopes, radars and satellites monitoring space with AI analytics parsing orbital mechanics. This enables cataloguing, manoeuvre prediction and activity analysis of thousands of space objects - crucial for optimizing satellite deployment as well as denying reliance on space assets by enemies. China's 2007 ASAT test destroying its own defunct weather satellite via interceptor missile hinted at latent capabilities.

On-orbit proximate operations constitute significant offensive potential given demonstrated ability to manoeuvre satellites close to a target before channelling attacks. The Shiyang-7 satellite notably grappled another

satellite in tests indicating capability to disrupt or destroy assets physically. Cyber intrusions into satellite ground systems abroad, and signals jamming round out non-destructive space control tactics that could supplement kinetic strikes.

China's ground-based ASAT missiles like the DN-3 pose serious threats with capacity to destroy crucial LEO satellites delivering imaging or communication services. Meanwhile, continued testing of anti-missile system interceptors provides foundations for ascending ASAT weapons. This combined intelligence and weapons testing trajectory betrays intent to hold vital space assets of perceived threats at risk.

Evolving DEW like high-powered lasers and microwave emitters pose newer generation threats allowing faster and stealthier strikes with lower attribution compared to kinetic missiles. Blinding or damaging fragile satellite optics degrades crucial ISR capabilities that modern militaries depend on. Meanwhile, China's advanced cyber espionage and attack infrastructure continues to exploit supply chain hardware flaws and software vulnerabilities across the global space industry.

China's Beidou navigation system reduces reliance on American GPS, and indigenous data relays and communication satellite networks powering the Digital Silk Road signify its global space leadership ambitions. To sustain this presence and project power abroad, counter-space programmes seek to offset any limitation that satellite loss may place on China's freedom of action. Its strategic thinkers also increasingly debate the merits of space arms control agreements.

China views establishing ascendancy in cislunar space as vital to its rejuvenation and securing comprehensive national power status. With stakes poised to rise further as the global space economy grows, shaping norms and risk reduction protocols remain urgent. But verification of

capabilities and separating civilian-military fusion dynamics pose arms control hurdles requiring creative diplomacy.

Conclusion

As space dominance gains prominence among military planners and strategists, emerging counter space weapons threaten to undermine satellites which have facilitated enormous socioeconomic progress in recent decades. With over 90 plus countries now reliant on space for security as well as essential services, risk mitigation and prevention of arms acceleration in on-orbit realms is urgent. The 2019 establishment of the US Space Force acknowledged space as a warfighting domain requiring specialized focus, doctrine and capabilities different from the Air Force.

With LEOs getting more congested, satellite protection measures including steerable antennas, low observability designs, electronics hardening against radiation and thermal extremes have become vital. Orbital repositioning protocols, redundant constellations across multi-orbits and integrated early warning-command arrangements must be instituted domestically while advocating similar global norms. Also LEO satellite constellation for military Satcom use needs to be now factored into our plans.

Though India remains traditionally a strong proponent for prevention of space weaponization through binding international agreements, changes in risk and capability calculus necessitate strategic review. Ambiguities around dual-use systems, difficulty verifying suspicions and separation of civilian, commercial space sectors from defence agencies all pose arms control protocol challenges. India's demonstration of ASAT missile interceptors destroying a test target in low orbit back in 2019 signals capability for

punitive retaliation if adversaries endanger our space assets through their own expanding counter space programmes. Offensive programmes may also preventively remove exclusivity of critical geographic zones.

ISRO has the benefit of advanced end-to-end satellite design, manufacturing, launch and operations expertise powering world class remote sensing, communication and scientific missions over the past five decades. Responsive launch also called Launch on demand (LOD) is the need of the future and hence quick turnaround and responsive space lift capabilities leveraging proven SSLV, PSLV, GSLV and GSLV-Mk III fleet at Sriharikota launch complex needs to be tailor made for strategic needs.

Optimizing sensor suites of existing satellites to diversify intelligence inputs without adding launch cost overheads offers avenues to augment real-time battlefield awareness. Incorporating EO, IR, multi and hyper-spectral bands as well as SAR radars in compact satellites yields various weather-proof monitoring capabilities aiding tri-service needs. In future, persistent ISR through Space is necessity.

International collaborations leveraging expertise of partners like France, Israel and Japan in early warning threat monitoring radars, seekers, directed energy programmes and other sensors should be expanded through the Defence Space Agency. In-orbit satellite servicing concepts, active debris clean-up systems and global SSA dataset access requests could also be pushed under UN auspices.

In the 21st century space domain, establishing resilient and responsive space lift, satellite longevity and replacement preparedness is vital to

sustain the information edge. Alliances upholding freedom of access, responsible norms, risk mitigation protocols and tactical capability cooperation offer promising bridges. India offers global leadership prospects upholding strategic high ground advantage while shaping an open, secure ultimate frontier.



Lt Gen Anil K Bhatt

Lieutenant General Anil K Bhatt, PVSM, UYSM, AVSM, SM, VSM (Retd) is the Director General of the Indian Space Association (ISpA), the apex industry body for the Indian space sector. He had an illustrious career spanning over 38 years in the Indian Army, and has served as the Director General of Military Operations, Corps Commander of the Chinari Corps, Military Secretary and has tenanted various other leadership roles. He is an alumnus of prestigious institutions like the Army Staff College-UK, College of Defence Management and National Defence College. As Director General of ISpA, he has been at the forefront of creating a vibrant private space industry ecosystem in India, providing visionary leadership in building collaborative partnerships between industry, government and academia to unlock the immense potential of the Indian space sector. General Bhatt also serves as the Chairman of the Board of Governors of IIIT Kota.

PATHOGENS AND VIRUSES

A LIKELY BIOLOGICAL WARFARE BIOTERROR THREAT?

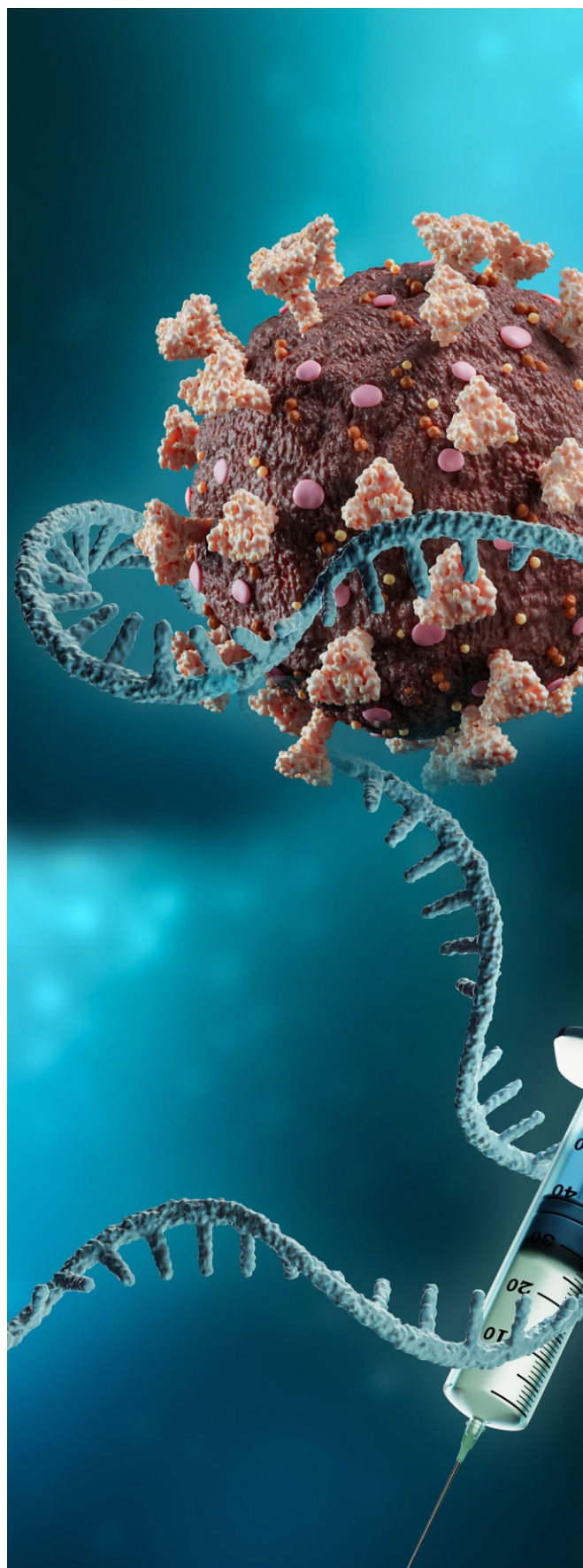
Global threat perceptions of Biological Warfare (BW) and Bioterror (BT) attacks portend catastrophic consequences for any unprepared targeted populace. Dangerous pathogens can be developed and used to target an inimical country, people, group or enterprise as world power politics becomes more unscrupulous, as this article highlights.

'Asymmetrical warfare is a euphemism for terrorism, just like collateral damage is a euphemism for killing innocent civilians'

- Alan Dershowitz

The Backdrop

The bizarre and sinister **VUCA** (Volatile, Uncertain, Complex & Ambiguous) and the **BANI** (Brittle, Anxious, Non-linear & Incomprehensible) habitat has plunged our planet, with exponential momentum into unfathomable mayhem. The devastating onslaught and calamitous ramifications of war, terror, strife and conflicts in the recent past, the current context and maybe future 'tense' in various 'hot spots' is distressing. In the not too distant past, the relentlessly ruthless COVID-19 pandemic, with suspicious origins in our Northern neighbourhood, unleashed a huge death toll of about 6.95 crore 'officially recorded' deaths worldwide. (Note : As per certain media reports, the long term



deleterious effects of the Covid-19 infection and fast tracked vaccines are worrisome. This data seems not to have been included in the world's official death toll, as mentioned above). This brutally ravaging pandemic with seemingly dubious derivations, eclipsed the cumulative deaths, disease and trauma due to terrorism and the 'war of terror' in the last few decades. Such disruptive chaos can emerge due to the surreptitious (ab)use of easily tweaked viruses and pathogens - which can emerge in a 'cold start' broth, as a dangerously repetitive reminder of China's 'Wuhan Gift' to the world. Interestingly, our Northern super power neighbour is in the news for another outbreak of atypical pneumonia. We optimists hope it is quickly arrested and exterminated within the Great Wall of China, but should remain watchful of its progression, and emphasise on respiratory hygiene and precautions on pollution colds & coughs.

The Indian Armed Forces have historically distinguished themselves in wars, combat zones and against 'extrinsically unleashed' terror attacks, in counter terror / insurgency operations, internal security; and as eminently reliable first responders in disasters and mass casualties. In the dark world of the **VUCA-BANI** environment, the security forces will need to widen their horizons, perspectives and capabilities to be 'battle ready', beyond the conventional paradigms and dogmas of warfare, considering the possible catastrophic influence of bio-threats and other non-fictional Chemical Biological Radiological Nuclear (CBRN) perils.

Overview

The contours of medical science as they relate to the ever evolving stratagem of conventional conflicts, security and defence, has undergone a major metamorphoses and pendulous upheaval. From the exotic mystique of science

fiction, BW and BT including the CBRN spectrum, have become a cruel reality with their devastating threat looming at the doorstep of virtually any region, nation, state or society. The sheer magnitude of morbidity and mortality resulting from use of such unorthodox weapons presents hitherto unprecedented challenges to the security ecosystem and the healthcare community in particular; and living beings, in general.

Consequently, our country and the world, needs robust sentinel bio-surveillance networks, effective response mechanisms and integrated countermeasures for optimum bio-security to build comprehensive safeguards, against the incomprehensible biological and unconventional armamentarium. Enhanced awareness of this threatening Armageddon and its wide ranging ramifications will enable the Government, the security mandarins, the scientific community and the medical fraternity to measure up to these myriad concerns. In the aftermath of a biological attack, frontline and healthcare workers would play a crucial role in recognizing the different manifestations of the unknown ailments; and alert public health officials, leading to prompt emergency measures, medical, immunological (vaccine related) and public health interventions, to prevent widespread mortality and severe morbidity.

So, What is BW and BT? Bio – Security and Bio – Surveillance?

BW is defined as the 'employment of biological agents to produce casualties in human or animals or damage plants'. BT implies the spread of terror through the use of bio agents to produce deleterious effects in the targeted

populace. The term 'Bio-security', originally used in the defence ecosystem, regarding the control of biological weapons, is a 'strategic and integrated concept that encompasses the policy and regulatory frameworks (including instruments and activities), that analyse and manage risks in public health, food safety, animal life and health, as also plant life and health, including associated environmental risks'. Bio-surveillance has been described as 'active data-gathering with appropriate assessments and interpretation of biosphere data that might relate to disease activity and threats to human or animal health-whether infectious, systemic, toxic, metabolic, or otherwise, regardless of intentional or natural origin-in order to achieve early warning of health threats, early detection of health events, and overall situational awareness of disease activity'.

Biosecurity and Biodefence came in to the lexicon of the scientific mindscape in the late 20th century to comprehend, conceptualise and institute effective actions to achieve bio-safeguards against virulent organisms which can inundate human beings, animals and plants, exposing them to biological threats of novel devastating infectious diseases. Biosecurity and biodefence, often used interchangeably, encompass deliberate planning, coordinated bio-intelligence analytics and seamless coordination for efficient countermeasures to combat BT and BW.

Historical Vignettes

The occurrence of BW and BT related diseases, with the devious intent to cause death and disease, is chronicled many centuries back. BW also finds fleeting mention in the pre-historic era, when Melanesian tribesmen used arrowheads contaminated with tetanus.



Health workers tackle a pandemic. Representational Image (Image US National Guard; Photo by Master Sergeant Becky Vanshur)

In 14th century BCE, the Hittite army sent rams infected with tularemia to their enemies; and in the Trojan War of the 6th century BCE, Scythian archers infected their arrows from decomposing cadavers and human blood containing tetanus and gas gangrene. In 14th century CE, the Tartar army catapulted plague victims over the city walls of Caffa, and in early 18th century, the Russian Army threw bodies of plague victims into Swedish cities in Estonia. In 1763, the British presented smallpox-contaminated blankets to native Americans. During the First World War, German troops hustled horses and mules infected with glanders and anthrax. In 1932, the Japanese allegedly attacked Chinese cities with the bio-agents of anthrax, cholera, shigellosis and typhoid along with plague; due to which at least 10000 reportedly died. The United States is said to have commenced an offensive BW programme at Fort Detrick, Maryland in 1943. By 1969, the US had reportedly weaponized the bioagents causing anthrax, botulism, tularemia, brucellosis and Q fever. These were said to have been destroyed unilaterally, as ratified by the Biological Weapons Convention (BWC), 1975. **The BWC in its utopian aims,**

towards devastation. Despite the 'BWC Agreement', the development of BW/ BT biothreats has reportedly continued unabated, albeit in a clandestine manner, 'beneath the watchdog's radar screen', aided by the surreptitious canopy of the 'Gain of Function Research' (GOFR) programme, which gave self-certified legitimacy to 'toying with; and tweaking' the virus genome, ostensibly to study its characteristics, so as to stay ahead of mutations and novel infectious diseases and outbreaks, which may emerge from the studied pathogens. Until recently, the jury was still out to ascertain whether the novel corona virus pandemic, was a relocated lethal by-product of the mutant miscreant's GOFR leveraged devastation.

The Bane of Biothreats

Biological threats which arise from emerging infectious diseases pose unrelenting dangers to global health security. India is indisputably vulnerable to these infectious diseases due to its geographically turbulent neighbourhood, population density, fast track urbanization, increased encroachment on wildlife areas, and overstretched resources. In recent decades, the country has experienced outbreaks of COVID-19, severe acute respiratory syndrome (SARS), H1N1 influenza, avian influenza, and the Zika virus. These biological threats can be naturally occurring, intentional or accidental.

Naturally Evolving Biothreats: Infectious disease threats do not recognise borders or barriers. Urbanization, climate change, global warming, habitat overlaps, economic disparities, and ultra-modern lifestyles, with suboptimal hinterland health systems, enhance the potential of naturally 'drifting & shifting' pathogens to exponentially spread rapidly across the globe. Novel infectious diseases, the resurgence and spread of once geographically limited and spill over

forbids the signatories to develop, produce, stockpile, acquire or retain BW agents, or the means to deliver them.

There is an increasing concern over the possibility of the terrorist use of biological agents to threaten military and/or civilian populations. The Indian plague epidemic in the 1990s, was retrospectively investigated for a possible BT attack. There are many more such apparently bizarre incidents that have occurred in the past. With affordable, user friendly, virtually 'off the shelf' lab technology, this perilous armamentarium is turning deadlier by the day, with grim spin-off side effects

zoonotic diseases (from animals to humans), along with multidrug antimicrobial resistance, can inundate response capacities and make outbreaks and pandemics unmanageable.

Intentional Acts of Commission:

Intriguingly but not unexpectedly, USA and other developed countries were amongst the pioneers in the GOFR acceleration in virology, which was undertaken with the seemingly noble aim to comprehend the genetic configuration of viruses and the nuances of virus-host interaction; ostensibly to generate higher yields for vaccine strains. Conversely, GOFR has given impetus to generation of genetically engineered transmuted viruses, resulting in formation of more highly pathogenic and rapidly transmissible, customized killer biothreats. Genome editing technologies, that give researchers (and rogues), the ability to change an organism's configuration and abnormal immunological host responses, have enabled faster, cheaper, highly accurate, and more efficient bioweapons. Nations and terror groups could develop or procure from a 'bioweapon lab's cafeteria menu' of modified and transmuted pathogens with immense transmissibility, enhanced severity, increased mortality, along with resistance to conventional treatments and known vaccines. Terrorists can conveniently carry out wanton targeted assassinations with customized bioweapons, which may affect only a single person or a select populace, based on their genetic code. You would all recall that *Russia has possibly executed targeted assassinations of their dissidents in recent years in Europe, using dangerous bio-agents.*

Unintentional (Leaks): The risk of laboratory leaks, as suspected in Wuhan, and 'inadvertent' accidents are increasing with the burgeoning economy of the biotechnology 'science-scape'. World

powers are making huge investments for monetary gains, but diluting safety checks in the field of biotechnology, thereby increasing the propensity of leaks which propagate outbreaks.

The Alarming Futuristic Forecast of the Unfathomable Disease 'X'

With COVID-19 having abated into an apparently manageable endemic disease, the World Health Organisation (WHO) and reputed healthcare professionals have propounded another grave pandemic, propelled by the perplexity of the (as yet) obscure but menacing 'Disease X'. It is apprehended that this unidentified new viral illness could have unparalleled catastrophic consequences, more than that of the Spanish Flu of 1918-1920 and the recent COVID pandemic, with mega million fatalities, perhaps comparable with the cumulative death tolls of the pandemics of this and the last century; and both the world wars, as well. Projections estimate that this new pandemic may have the cataclysmic enormity to result in 20 times more fatalities than the coronavirus pandemic; with far more suffering and severe morbidity amongst the afflicted. Despite COVID-19 causing a mammoth number of deaths across the world, the vast majority (above approximately 90+ %) of the infected populace managed to recover, though the long term consequences of the novel Corona virus, and more so some of its rapidly rolled out vaccines, seem alarming. With its destructive abilities and higher fatalities, the horror story of **Disease X** could be extremely contagious with the killing potential of the Ebola virus [which had approximately 67% death rates]. The world cannot ignore possible

devastating consequences of the looming '**Disease X**', with the crystal ball forecast of runaway escalation. Unrestrained urbanisation, unabashed deforestation, unhindered land grab of animal abodes and unchecked proliferation of bioscience technology add highly explosive fuel to this volcanic inferno.

Preparing for the Disease X Pandemic

Concerted collaborative efforts through harmonious partnerships to forecast, identify, overcome and achieve the elimination of the indeterminate 'Disease X' and future pandemics, should be the highest priority of WHO, global and national policymakers, and the scientific community. This will necessitate expeditious impetus to upscale research, innovation, development and production (RIDP) of targeted vaccines and efficacious drugs, in addition to multidimensional countermeasures. The '**100 Days Mission**', as elucidated in some publications, is an aspirational and ambitious, albeit potentially hazardous enterprise, due to the possible flouting of defined safety mechanisms. The ambitious yet achievable initiative hopes to develop virus strain specific vaccines in just 100 days, from the hitherto achieved record of 326 days, during COVID-19. The scientific and research domain experts need to cultivate and fast track the assembly line of varied safety assured technologies to create dissimilar prototype vaccines for bio-agent prioritised biothreat virus families. This will quicken the launch of multipronged vaccines to attack various components and genomic



The Bio Threat. Representative Image (photo credit Tereshchenko Dmitry via Shutterstock)

material of the microbial biothreat; and achieve better immunogenicity against viruses. My two cents insight on this is that **since the intelligence and scientific experts failed to predict the COVID pandemic, this may possibly be a “convenient, ‘CYA’ attempt at: we told you so, nebulous, indeterminate astro-forecast like guesstimate”.**

Biodefence should be configured and customized to two distinct target populations, namely the civilian non-combatant populace and military combatant security forces. The recent Coronavirus pandemic propelled ‘biosecurity’ as a global priority and geo-strategic existential imperative, with future implications in view of the varied terrorist bio-attack scenarios and myriad biothreat prospects.

Thus far, the global bio-defence strategy, is fairly nascent and relatively undefined. A template framework for BT risk assessment, if appropriately crafted, can be a quantum force multiplier for policy makers, governance agencies, security ecosystems and healthcare professionals to assess and review the

biothreats and bio-terror agents, in order to consolidate strong bio-defence through robust and effective bio-surveillance modalities, with feasible bio-deterrence and guaranteed biosafety.

We can divide bioterrorist attacks into three tiers namely, **strategic** (large scale), **operational** (middle scale) and **tactical** (small scale), with a four component chain model, which includes perpetrators, agents, means of delivery, and targets. Quantitative and qualitative risk assessment parameters are therefore important, for credible risk assessment and remedial measures.

Relevance of Bio-Surveillance

History and genomic footprints have unequivocally reminded us that apparently banned conventional and modern biological weapons have mostly emerged from pathogens of the animal kingdom. Hence, natural and manmade bio-threats, will mostly materialise from a host swap of microbes, that leap from animals to humans. A robust bio-surveillance consortium comprising administrators, clinicians, microbiologists, public health officials, veterinarians, bio-intelligence experts and biosafety auditors can enable early identification of a bioweapons attack, thereby enabling remedial measures, safe immunoprophylaxis and treatment of diseases in the vast majority of people (and/or animals) exposed but not yet ill. Significant advancements have been achieved in bio-surveillance from the erstwhile automated BT detection system called RODS (Real-Time Outbreak Disease Surveillance), for multiple data collection and analytics to clinically correlate and detect possible BT events at the earliest. The principles and practice of bio-surveillance, a relatively innovative, trans-disciplinary arena, of real-time disease outbreak detection, is easy to apply to both natural and manmade pan/epidemics. Microbial spillovers from animals to humans, along with novel tweaked microbes and genetically engineered pathogens, should have stringent sentinel watch expertise to track bio-threat emergencies through Artificial Intelligence (AI) and tech enabled platforms.

Identification of Bioweapons

Humungous efforts are being directed for the development of biochips, immuno-polymerase chain-reaction methods, genetic sequencing, BW tickets, single-particle fluorescence counters, ligand

based probes, fluorescence-based transduction, and other techniques, to detect specific markers of potential biological agents and identify the biothreats and ‘*neuter-alize*’ their perpetrators.

The key objectives of biodefence against potential bioweapons, are to synergize and coalesce the sustained efforts of the national, regional and global bio-safety stakeholders, with public health officials and domain experts, to track the trail of biothreats. This has to be spearheaded by the governance and administrative machinery; and ably supported by the scientific community and healthcare fraternity, to provide multi-layered defence mechanisms against BW attacks. The traditional approach towards protecting human beings, agriculture, food, forest and water; by focusing on the surreptitiously launched, naturally leaping or unintentional release of virulent diseases, should be strengthened by focused efforts to address current and anticipated future biothreats, that may be deliberate, manifold, recurring and catastrophic.

Planning and Preparedness

We should focus on training the varied human resources and creation of hi-tech specialized facilities for the development of contemporary bio-threat identification systems, detection platforms and cogent response mechanisms. Biological agents are relatively easy to obtain, procure, ‘tweak’ and deploy by terrorists who are becoming fanatically emboldened, destructive and threatening. Advanced tech spurred bio-surveillance networks can provide early warning, identify contaminated areas and populations at risk; and facilitate prompt treatment. Effective yet safe vaccination drives, containment, quarantine and control measures to

prevent dissemination are vital to achieve biosecurity. Microbiological forensics and allied technologies are evolving to identify biological agents, their geographical origins, initiation, acquisition and launch-pads along with decontamination technologies and mitigation measures, to restore normalcy without causing collateral consequences. Early detection and rapid responses to BW/ BT attacks are contingent on the harmonious and effective cooperation between global agencies, Government, officials, healthcare fraternity, scientific community and law enforcement agencies, beyond siloed vertical hierarchies, which currently may give the impression of ‘a bridge too far’.

Waxing Eloquent on Vaccines

Without a realistic, feasible yet fast tracked timeframe, optimum funding and synergistic collaboration, we may be faced with the haplessness of mission insurmountable, in the immediate aftermath of bioattacks. Effective preparations entail the creation of a vaccine library with assured impeccable safeguards, where in advanced research is ramped up to produce immunogenic agents against prioritised high risk virus families, to launch new effective and precise vaccines, which can be rapidly developed for any identified biothreat, from its prototype precursors. Theoretically, the creation of a vaccine library is a seemingly flawless concept only if failsafe protection against ‘*collaterally damaging*’ adverse effects is guaranteed, and if global mega-funding and hi-tech support is fully committed and sustained. While the vaccine library is an innovation imperative in the long term, adequate worldwide safeguards are indispensable. Concerns are being

evinced based on suspicion and information, which is indicative of the ‘*long term*’ effects of some COVID vaccines. This underlines the imperative of enshrining established assurance of safety in future vaccination campaigns, for fast tracked efficacious vaccines against biothreats and emerging infectious diseases, so that we do not compromise the non-maleficance maxim of *primum non nocere* (i.e. first, do no harm)

Towards a level playing field for ‘Vax Populi’ : Besides the goals, objectives, essential measures and key indicators to achieve tangible global biosecurity, pacts and agreements should be enshrined, to achieve the long overdue vaccine equity and its assured safety more for the poor ‘**have-nots**’ than the affluent ‘**haves**’. Curbs, dissuasion and consequences of non-compliance should be imposed to prevent short-shrifting safety checks. Deceitful unscrupulously profiteering cliques also reportedly stockpile ‘*boarded*’ vaccines for opportunist profiteering; and then epitomize magnanimous malevolence in their sham charitable allocation. In the ideal collaborative global arena, shared apportioning of vaccines is critical to prevent the proliferation of pandemics. This participative global partnership must have an associated exponential benefit accrual so that national governments and global leaders are incentivised to uphold biosecurity, as the ethos and edifice of the WHO's Pandemic Treaty. This contrite accord paves the way for all countries and all stakeholders to achieve synergy in response mechanisms, against biothreats and pandemics, in a seemingly aspirational, binding agreement for defined cooperation in



Biological weapons (photo courtesy biologické zbrane Czech Republic mzp.cz)

vaccine equity bio-safeguards and accountability. If we pledge to offset vaccine inequity, quantum scaling up of local manufacturing, will enable low-income countries to achieve vaccine self-sufficiency at affordable prices. Stringent safeguards in vaccination overdrives, should be made mandatory through legislation and rigorous deterrence.

The development cycle of creation, safeguard validation and mass production from **bug to drug launch** takes up to ten years, before its complex distributary equity, is achieved. The core bio-defence strategy goals would also require the quick reduction of the timelines of all these processes, with its foundation fortified by preparing safe viral lineage vaccines, as foundational firmaments. Bio-safeguard initiatives can be successful if adequate investments are made in the cutting edge RIDP continuum.

Chinese Perplexing Designs

China has achieved the dubious distinction of being termed as the world's largest disease incubator and the globe's

leading disease disseminator. India and South East Asian countries must hence have strong collaborative biosecurity and biodefence systems in place. As per print media reports of 2022, "*Pakistan and China are continuing with bioweapons research in a secret facility near Rawalpindi*". The article stated that China is creating Covid-like pathogens in Pakistan, which have the potential of causing virus contamination on a scale far higher than Covid. The Pakistan Army-run, **Defence Science and Technology Organization's** ('bio-enterprise') laboratory infrastructure has been stated to be located in the Chaklala Cantonment, at Rawalpindi, in Pakistan. The seemingly secret project is titled: *Collaboration for Emerging*

Infectious Diseases and Studies on Biological Control of Vector Transmitting Diseases. Not surprisingly, it is further alluded that this sinister Sino-Pak joint collaboration appears not to be configured to carry out scientific experiments, but craftily customized for the covert purpose of weaponizing pathogens.

India Prepares – Getting Ready

The integrated **One Health Approach**, accelerated by the Government of India, is a collaborative, multi-sectoral, and trans-disciplinary campaign — working at the local, regional, national, and global levels — with the goal of achieving optimal health outcomes, recognizing the interconnection between people, animals, plants, and their shared environment. It also encompasses managing certain biological materials and potential biothreats across the earth-scape, thereby strengthening counter-BT mechanisms, while giving an impetus to scientific progress. Through its focused strategies, the Indian Government has established a network of Vaccine Research and Development Laboratories (VRDLs), and upgraded the facilities therein. The landmark initiative envisages coverage of the entire country for prompt diagnosis, early identification of dangerous pathogens, before and during outbreaks and epi/pandemics, data collection and collation of potential viral biothreats, to enable speedy mobilization of resources and remedial measures to save human lives. The participative "**NI-Kshay Mitra**" campaign gives a fillip to inspire people's and NGO's cooperation in this arena.

India's role, as a global player and a key regional leader in Asian geopolitics, is ever expanding at a fast pace. Its endeavours and strategies

in defence, health, life sciences, and biosafety cooperation are increasingly acknowledged in strengthening and balancing regional and global biosafety. Herein, it is also pertinent to mention that one of the US National Defence Strategy priorities is to 'Defend the Homeland', commensurate with the growing multi-domain threat posed by China. This reinforces the urgency to develop and fortify national and regional strategies to address our country's contextual geo-strategic challenges and concerns.

India and USA have recently determined to promote and ramp up partnerships with cutting-edge biotechnology and bio-manufacturing, and to improve biosafety and biosecurity, innovation, practices and norms. The good news is that India has a strong and robust bio-economy, which is expected to reach USD 150 billion by 2025 and cross USD 300 billion by 2030. Our country has been ranked among the top three in South Asia and top twelve destinations for biotechnology in the world. India is leveraging the 'Network of Infrastructure under Biosecurity and Biosafety', with a network of VRDLs, across the country, to strengthen the nation's biosecurity and biosafety domains; and for preparing the country for a robust response to future epidemics and pandemics.

The collaborative framework with USA should enshrine pan spectral emergency response capabilities, robust public health systems with trained and digitally AI enabled officials and personnel, hi-tech lab detection networks, pharmaceutical readiness to treat at the volume, quantum and scale required, along with achieving a state of vaccine library maturity, with truncated timeframes to bulk produce safe and specific biothreat targeted vaccines with equitable distribution. Adequate biohazard

containment assets from decontamination to infection control facilities will also be required. From a fly on the wall worldview, these are at best, in a nascent, if not nebulous, or perhaps, even a non-implementable stage. Integrated interdisciplinary research, innovation development and production pipelines, with stringent but non-restrictive, safety checks and biosecurity audits are therefore critical to comprehend, control, counter and conquer the hi-tech propelled bio-threats, with the lethality of its bio-armamentarium, and the 21st century biotech savvy, rogue terrorists.

The world and our nation, should shorten its learning curve to achieve robust biosecurity with resolute tenacity, through intrinsic bio-resilience and bio-deterrence, to be optimally prepared for the frighteningly forecasted **Disease-X**. We ought to implement sustainable strategies and enhance capacity building to rapidly detect incipient threats and emerging pandemics, analyse the voids and gaps in preparedness, and ramp up comprehensive biosecurity mechanisms. This will require upscaled bio-surveillance with an incentivised impetus to align with the global bio-security integration systems. We should also prioritise adequate funding for biosecurity counter-measures. As we approach the end of the first quarter of the 21st century, India and the world should fortify strong partnerships for early warning, detection and rapid response systems, to achieve collaborative and failsafe global biosecurity. The recently accomplished, visionary Presidency of G20, showcased the pre-eminent position of India, as the iconic ambassador of 'Vasudhaiva Kutumbakam', which enshrines "One Family - One World - One Future", in

consonance with the glorious heritage of our great nation.

It is apt to end with a quote from Henry Ford, the industrial magnate and the founder of Ford Motor Corporation, who stated... **"Coming together is the beginning. Keeping together is progress. Working together is success"....**

(Acknowledgement: The author gratefully acknowledges the noteworthy contributions and valuable insights of Lieutenant General PR Venkatesh, PVSM, SM, Brigadier Sourav Sen (Retd), Major Mohammed Ashraf Namaji and Dr. Pragya Yadav).



Lt Gen RS Grewal

Lieutenant General RS Grewal, AVSM, VSM (Retd), an alumnus of the Armed Forces Medical College, Pune superannuated in April 2020, as DGMS (Army), after a distinguished career of about 39 years, in various prestigious instructional, command, staff & administrative appointments in the Armed Forces Medical Services. He has commanded the highest multi-speciality tertiary care hospital in Leh (Ladakh) and the largest Command Hospital at Pune. In his second innings, he has been the Vice Chancellor of Sikkim Manipal University, Gangtok and Member, Medical Advisory Committee, National Medical Commission till July 2023. He has now 'returned to his roots' in the academic-clinical domain. He has several scientific research publications to his credit, including contribution of chapters in widely subscribed reference text books.

PRIVATE MILITARY CONTRACTORS

"THE DOGS OF WAR"

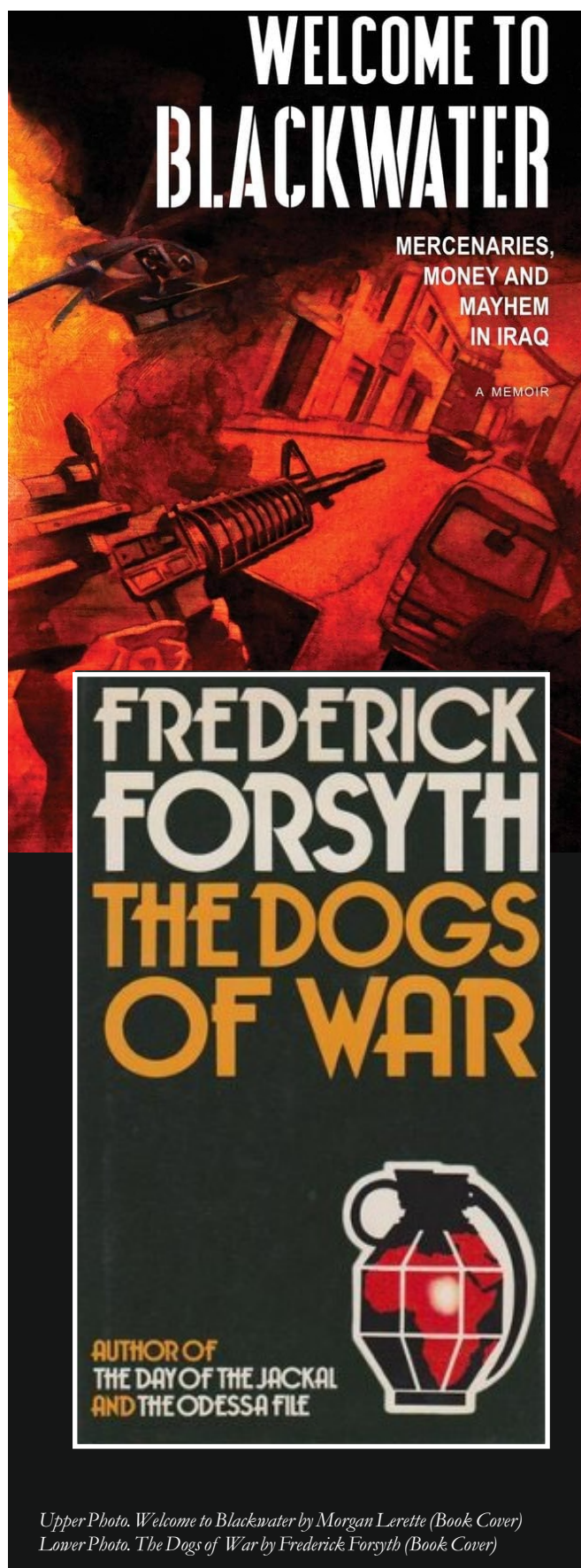
NON - STATE ACTORS OF STABILITY OR INSTABILITY?

Many of us have read Frederick Forsyth's famous novel, **"The Dogs of War"** depicting the powerful intervention by mercenaries to destabilise new regimes in Africa. Are mercenaries or Private Military Contractors (PMCs) a new phenomenon, or have they been around for ages? Well, the term PMCs is new, but similar security services were around for centuries. In olden and medieval times, a King had several feudal lords or vassals who maintained soldiers for their own security and for fighting for the King when required or sought by the King. Indian Kings and Princes too would pool in warriors from their Jagirdars and Subedars when a threat developed. These **'State Forces'** were not totally **'private'** however, but owed allegiance to an authority. Many PMCs today owe allegiance to a power, but also conveniently don 'the cloak of deniability' – like our neighbourhood non-state actors. And PMCs will continue in conflicts in future as they meet the clandestine requirements of different nations, and provide lack of accountability too.

Introduction

The modern-day growth of PMCs took root in the era of neo-economic liberalisation of the Western nations post world war providing the ideological justification for private security.¹ To the veterans, end of the cold war, accompanied by the increasing number of intra-state conflicts provided an alternate avenue for employment to plug the gap in the security sector of the newly independent countries that were in the middle of conflicts.

¹ Paul D. Williams and Alex J. Bellamy, "Privatisation," *Understanding Peacekeeping* (Cambridge: Polity, 2021), 288-306



Upper Photo. *Welcome to Blackwater* by Morgan Lerette (Book Cover)
Lower Photo. *The Dogs of War* by Frederick Forsyth (Book Cover)

As the number of conflicts increased, the PMCs flourished generating revenue and employment for the war veterans and in some cases criminals, and also assisted in a boom in the arms industry. It is reported that in the late 1990s, the PMCs were able to generate revenues of 20 billion USD per annum.² PMCs lack accountability, feed on instability and hence are up for sale to the highest bidder.

Actors of Stability or Instability?

The list of roles that PMCs can play is long, covering anything from training and advisory roles, logistic support, acquisition of intelligence, and providing static guard and personal protection to undertaking military operations either independently or jointly with the security forces of the country employing PMCs. There is an absence of internationally accepted legislation to regulate PMCs, and the states that are employing PMCs and those who are providing them are also unwilling to regulate them. PMCs can be actors of both stability and instability depending on the way they are employed.

Actors of Stability

In the long-running Angolan Civil

War, Angolan state oil company Sonangol hired the services of **Executive Outcomes** (EO) to secure and defend its Soyo oil field (North of Angola) from the UNITA rebels in 1993 and for defending the diamond mines. This way, even though the civil war continued, the Angolan Government, with the help of EO, managed to reduce the capacity of UNITA to continue the war to a great extent and finally forced the outfit to sign the Lusaka Peace Agreement. For its services, EO was paid an amount of 40 million USD per annum and undisclosed diamond mining rights. One of these rights amounted to 25 billion USD per annum.³

In 2014, the Nigerian Government, to fight Boko Haram, hired South African mercenaries - **Cornella Services, Pilgrims Africa** and **Specialised Tasks, Training, Equipment and Protection International** (STTEP) to train Nigerian soldiers. The mercenaries undertook joint operations against Boko Haram. The mercenaries and specially

trained Nigerian soldiers made some remarkable gains while fighting Boko Haram. Destruction of the Boko Haram Headquarters and rescuing a number of kidnapped school girls was a decisive moment in Nigeria's fight against Boko Haram. A few African nations are contemplating using this model in their respective countries.

Nigeria continues to employ PMCs for training purposes. Collaboration with **Starter Point Integrated Services** (SPIS) to train Nigerian soldiers in Infantry School in 2020, hiring Israeli firm **HLSI Security System and Technology Limited** in 2021 with a contract of 195 million USD for the training of a special intervention force, and the acquisition of sea, land and air capabilities are two such examples. The Nigerian National Petroleum Corporation (NNPC) also hired a PMC to counter piracy at sea, who successfully intercepted a vessel carrying stolen crude oil.⁴

The Central African Republic

² Paul D. Williams and Alex J. Bellamy, "Privatisation," *Understanding Peacekeeping* (Cambridge: Polity, 2021), 288-306

³ Jorås, Ulrike, and Adrian Schuster, eds. "Profile of the Private Security Sector in Angola." *Private Security Companies and Local Populations: An Exploratory Study of Afghanistan and Angola*. Swisspeace, 2008. <http://www.jstor.org/stable/resrep11104.14>.

⁴ Murtala Abdullahi, "Nigeria's Frosty Interest In Private Military Contractors," *HumAngle*, April 24, 2022, <https://humanglemedia.com/nigerias-frosty-interest-in-private-military-contractors/>; Teniola T Tayo, "Soldiers for rent in Boko Haram Crisis," *Institute for Security Service*, February 8, 2021, <https://issafrika.org/iss-today/soldiers-for-rent-in-the-boko-haram-crisis>. Also, see, Ahmad Sababi, "Over 40 insurgents killed as ISWAP and Boko Haram clash in Borno," *The Cable*, August 24, 2023, <https://www.thecable.ng/over-40-insurgents-killed-as-iswap-boko-haram-clash-in-borno>



Wagner Group Mercenaries Flag (photo courtesy Arab Center, Washington DC)



Wagner Group fighters (photo courtesy NBC News)

(CAR) also involved PMCs to bring back stability.⁵ In 2022, the CAR Government allies and armies' along with **Wagner Group** personnel and Rwandan soldiers repelled the attack of six armed groups who were planning to attack the capital city of Bangui.⁶ The **Wagner Group** continues to operate in CAR.

There are different shades in the form, organisation, indoctrination and allegiance of PMCs. Many non-state actors, akin to PMCs operate in the Islamic nations and in the Middle East. In Lebanon, the government supports the military operations by **Hezbollah** against Israel. **Hezbollah** is funded by a foreign country and is a non-governmental armed outfit, hence can be called private, but it is considered by Lebanon as a resistance movement to defend the sovereignty of Lebanon against Israeli aggression. Even though Hezbollah's military deterrence has played a role in preventing a major conflict until now, at the end of the day, it is a private organisation.

Actors of Instability

The PMCs notoriety in violation of Human Rights (HR) and International Humanitarian Law overshadows their

selective positive contribution. In CAR, there are reports of PMCs' HR violations while operating along with CAR Armed Forces. There are similar reports of EO's involvement in Angola and in mining operations in Sierra Leone; **Sandline International** has also been blamed in Sierra Leone.⁷ In 2000, there were reports of dozens of PMCs which included former soldiers of the Soviet Armed Forces, veterans of the French Foreign Legion, and businessmen who were engaged in arms trafficking in Democratic Republic of Congo.⁸ Recent instances of HR violations by the **Wagner Group** in Mali have again drawn the attention of

the world to the risk to civilians by the unregulated PMCs.⁹

In 2000, **DynCorps**, a US-based security organisation was accused of raping and killing young girls and women and trafficking when the agency was contracted to train Bosnian police.¹⁰ Another notorious example of PMCs violation of HR is that of **Blackwater** killing 17 Iraqi civilians and injuring 20 at Nisour square in Baghdad.¹¹ Four employees were convicted in the United States and later pardoned on 22 December 2020, by President Donald Trump.¹²

⁵ Michael Amoah, "Private military companies, foreign legions and counterterrorism in Mali and Central African Republic. *Alternatives*," Sage, Vol. 48, No.2. 2023, pp. 133-150, DOI: 10.1177/03043754231155754

⁶ Michael Amoah, "Private military companies, foreign legions and counterterrorism in Mali and Central African Republic. *Alternatives*," Sage, Vol. 48, No.2. 2023, pp.11, DOI: 10.1177/03043754231155754

⁷ Francis, David J. "Mercenary Intervention in Sierra Leone: Providing National Security or International Exploitation?" *Third World Quarterly*, Vol. 20, No. 2, 1999, pp. 319-38. <http://www.jstor.org/stable/3992920>.

⁸ "DR Congo. North and South Kivu, Security Companies, Business as Usual," *South World*, May 1, 2023, <https://www.theguardian.com/world/2020/dec/23/trump-pardons-blackwater-contractors-jailed-for-massacre-of-iraq-civilians>

⁹ "Mali: New Atrocities by Malian Army, Apparent Wagner Fighters," *Human Rights Watch*, July 24, 2023, <https://www.hrw.org/news/2023/07/24/mali-new-atrocities-malian-army-apparent-wagner-fighters>

¹⁰ Matt Heibel, *Military Inc.: Regulating and Protecting the "A-Team[s]" of the Post-Modern Era*, 18 *Pace International Law Review*, Vol. 531, No. 6, 2006, pp. 533, DOI: <https://doi.org/10.58948/2331-3536.1090>

¹¹ Matt Heibel, *Military Inc.: Regulating and Protecting the "A-Team[s]" of the Post-Modern Era*, 18 *Pace International Law Review*, Vol. 531, No. 6, 2006, pp.554, DOI: <https://doi.org/10.58948/2331-3536.1090>

¹² Michael Saffi, "Trump pardons Blackwater contractors jailed for massacre of Iraq civilians," *The Guardian*, December 23, 2020, <https://www.theguardian.com/world/2020/dec/23/trump-pardons-blackwater-contractors-jailed-for-massacre-of-iraq-civilians>

Our Neighbourhood – PMCs or Terrorists

Closer home in South Asia, one sees a different shade of state-sponsored PMCs. Amongst many, **Jaish-e-Mohammed** (JeM) and **Lashkar-e-Taiba** (LeT), are two major terrorist organisations that have their training camps in Pakistan and Afghanistan and operate in Pakistan's neighbourhood with impunity.¹³ Pakistan is known for using these home-grown terrorist organisations as PMCs in pursuit of its strategic interests in the neighbouring countries. India has often faced attacks launched by these Pakistan-sponsored PMCs. There is however a clear difference between groups like **Hezbollah**, **Hamas**, **JeM** and **LeT**. Hezbollah has been acknowledged by the Lebanese Government as a resistance force. Besides, Hezbollah is a political party and undertakes several social activities for its large following in South Lebanon. Hamas also has a political wing, but is not under the control of the Palestinian Authority. Hamas is not accountable to any Government, Hezbollah too has such a standing. JeM and LeT on the other hand are sponsored and funded by Pakistan's intelligence agencies but Pakistan does not accept their ownership officially. These terrorist organisations are actors of instability not only in Pakistan's neighbourhood but also in Pakistan.

The HR Question

In conflicts, whether it is inter-state or intra-state conflict, the biggest challenge is protecting innocent civilians when the state itself is complicit in crimes against its citizens; or how to protect them from the threat from armed groups. Some states are in the midst of armed conflicts where peacekeeping missions are deployed, and PMCs are also operating with the knowledge and tacit approval of the host

states; examples CAR and Mali. The host states prefer to turn a blind eye to the crimes committed by the PMCs as it helps them to remain in power.

But there are proponents who believe that PMCs can be selectively used to fill the security gap in states that are facing armed conflict. If the PMCs become members of the International Stability Operations Association (ISOA), formerly the International Peace Operations Association (IPOA), and uphold the ethical standards as set out in the ISOA code of conduct, PMCs could be a force multiplier.¹⁴ That apart, despite many positive contributions on the part of the PMCs to maintain stability, the reality is that the PMCs personnel are quite indisciplined, roguish and use the gun in their hands for crimes, looting and sexual offences.

PMCs are actors more for instability and less for stability; with a record of HR Violations.

The Future

PMCs are here to stay. The Americans found it convenient to employ **Blackwater** for security services in Afghanistan, and used them clandestinely for illegal operations too. The Russians too have used the **Wagner Group** extensively in the Bakhmut battle in Ukraine, and in many parts of Africa, to serve their strategic interests. Iran too will continue to support Hezbollah, Hamas and other such groups; and Pakistan will likewise retain their terrorist groups. The major advantage of such terrorist groups or PMCs is the **'cloak of deniability'**; and that countries can use such PMCs for their strategic, clandestine operations without involving their regular Armed Forces.



¹³ "Pak-based terror group JeM, LeT maintain training camps in Afghanistan: UN report," *The Hindu*, May 30, 2022, <https://www.thehindu.com/news/international/pak-based-terror-group-jem-let-maintain-training-camps-in-afghanistan-un-report/article65475232.ece>

¹⁴ For more on ISOA, see <https://stability-operations.org/>

Major General (Dr) AK Bardalai, commissioned into the Indian Army on 11 June 1977, is a graduate of the National Defence Academy, Pune and Defence Services Staff College Wellington. General Bardalai commanded an infantry battalion in Siachen Glacier, an infantry brigade in the mountainous terrain and counter-terrorism operations in North East India and later commanded an infantry division in the western theatre. He was the Commandant of the Indian Military Training Team in Bhutan from October 2011 to January 2014. He has rich experience as a UN Military Observer in Angola, Director of UN Peacekeeping at Integrated HQs of MoD (Army), a Research Fellow (UN Peacekeeping) with United Service Institution (USI) of India, New Delhi and the Deputy Head of the Mission and Deputy Force Commander in UNIFIL (Lebanon) from March 2008 to March 2010. Post retirement, he is actively engaged in the academic study of UN Peace Operations. He holds a PhD in UN Peace Operations from Tilburg University (the Netherlands).



**Major General
(Dr) AK Bardalai**

TRENDS IN MARITIME WARFARE

ECHOES FROM THE PAST BUT ALSO NEW WAVES

The Russo-Ukrainian conflict currently underway has been widely commented—and is being analysed “live” across the world. Some commentators have said it is very different from previous conflicts in all dimensions of warfare. These include the generally well-known Air, land and sea dimensions and the cyber and space warfare dimensions. This article looks at the maritime dimension.

Not all that ‘New’

In reality, the Russo-Ukraine conflict is not vastly different from some earlier conflicts where the use of technologies and tactical measures seem either similar but with evolutionary changes as well, when compared to the recent Armenia-Azerbaijan war and many aspects seen in the long wars that America was engaged in Afghanistan and Iraq. Where the current inter-state war in Europe differs is that the maritime dimension is more obviously present than in the other conflicts mentioned. Even here, the 13 April 2022 attack on the Russian Navy cruiser and the Black Sea Fleet’s then most powerful ship, Moskva, had precedents. It is likely that the Russian Navy may principally have expected such an attack, but they were not sufficiently alert tactically to defend themselves against such a strike. At the same time, using shore-based missiles for attacking ships was not something that Ukraine invented; there are precedents from decades earlier.



*Schematic showing Maritime Domain Awareness
(photo courtesy marineinsight.com)*

The first use of anti-ship missiles (ASMs) actually occurred in conditions of an uneasy peace about four months after the famous ‘Six-Day’ war (05 to 10 June 1967) between Israel and an alliance of Egypt, Syria and Jordan. Although Israel had won the war and captured a lot of territory, their guard was down and the Egyptians used the ‘surprise’ principle of war. On 21 October 1967, more than four months after the actual war, Egyptian missile boats (of NATO code-name ‘Komar’- class) within Port Said fired four anti-ship missiles (NATO code name ‘Styx’) at *Eilat* which was patrolling in the Mediterranean Sea off Port Said. She was the first ship to be sunk by ASMs. Thereafter, as is well known in India, the Indian Navy used its missile boats spectacularly to attack ships off Karachi and some targets on land as well twice in the 1971 war. This first attack was on 04 December which is rightly celebrated as Navy Day. From 1980 to 1988, during the Iraq- Iran war, the Iraqis fired shore-

based and air-launched missiles at merchant ships as well as at a US Navy frigate (*the USS Stark*) with two Exocet missiles. These missiles were quite effective in the 1982 Falkland/Malvinas conflict as well. The short point for emphasis is that precision ordnance like homing torpedoes and ASMs have long been in use. Developments in electronics, homing systems, propulsion ranges, speed, counter-measure capabilities have all improved and may be expected to further improve with technological developments.

More Echoes from the Past

For centuries, Navies had to fire on the move often at an enemy on the move. In the age of sail, the effective ranges of fighting between battleships (as were called in the age of fighting sail) were a few hundred yards sometimes ending in muskets being used and ships physically entangling the adversary and sailors boarding an enemy warship to overcome the crew. When larger, powered artillery cannons in moving turrets started appearing in the larger all- steel, coal and then oil powered cruisers and battleships, they brought hitting power at thousands of yards, with gun calibre varying from 6 inches to 15 inches by 1914 when the First World War (WW1) started. However, accuracy was very poor so the effective fighting range was now about 2000-3000 yards and it still took several dozens of shells to score one lucky hit on an enemy that was not only also moving at some speed but also capable of firing back.

The problem of fire control (FCS) consisted of computing a target's predicted position when a shell or salvo fired at a given movement could accurately hit it, based on estimated course and speed of an enemy, one's own speed and course, the range to the target which was determined by slowly improving rangefinders, etc.

Target data had to be computed through some basic computing devices and data was transferred to a moving turret with multiple barrels to elevate barrels at a particular angle of elevation and direction (called training angle). By the middle of the Second World War (WW2), range finding and predicted position calculations were helped by radars and gun mountings began to be 'slaved' to the FCS and accuracies improved. At the same time, the Americans had developed acoustic homing torpedoes while the Germans had submarines with rudimentary homing devices that led a torpedo towards a target's propeller and wave related noises. In the post WW2 period, there were steady improvements in precision, lethality and speed of ordnance that included guns, better torpedoes and of course ASMs and Surface to Air Missiles (SAMs). It can be correctly said that navies were the early birds in the need and efforts towards developing precision in FCS as well as varieties of ordnance.

Of course, the Air Force followed soon and also worked hard at accurate bomb dropping using advanced bombing sights. It was much later that guided/ homing bombs were devised to be practically effective. Although the term Precision Guided Munitions (PGM) is thought of mainly with respect to Air Forces and aircraft, it is across services and all homing weapons may be called PGMs. For aircraft, issues of their higher speeds, altitude and the higher speeds of enemy aircraft that can manoeuvre rapidly pose great challenges. It is also a reality that army tanks began firing on the move often at mobile targets like enemy tanks; and artillery effectiveness improved by battlefield targeting radars, sensors for

locating and ranging targets and advanced computers for fire control solutions.

Fort and the Fleet

There were periods in history when cannons based ashore in coastal forts and certain vantage points could target ships while having a certain level of immunity from ships trying to use their cannons effectively. Shore-based anti-ship artillery had its own pros and cons. Among the advantages were that these cannons could be larger in terms of length, as well as calibre. They were often at a greater height than the cannons in ships, and therefore had a range advantage. Also, unlike a ship, the cannons were on a stable "deck" ashore! But, they had limited arcs of fire, and could not really move from place to place as could ships with their cannons. While the maxim that "*a ship is a fool to fight a fort*" was often correct, there were exceptions. (*Incidentally, the line is often attributed to Admiral Nelson, but he did not actually say it and did fight forts along the coasts of Denmark quite effectively*).

Figuratively speaking, the capabilities now available to the '**Fort**' on land today have increased in variety and intensity. It may become increasingly difficult for ships to operate in an enemy's littoral (ie along the coast and in seas proximate to the enemy) and the Russian Navy should have been more alert to the possibility. India has built up such measures over the years. For instance, truck-mounted versions of Soviet/Russian ASMs were part of the Indian Navy's arsenal for decades and are now being replaced by ASM versions of the very lethal Brahmos missile. Many readers of this magazine may already be aware that such land-based mobile ASMs are



Source: Timothy M. bond, et al, "What Role can Land-Based Multi-Domain A2/AD Forces in Deterring or Defeating Aggression," RAND Report, 2017.

being given to the Philippines to be part of their sea control architecture in an area of great security concern for them in the light of China's muscle flexing in waters that belong to the Philippines. There are other measures, for example manned and unmanned shore-based aviation of the Indian Navy, and maritime strike capabilities with the IAF that have existed for decades but are also being modernised.

Echoes from the past for the Fort and Fleet can be heard in India's case as well especially for the Marathas. They built a series of forts along the coast that complimented their naval power. Though their Navy (including in Chhatrapati Shivaji's time) could not create the strategic and long-term benefits potentially possible, they were of significant tactical help in many cases. That Navy Day on 04 December 2023 was celebrated in and around the old fort of Sindhudurg in Maharashtra's Konkan belt may be a tacit recognition of the growing roles of the 'fort' in assisting defensive effectiveness when operating in

conjunction with one's fleet and the severe trouble it can cause an enemy's fleet in waters it can influence from land.

China's Fort and Fleet Framework

In China's case, a modern version of this combination has acquired contemporary effectiveness that has become a problem for several nations operating in the Western Pacific, the US included. Briefly, the People's Liberation Army (PLA) Navy's capability to checkmate other navies and littoral forces of say, Japan, Taiwan or others to operate in the waters of the Indo-Pacific up to even 1500 to 2500 kms from the Chinese coast is aided by the land-based multi-dimensional instruments consisting of a varied

arsenal of land-attack and anti-ship missiles; by hundreds of land-based aircraft belonging to PLA Air Force and PLA Naval Aviation; and expeditionary capability resident in amphibious troops belonging to Naval infantry and the regular Army. All this is supported in a central way by the ISR (Intelligence, Surveillance and Reconnaissance) of various types enabled by aircraft and UAVs and also by the other two dimensions of warfare, space and cyber being used defensively and offensively. This architecture of 'active defence' as the Chinese term it but A2AD (Anti-Access/Area Denial) as the Americans call it, is a strategic, operational and tactical problem opposing forces have to live with and solve as best as can be done. For illustration, a sketch of Chinese missile coverage arcs over the Pacific and the Indian Ocean are shown in the above image.

So, What is Evolving?

With some illustrations from the past and present, we have seen a continuum of sorts, as well as change...which is generally slower than what commentators and even professionals often feel. It is still too early to draw conclusions and reliable inferences from the Russo-Ukraine war, just as it was after the previous Armenia - Azerbaijan conflict that was thought to be "revolutionary" as far as the use of drones for ISR and combat was considered. Subsequently, more sober and less excited analysis showed its evolutionary characteristics, and even shortcomings in the ability of both sides to adapt to capabilities, understand limitations and be tactically and operationally more imaginative. It is similar for the Ukraine conflict.

In three areas, we see the impact of technological changes and the benefits of multi-dimensional strategies and operations in the maritime domain.

First, is the increased pervasiveness, persistence and accuracy of ISR available to more advanced nations that are investing more in what, to use relatively recent jargon, is domain awareness with its more popularised version i.e. **Maritime Domain Awareness** (MDA). Today, among the clutter of land topography, traffic, movement, urban density, human activities, other types of clutter, it is still possible for vehicles to be tracked, (whether our cars by Google or car manufacturers or even tanks and artillery). Likewise, over the sea, surface detection capabilities have improved significantly in the last decade. It is true that the density of surveillance may be lesser than over land, but it could be contextual to the need for such surveillance in times of tension or conflict. All manner of orbiting satellites (which should be rightly thought of as the first very high-altitude unmanned drones from the late 1950s) can be reoriented in time and space to provide adequate search, tracking and even reasonable targeting data. Satellites could be supplemented by UAVs and Maritime Patrol Aircraft (MPA), Over the Horizon Targeting (OHT) radars and even manned and unmanned submarines. In the relatively lesser clutter of a sea-surface, the heat and UV signature and the visual/ optical track left by a ship's wake all matter. Detection of submarines through enemies' capabilities for Underwater Detection (UDA) is more difficult, but is a work in progress by several nations to enhance their capabilities for detection, while increasing attempts at improved stealth.

Second, is the varied types of ordnance improvements that can be discerned. This is especially so for land-

based ordnance that could be used against targets at sea with greater range, endurance, precision, speed of attack and explosive effects. China seems to be at the fore-front of efforts with hypersonic missiles, anti-ship ballistic and a variety of cruise missiles. The Americans are not down-playing this concern.

Third, is the multi-dimensional jointness and coherence that could improve. This is seriously beneficial in all contexts and India seems to be more alive to this thinking which would create synergistic advantage. The Chinese PLA has probably taken the biggest strides in

this area and their models need to be studied and replicated to the extent required. In other words, **one's own fort and fleet could be jointly effective to counter someone else's fort and fleet.**

To sum up, seapower has been central and critical to a nation's overall maritime effectiveness and the leverage and influence it provides to deter or help win conflicts with other dimensions of statecraft and military instruments. **Our Navy continues to enhance its overall maritime effectiveness in tune with the rapid technological advances.**



Rear Admiral Sudarshan Y Shrikhande, AVSM, (Retd) was commissioned in July 1980. During his long service, he commanded IN ships Nishank, Kora and Khukri. He is a post-graduate (with distinction) of the Soviet Naval War College (1988), DSSC Wellington (Scudder Medal), Naval War College and of the US NWC with highest distinction (2003) winning the Levy, Bateman and Forrestal Prizes. He was the Defence Adviser in Canberra with concurrent accreditation to four other South Pacific nations from end 2004 to early 2008. He contributes as a strategic analyst and post retirement is involved in teaching strategy formulation, operational art, force structuring, leadership, ethics and diverse military subjects in several military and civilian institutions. He is associated with the Vivekananda International and Observer Research Foundations as well as FINS and the Stimson Centre, Washington DC. Apart from being an Adjunct Professor at the Naval War College, Goa and Takshashila Institution, Bengaluru, he is Editor-in-chief of the Indian Naval Despatch. He has participated in Track 2 dialogues with a few countries as well as in other national and international conferences.



**Rear Admiral
Sudarshan Y Shrikhande**

DRONES

SHAPING COMBAT SPACE IN THE RUSSIA - UKRAINE CONFLICT

The air medium has been the game changer in war in the last century, with aerial weapons deciding the victor in many battles. The speed, accessibility, precision and strategic effects that can be brought in from the skies is immense; drones or unmanned aerial vehicles are proving to be potent, effective and economic in conflict.

This article discusses their employment in the Russia-Ukraine Conflict.



In the ongoing Russia - Ukraine conflict, drones have acquired a significant role in war fighting. Drones are Unmanned Aircraft Systems (UAS), which have the capability to fly autonomously, stay airborne for long periods of time, and perform one or more critical functions such as intelligence, surveillance, reconnaissance, electronic warfare, target identification, target designation or offensive functions namely, carrying out attacks on targets, et al.

Drones have been used in several conflicts, starting as early as the Vietnam War, till most recently in the Armenia- Azerbaijan confrontation in Nagorno- Karabakh, where Azerbaijan effectively used the Israeli made **Harop** Loitering Munitions. However, the scale of utilisation in the Russia-Ukraine conflict is unprecedented. As per estimates of the Royal United Services Institute, Ukraine is *losing* 10000 drones per month, giving an indication of the numbers in use. One possible reason for this scale of utilisation is that Air Defence systems are a substantial threat to manned aircraft, making unmanned aircraft a preferred option.

Roles of Drones

Drones are being used for a variety of roles such as intelligence, surveillance, reconnaissance,

electronic warfare, target identification, target designation, directing artillery fire and even for carrying out offensive missions. Drones carry photo, video, or other data collection sensors, which allow forces to locate enemy bases, observe troop movements, and choose targets. It also enables documentation of attacks, which could be used appropriately to influence target audiences. Drones have documented the destruction of cities by Russian forces, the flooding of Ukrainian territory following the Kakhovka dam breach, and attacks against Russian ships, tanks, troops, and material. Ukrainian forces have used armed drones such as the TB2 to target the Russian convoys headed for Kyiv. On 14 April 2022, *Moskva*, the Flagship of the Russian Black Sea Fleet was hit and sunk by Ukrainian forces, using the subsonic sea skimming R-360 Neptune anti shipping cruise missiles. The Ukrainians are believed to have used the TB2 drones to distract the formidable and layered defence system of the *Moskva*, which made the attack successful.

Drones Used by Ukraine

Ukraine is using a variety of drones, ranging from the very small **Black Hornet** with a wingspan of only 12 centimetres to drones with wingspans of over 15 metres. Single-use drones, termed Loitering Munitions, which hover above a target before diving into it and exploding with it, are also reportedly in use. Some important drones being used by Ukraine are discussed hereafter.

The **Baykar Bayraktar TB2**, is an Unmanned Combat Aerial Vehicle of Turkish origin, capable of remotely controlled or autonomous flight operations. It is 6.5 metres long, has a wingspan of 12

metres, can fly at a maximum altitude of 25000 feet, and has an endurance of almost 24 hours. It has a maximum take-off weight of 650 kgs, and can be armed with four laser-guided bombs.

The **Punisher** is a small and nimble locally made drone, designed and manufactured by a company operated by veterans of the Crimea conflict. The company describes the drone as “*reusable, fast, unexpected, precise, lethal*”. The **Punisher** has a 2.3 metre wingspan, can fly at 400 metres altitude at a cruising speed of 43 knots, endurance of 90 minutes and a range of 45 kms. It can carry a combat payload of 2 kg. The small size and low altitude allows the Punisher to reach deep behind enemy lines with little risk of detection before or during strikes and then return for a quick five-to-seven-minute servicing.

Quadcopter Drones are also being used to carry horizontally placed Molotov cocktails, which are triggered remotely to target troops on the ground.

The **Switchblade** Kamikaze drones were given to Ukraine by the USA as part of a military aid package. The Switchblade has two variants-the 300 and 600. The 300 is designed for pinpoint strikes on personnel, and the larger 600 is meant to destroy tanks and other armoured vehicles.

Some Drones Used by Russia

The **Kalashnikov Kyb** drone is a small drone about a metre wide and a metre long, with flight duration of 30 minutes. It typically cruises at 80 km per hour. It can carry a payload of 3 kg.

The **Orion-E** combat drone is considered Russia’s best strike drone. It is a battle tested drone, which was used in combat in Syria. The **Orion E** has a maximum flight altitude of about 8000 metres and flight endurance of up to 24 hours. The cruising speed is up to 200 km

per hour with a maximum payload of 250 kgs. The **Orion-E** can carry up to four air-to-ground missiles / bombs. It also has electro-optical and infrared cameras under its nose, and possesses a laser-target designator to deliver guided weapons.

Forpost R is a license-produced version of the Israeli IAI Searcher II drone. **Forpost R** has a maximum speed of 200 km per hour, mission endurance of about 18 hours, and a service ceiling of about 6000 metres. The primary mission of the **Forpost R** is reconnaissance, and is equipped with improved radar identification equipment and other reconnaissance devices.

Anti Drone Measures

The two main methods to down a drone are kinetic and electronic. The first means shooting down a drone with bullets, rockets, or similar projectiles. The second implies jamming or interrupting the signal between the drone and its operator(s). Besides these,

net throwers, drones that fight drones, and even birds of prey trained to take out rogue hobbyist drones can intercept drones.

Ukraine employs a variety of Air Defence systems, deployed in tiers, to defend against Russia’s missile and drone attacks. SAM systems such as SA-8 Gecko, SA-10 Grumble and SA-11 Gadfly (Buk) are deployed in short, medium and long range layers around the Vulnerable Point (VP). Western medium to long range systems, such as IRIS-T, NASAMS, SAMP/T, Aspide and Patriot, have also been deployed alongside legacy Soviet equipment. For closer ranges, they employ man-portable Air Defence weapons such as Igla and Stinger, which have even been credited with taking down Russian cruise missiles. The innermost layer of anti-aircraft guns such as the German Gepard or US Avenger have been used to great effect against drones.

Russia has deployed its advanced electronic warfare systems for protection against aerial threats,



Some of the drones used in the Russo-Ukraine Conflict (Image courtesy www.dronesshield.com)

including drones, using a combination of jamming and spoofing. They have deployed the Krasukha-2/4, R-330Zh Zhitel, and RB- 301B Borisoglebsk-2 ground-based electronic warfare systems, which use a combination of jamming and spoofing. Although not initially designed for counter-drone activities, they are effective for countering drones if employed correctly.

For the kinetic kill, Russia has a plethora of Air Defence systems deployed in layers around their VPs. To quote an example, the defences on the Flag Ship of the Black Sea Fleet, *Moskva* included S-300 Surface to Air Missiles and SA-8 Osa missiles. The radar systems on *Moskva* included MR 800 series – 3D radar with digital sensors, a second layer comprising MR 710-3D search radar, and additionally, Fire Control radars integrated with S-300 and OSA (SA-8) missiles. The innermost layer comprised Close In Weapon Systems (CIWS) namely, AK 130 (130 mm), dual purpose L-70 and AK 630 CIWS.

Some Points of Interest

A large number of the drones employed in the conflict were originally designed for commercial purposes or for hobbyists. They are therefore available in large numbers at low cost and are easy to use. As they are not built for war, these drones have low survivability in the battlespace, but given their price and availability, they are generally dispensable.

Another note-worthy point is that individuals have come forward and donated drones to the war effort. Further, thousands of drones are reportedly acquired through crowd funding efforts of the public. This public participation in the conflict by the populace is feasible since non-military drones are relatively low-priced, are readily available in quantities, and are easy to purchase by

individuals, without getting involved in formal procurement procedures.

Prognosis

The ongoing conflict between Russia and Ukraine is throwing up the central role that drones are playing in conflict zones. The advantage of an unmanned system which can penetrate deep into the territory of the adversary and carry out a variety of missions, with no human attrition, is being driven home forcefully. Not only are these unmanned systems able to produce tangible results, there are intangible results such as degrading the morale of the enemy by a constant fear of an aerial attack from an invisible enemy. Using quad copters to drop Molotov on the adversary is just an example of the versatility of these systems, and the creative ways in which they could be employed.

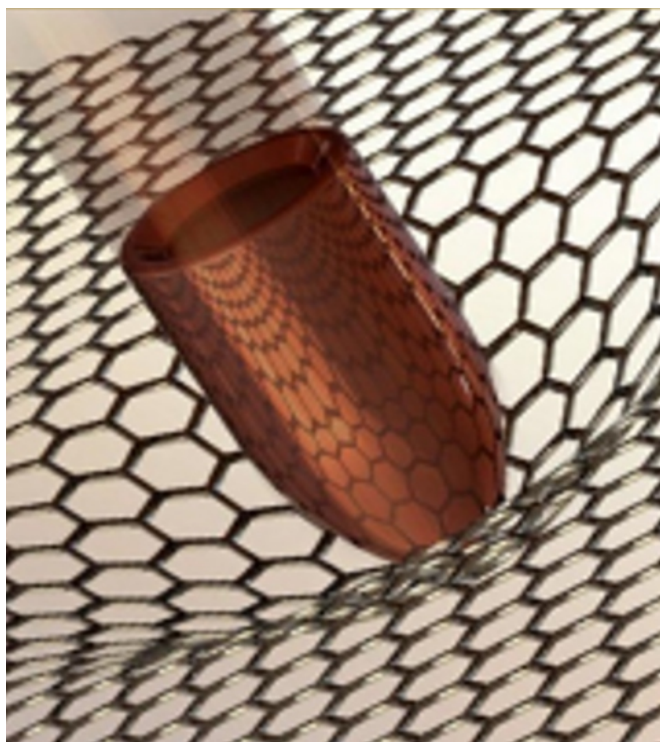
References:-

1. *Combat Drones in Ukraine* by Adam Lowther and Mabbube K Siddiki
2. *Drones in Ukraine and Beyond: Everything You Need to Know* by Ulrike Franke
3. *In a State of Denial: The Air War in Ukraine* by Francesca Verville and Catarina Buchatskiy



Air Marshal Harpal Singh

Air Marshal Harpal Singh, PVSM, AVSM, VM (Retd) joined the 56th NDA Course and was commissioned as a fighter pilot in June 1980. He has about 2500 hours of flying experience mainly on MiG 21, MiG 23, MiG 27 and MiG 29 aircraft. He has commanded a MiG 29 Squadron and has also been a Chief Operations Officer at an Air Force Station. He has commanded two Air Force Stations in the West and East respectively. Besides his DSSC Course, he has also attended the Senior Officers Course at National Institute of Defence Studies, Japan. He has been the Deputy Commandant College of Air Warfare (CAW) and has held important appointments in the strategic arena. He was SASO, SWAC, LAF and thereafter Director General (Inspection and Safety) of the LAF till his superannuation in May 2019.



Military applications for graphene - a nano, bullet proof material
(photo courtesy nanografi.com)

NANO TECHNOLOGY

The Armed Forces are amongst the most visible users of nanotechnology. Small and micro drones, mosquito drones, nano satellites for military communications and surveillance, sensors, medical care on the battlefield, smart textiles, lightweight and durable material for weapons and vehicles are some of the innovations changing the dynamics on the battlefield. This narrative discusses the technological applications in defence.

Ring!!Ring!! My intercom buzzed, it was my Commanding Officer (CO) on the line. "Rahul, the Commander wants us to speak about some disruptive technology in the fortnightly officers training next week. Any suggestions?" I pondered and remembered having been introduced to Nanotechnology during my M. Tech. in Cyber Security the previous year. "Sir, we could talk about nanotechnology", I responded. "That is a good idea, Rahul. Prepare for it then, I am sure it will be informative for many of the attendees", continued the CO. I replied "Wilco, Sir" and my brain started ticking. I remembered the Professor highlighting that Nanotechnology encompasses the deliberate manipulation of size and shape at the nanometre scale (equivalent to the atomic, molecular, and macromolecular scales) in order to create, characterise, manufacture, and implement structures, devices, and systems that possess at least one exceptional or novel property or characteristic. The technology facilitates the fabrication of nano-scale components and structures.

The concept was first talked about in 1959, when an American physicist called Richard Feynman held the first systematic discussion on nanotechnology

in a lecture, when he spoke about "controlling and manipulating things at a nano-scale". Nario Taniguchi, a Japanese physicist, first used the word "Nanotechnology" in a 1974 article on manufacturing techniques.

So what is nanotechnology about? To put it simply, nanotechnology is the study and manipulation of matter on the nano-scale. Dimensions between 1 and 100 nanometres are under the purview of the nano-scale. One nanometre is one billionth of a metre in size. Unusual material qualities emerge at the nano-scale and significant variations in material behaviour are detected. For instance, if you alter a particle's size, its hue shifts accordingly because the arrangement of atoms in particles on the nano-scale causes them to reflect light in a unique way. Silver might seem yellow or amber, whereas gold can appear dark red or purple. A material's surface area can be expanded by the use of nanotechnology. More atoms can now form bonds with foreign substances. One of the main reasons nano-scale materials can be stronger, more durable, and more conductive than their bulk

counterparts is because they have a higher surface area.

A few days later while I was working on the presentation for the lecture, my colleague Hemant walked in. "What are you working on?" queried Hemant. "Nanotechnology, I have to take a lecture next week" was my response. "But doesn't nanotechnology have more applications in the civilian sphere," Hemant continued. I agreed and opined that although still in its infancy, nanotechnology is already having a profound effect in many different fields. Applications made possible by nanotechnology are already in use in a wide range of fields like agriculture, industry, social and human engineering, healthcare, electronics and energy generation. Nanotechnology and nanomaterial is also being applied in many industrial sectors to include health, food, defence, information technology, power, energy, space and environment. Nanotechnology offers cost-effective precision agricultural solutions for herbicides and fertilisers, using nano capsules instead of standard spraying methods. Food packaging with silver nanoparticles kills bacteria,



Artistic illustration of Nanotechnology In Warfare And Defence Showing Advanced nanotech display system and Nanotech weapon system (photo credit unrevealedfiles.com)

carbon nanotube sensors detect spoilage, and silicate nanoparticles seal food packets against external gases, extending the shelf life. Large, hydrophobic carbon nanotubes can remove pollutants from water and remediate wastewater. Such uses of nanotechnologies are currently being developed in the civilian sector, and these applications will soon be used in the military sector with several countries making significant strides towards the development of capacities in this field. “Yes, undoubtedly, nanotechnology will have significant spin-offs in the defence sector,” stated Hemant as he glanced at my power point slides.

As I read more about the subject, I realised that Nanotechnology would impact warfare in several ways with lighter, tougher, heat-resistant nano material available to make war-like equipment, weapon platforms and missiles. I reflected that India must keep up with the latest technological developments, and be operationally ready to defeat inimical endeavours to use such disruptive technologies.

I entered the text on my next slide, titled **Military Specifics**. Defence related research establishments are conducting research in a wide range of areas related to target engagement, mobility, protection, logistical support, equipment, survivability, lethality, vehicle and weapon performance, etc. I listed these fields on the slide, as

- (a) **Surveillance.** Nanotechnology allows miniature sensors to detect mines, explosives, Chemical Biological Radiological Nuclear (CBRN) contamination, soldier’s health and location and battlefield situational awareness. Interconnected nano sensors can produce a surveillance dust that secretly collects and sends all surveillance data to a command post for analysis.
- (b) **Unmanned Aerial Vehicles (UAVs) and Drones.** Nanotechnology improves drone performance and lethality. It reduces weight with great structural strength, nano coatings lower detection probability, and drones can use nano sensors for combat surveillance and hazardous material identification.
- (c) **Soldier Suit.** Nano fibre-based textiles provide lightweight, flexible, bullet-resistant, biochemical, thermal, adaptive camouflage, and health monitoring capabilities for battlefield soldier suits. Battle suits may have a carbon nanotube smart helmet with facial recognition, field sensors, night vision, camera, GPS and communication devices. It will be lightweight and ballistic-resistant.
- (d) **Camouflage and Concealment.** Nano material in military equipment, vehicles, and aircraft can vary light/heat reflection and absorption, reducing thermal and optical traces.
- (e) **Vehicle Enhancement.** Nano technology has significant implications for motor vehicle designs, including weight reduction, improved safety, fuel efficiency, durable chassis, engine and body, and fire resistance for crash-proof vehicles.
- (f) **Future Weaponry.** Nano technology-based weapons will be lightweight and robust, featuring miniature cameras, sensors, and radar on projectiles for target tracking and course correction.
- (g) **Tracking.** Small smartphones with nanotechnology can aid in communication and military tracking. RFID-enabled microchips can identify troops and track casualties in combat.
- (h) **Logistics.** Nanotechnology can improve the efficiency of the military logistics supply chain during wartime. Using RFID tags,

nano sensors, enhancing battery life and fuel cells can improve logistics in the battlefield.

- (j) **Power and Energy.** Nano device energy needs will spur innovation in nano -powered devices. The shelf life of conventional Li-ion batteries is restricted by finite cycles. Nano-structured anode power sources offer about 10 times higher energy density and reduced weight.
- (k) **Healthcare.** Nanotechnology has numerous healthcare applications, including patient diagnosis and targeted medicine delivery. It targets the malignant cells specifically, minimising collateral damage to healthy cells, making it suitable for cancer treatment. Battle casualties and other casualties can be treated more effectively.
- (l) **Satellites.** Using nanotechnology, electronics, solar panels, power packs, communication, and computer components can be miniaturised while maintaining strength, and nano satellites have thus appeared on the scene. Small satellites can be attached to larger ones to prevent detection.

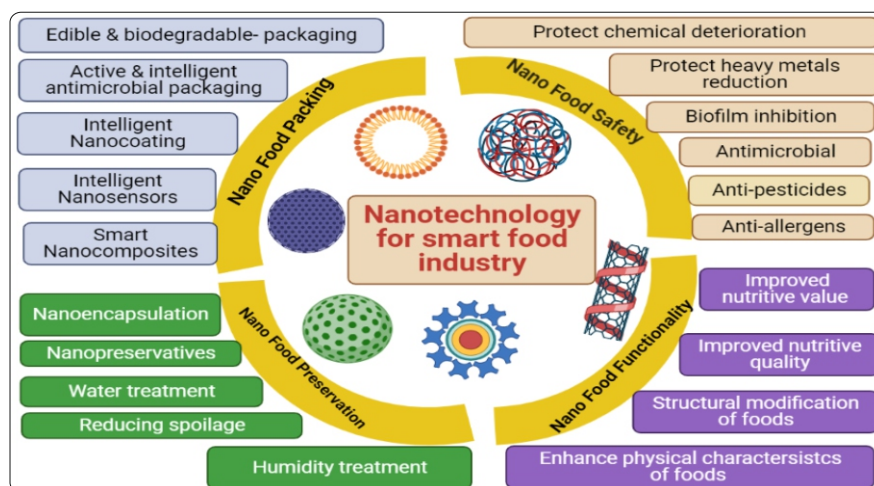
The potential exists for nano technology to be a game changer in terms of future disruptive technologies. Scientific and technological advances have the ability to affect our military's fighting capabilities. The world's leading defence industries are investing extensively in developing new nanotechnology-based products. Current nanotechnology studies concentrate on bettering healthcare infrastructure and developing lightweight, durable, and multipurpose materials for use as armour to increase safety and connectivity in network-centric battlefields. Having looked at the military applications, I covered the impact these

would have on modern warfare in my next slide, as described hereafter.

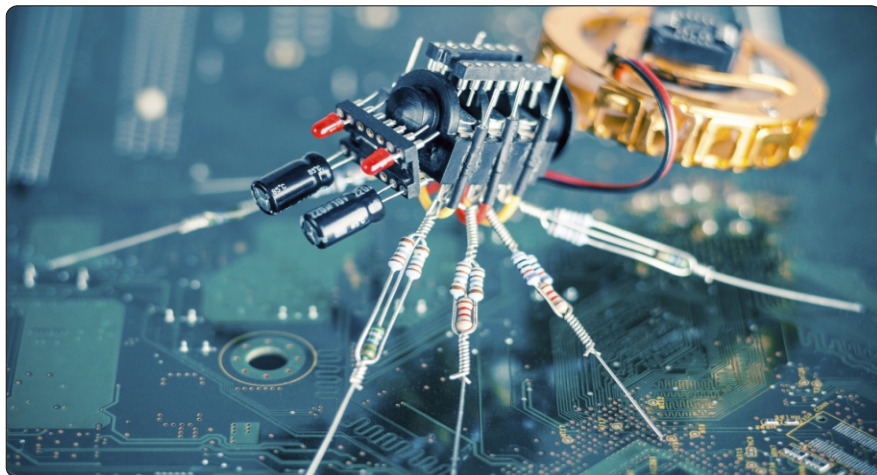
- (a) **Decision Support.** The direct impact of nanotechnology on decision-making is limited. However, improving essential abilities such as communication, computers, and surveillance can have a noticeable impact. While nano technology may not directly affect command and control, it can improve communication and battlefield transparency.
- (b) **Mobility.** Nanotechnology-enabled lightweight vehicles will significantly improve military mobility. These vehicles will have improved endurance due to lower weight, improved fuels and lubricants. Miniaturising equipment enables vehicles to carry more, have wider ranges, move faster, and offer more battlefield options.
- (c) **Precision in Engagement.** Nano technology will transform war effects by creating lighter, more durable battlefield systems and weapons, resulting in increased agility, accuracy

and firepower. Nanotechnology-based small drones, satellites, sensors, etc. will open new fronts against the enemy.

- (d) **Robustness.** The mechanical, optical and electrical properties of nanomaterial can be beneficial. Our survival chances can be improved with lighter, stronger armour. Armour for individuals and vehicles will be lightweight and offer better safety against ballistics and explosive glass.
- (f) **Communication.** Small communication devices can be printed on soldier clothing, folded, washed, and carried in a pocket. Miniaturised communication devices would be immensely useful, especially with the rise of autonomous and semi-autonomous systems in a networked battle space.
- (g) **Situational Awareness.** The deployment of numerous small, invisible and durable unattended sensors is particularly desirable in battlefields. Miniature drones and nano satellites boost surveillance



Application of nanotechnology in different areas of the food industry (image credit mdpi.com)



Nano technology in microchips (photo courtesy igyaan.in)

capacities without being detected by the enemy.

- (h) **Logistics.** Nano technology has significant implications for force sustenance. The majority of impacts are secondary, including lighter, more durable vehicles, higher fuel efficiency, reduced maintenance and increased load carrying ability. Battery space may need a much higher power supply. Any capacity to minimise energy load through lighter cars, more efficient systems, or smaller, long-lasting power sources promises more opportunity. Nanotechnology, bio information, and communication technologies could monitor, support, and maintain army capacity during operations.
- (j) **Doctrinal Change.** Nano technology-based systems in the military will have significant effect. Military doctrines must adapt to incorporate, deploy and utilise these systems. Innovative nano technology systems, such as surveillance dust, will redefine intelligence collected from the battlefield.

It would be important for me to also

inform the officers of Indian initiatives in nanotechnology. My research showed that the Indian Government established the Nano Mission in May 2007, investing 10 billion in the 11th Five-year plan to advance nano research and technology for national benefit. Since inception, the mission has funded 240 research projects, including high-performance fuel cells, electro chemical sensors for lung cancer diagnosis, biodegradable nanoparticles for drug delivery, carbon dioxide conversion, early detection of oral and liver cancer. The Union Government established 20 nanotechnology centres around the country.

In 2004, India, the US, Germany, Japan, Russia, and Ukraine formed a national Centre for Nano Materials in Hyderabad to promote bilateral nanotechnology research projects. The Department of Biotechnology, Ministry of Electronics and Information Technology, Department of Industrial Policy and Promotion, and Department of Industrial and Scientific Research are all actively involved in nano technology research, which is a multidisciplinary field.

The Nanotechnology Initiatives Division (NID) aims to strengthen the semiconductor manufacturing ecosystem in the country by conducting cutting-edge research in nano electronics. Biotechnology and nanotechnology are among five important technologies with the greatest potential to boost Indian industry and support national security. I assessed that although India has made progress in nanotechnology, its patenting activity lags behind other countries.

The D Day arrived, and my lecture was received well. The Commander asked me to suggest the way forward for our nation and the Army. I indicated that India needs a comprehensive strategy for developing and commercialising ideas based on nanotechnology. Research in this area might benefit from more funding and the establishment of incentives. Top-tier scientists should be encouraged to invest in nano technology research. There needs to be communication and cooperation between the government agencies, research institutions, universities, industry and think tanks. More enthusiasm from the Government without being hindered by bureaucratic processes is the need of the hour. The nation's economic growth, military prowess and, implicitly, national security, all stand to benefit from active participation in bilateral or multilateral agreements with world pioneers in this field.

For mass production and marketing of nanotechnology, better synergy between academic institutions and industry is also necessary. The Government is also planning to offer tax breaks to the nanotechnology sector and emerging businesses. The advanced countries have also created a workable regulatory framework for nano technology. For India to fully take advantage of nanotechnology's benefits, the country needs to construct a safe, yet research-friendly, regulatory framework that takes human and environmental safety into account. Without this safeguard, a fantastic opportunity may be lost if something goes wrong as a result of our usage of nanotechnology.

The Commander nodded in agreement. In his summing up remarks, he emphasised that **disruptive technologies affect not only military conflicts but also economic growth and overall state power.** The options available to us in foreign policy are further constrained by technological gaps. It would be prudent to invest in expanding our capabilities and our arsenal of cutting-edge technology rather than playing the ostrich and ignoring the fact that they will shape the nature of future battles. The process of identifying and developing/importing these qualities, as well as making the necessary policy, doctrinal, organisational, and mental shifts, can take a long time. This can only be achieved by a combination of political will and military leadership at the highest levels of the nation.

As we drove back to the unit, the CO complimented me and remarked that our talents and limitations are as different as India's problems. After observing the effects of technology on the way the United States conducts war in previous operations, the Indian military has begun the process of ushering in modernization.

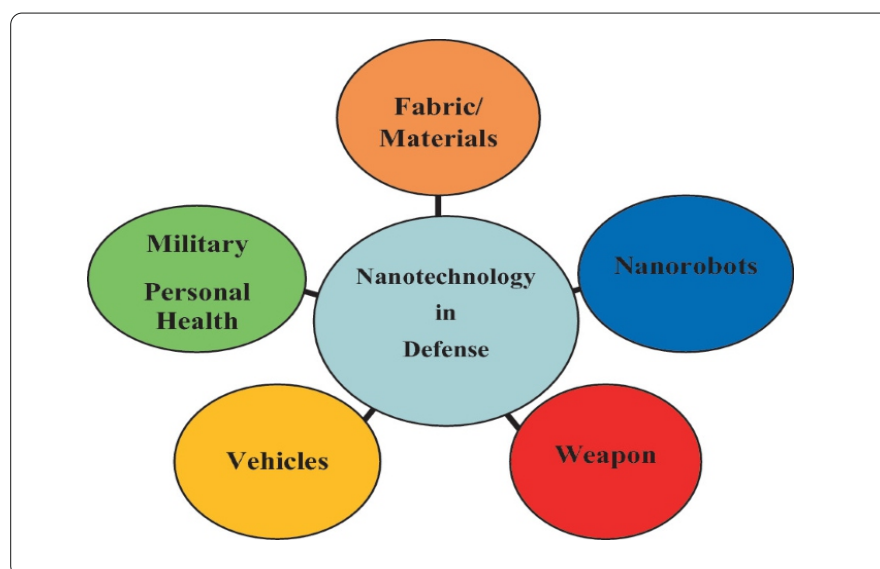
There will always be obstacles in the path to modernization, such as acquiring strategic and niche technologies, developing creative concepts to exploit new technology, and managing people and organisations to maximise the value of available resources.

I added that there are examples of technologies that were originally designed for military use but later proved to be a boon for civilians; for instance, advancements in aviation were sparked in the First World War. Access to a few of these niche technologies by non-state actors or a band of criminals is a danger too, this potential risk must be recognised and guarded against appropriately. The CO concluded that if India wants to be taken seriously on the international stage, it must continue to invest in these technologies, as advanced nanotechnology capabilities may determine the balance of military power between states.



Lt Col Rahul Hermon

Lieutenant Colonel Rahul Hermon was commissioned into the Corps of Signals in December 2008. A third generation Army officer, he has served in various terrain including in a Rashtriya Rifles battalion, where he was awarded the Army Commander's Commendation Card. He has been an Instructor at the Military College of Telecommunication Engineering, Mhow, and then went on to do his M.Tech. in Cyber Security from the Defence Institute of Advanced Technology, Pune. An excellent tennis player, he has represented the Corps of Signals Team twice in the Pentangular Sports Meet. He is married to Lieutenant Colonel Aditi Bhonsale (Retd).



Nanotechnology applications in the defence sector (Image credit link.springer.com)

STRIKING SHADOWS - THE BIOMETRIC DANGER

EXPLOITING BIOMETRIC PROFILES TO TARGET CRITICAL LEADERSHIP

Electronic warfare (EW) plays a critical role in modern military operations by harnessing electromagnetic energy to exploit, deceive, or attack an adversary's electronic systems. The incorporation of Artificial Intelligence (AI), robotics, and cyber security has added new dimensions to electronic warfare capabilities. Adversaries leverage the Electromagnetic Spectrum to disrupt command and control structures, impeding decision-making processes. This article discusses how biometric profiles are built up and used to target senior leadership.

Introduction

AI contributes significantly to EW, enhancing signal processing, electronic countermeasures, threat assessment, and autonomous EW systems. Robotics complements EW through the deployment of unmanned aerial vehicles (UAVs), robotic ground vehicles, and autonomous underwater vehicles (AUVs). Cyber security measures are indispensable for safeguarding EW systems from cyber-attacks, ensuring secure data handling, and maintaining network resilience.

Electronic Attack serves as a strategic tool, intentionally interfering with communication channels to create chaos within the adversary's leadership. The psychological impact is significant, aiming to demoralize forces and weaken the resolve of opposing leadership.

Beyond military applications, Electro Magnetic Spectrum Operations (EMSO) finds relevance in cyber and electronic warfare, spanning from counterterrorism to high-end conflicts. Vulnerabilities lie in unsecured networks, which are susceptible



to deception. Reliance on digital communication is also a weakness, and the recent use of entirely non-digital and analog devices by Hamas is a stark example of how “outdated” communication networks may be more secure from modern surveillance.

Threats against critical leadership include cyber-attacks, misinformation campaigns, and intercepted communication. Protecting critical leadership requires robust cyber security measures, real-time threat monitoring, and ensuring information integrity. While these technologies are potent tools in modern conflicts, they also pose challenges, necessitating a delicate balance for the security of critical leadership.

Exploitation of Biometric Signatures

Adversaries may exploit biometric data for espionage and intelligence gathering, as well as physical destruction and exploitation of leadership, by identifying emotional

vulnerabilities. Embedding GPS and sensitive receiver tags with RF systems in critical resource targets is a covert tracking and monitoring tactic with significant implications, and adversaries may utilize this tactic to gain intelligence, target specific assets, and disrupt an enemy's capabilities. One may recall how the United States targeted Qasem Soleimani, the Iranian Republican Guards leader in Baghdad. Let us look at the various layers which add up to make the biometric picture of a critical leader.

Voice Identification: Leaders' voices, akin to musical notes in a symphony, hold a distinctive tonality and pitch that contribute significantly to their unique biometric signature. The way they articulate their thoughts, coupled with subtle speech patterns and accents, forms a vocal fingerprint that aids in swift identification. This auditory signature becomes a key element in understanding the essence of their communication style and adds a layer of individuality to their leadership persona.

Physical Characteristics: Beyond the audible, the physical attributes of leaders are woven into their biometric narrative. Their movements, a dance of biometric patterns, convey a distinct physical body signature. From the subtle gestures that punctuate their expressions to the facial features that define their presence, advanced biometric systems discern a unique identity. In this intricate choreography of physicality, leaders reveal a silent but compelling story of who they are.

Behavioural Analysis via Social Media: In the digital landscape, leaders leave behind a trail of their online existence. This digital footprint tells a tale of their preferences, interactions, and engagement style. The content they choose to share, the tone of their online

expressions, and their interactions with a global audience become chapters in the narrative of their behavioural profile. Social media platforms, akin to modern-day storytellers, unveil a facet of leaders' lives beyond the public eye.

Communication Channels and Recorded Messages: Speech, a vessel for conveying thoughts and emotions, is meticulously analysed in the biometric saga. From scripted speeches delivered on formal stages to unscripted moments captured in recorded messages, leaders imprint their linguistic fingerprint. The words chosen, the emotional resonance embedded in their communication—all contribute to a comprehensive understanding of their behaviour. Each speech becomes a chapter, revealing layers of their character.

Participation in Conferences and Interactions with Troops: On the stage of public engagements and interactions with troops, leaders reveal a dynamic aspect of their identity. Public speaking engagements offer insights into their communication style, rhetoric, and language use. Meanwhile, personal interactions, especially with troops on and off the battlefield, paint a human portrait of leadership. These interactions become poignant chapters that showcase not only the leader's communication prowess but also their ability to connect on a personal level.

Individual Preferences, Decision-Making Styles: Away from the spotlight, leaders exhibit peculiar likes or dislikes, enriching the narrative of their personality. Examining these preferences—be it in hobbies, cultural interests, or personal habits—adds depth to the biometric story. Similarly, the approach a leader takes to decision-making, whether consultative,

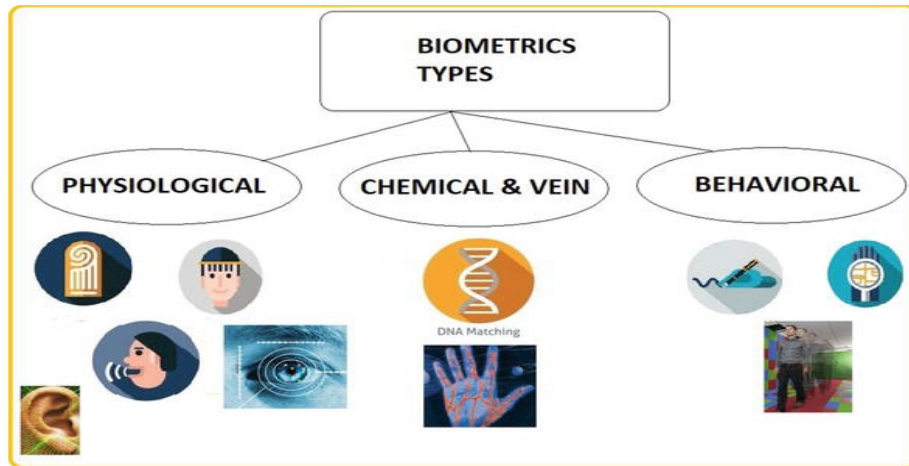
authoritative, or consensus-driven, forms a crucial chapter in the unfolding tale of their behaviour. These nuanced aspects highlight the individuality within the realm of leadership.

Views and Expressions: A leader's stance on key issues becomes a defining chapter in their biometric narrative. The examination of their views contributes to a broader understanding of their ideological and policy viewpoints. The consistency or evolution in expressed views over time adds layers to the behavioural analysis. These chapters shape the narrative of a leader's thought processes and provide insights into their strategic perspectives.

Eye Movements and Overall Behavioural Analysis: In the windows to the soul, leaders' eyes tell a silent story of cognition and emotion. Analysing eye movements during speeches or interactions offers glimpses into their cognitive processes. The subtle cues, such as pupil dilation during various scenarios, become signals that unravel emotional responses and engagement levels. When these elements are integrated, a comprehensive contextual understanding of the leader's behavioural patterns emerges—a story enriched by their unique likes or dislikes and decision-making styles.

Risks and Implications

The exploitation of vulnerabilities in EW poses risks such as covert surveillance, targeted actions, logistical disruption, counter-intelligence compromise, signal interception and spoofing, jamming and denial of service, data compromise, and weaknesses in biometric recognition systems. A couple of these are amplified hereafter.



Biometric types (image credit intechopen.com)

Covert Surveillance (Tracking and Intelligence Gathering): The exploitation of vulnerabilities opens the door to covert surveillance, an insidious intrusion into the very heart of operational secrecy. Adversaries, armed with a nuanced understanding of vulnerabilities, can surreptitiously monitor activities, gaining invaluable insights into military strategies, troop movements, and sensitive operations. Embedding GPS and sensitive receiver tags allows adversaries to monitor the movements and locations of enemy personnel, equipment, and vehicles in real-time. Continuous tracking can provide data on patterns, routines, and operational activities, potentially revealing vulnerabilities or opportunities for attack.

Targeted Actions: Vulnerabilities become gateways for adversaries to orchestrate targeted actions, pinpointing critical assets or leaders. This strategic manoeuvring allows them to exploit weaknesses in defence systems, launching precise and debilitating attacks that can cripple communication channels, disrupt strategic infrastructure, or compromise critical resources. Adversaries can use the

gathered information to launch targeted attacks against specific critical resources, leading to disruptions or even casualties. Knowing the location and movements of enemy forces enables adversaries to set up ambushes or other tactical actions.

Mitigation of Vulnerabilities

Implementing comprehensive security measures, including physical security, encryption, biometric spoofing detection, multi-factor authentication, access control policies, cyber security practices, counter-intelligence, and insider threat programmes, education and training, leadership training, family security, personal security measures,

intelligence sharing, and crisis response plans, is crucial for safeguarding biometric data and protecting critical leadership.

Muffling or preventing the voice signature, also known as voiceprint, involves taking measures to make it more challenging for voice recognition systems to identify and authenticate your voice. Though it's impossible to eliminate your voice signature entirely, some tips to reduce it are:

- **Change Your Speech Patterns:** Experiment with altering your pitch, tone, and speaking speed. Try to vary these elements to disrupt the consistency of your voice.
- **Use Different Accents or Dialects:** Incorporate different accents or dialects into your speech. This can introduce variability that makes it more difficult for voice recognition systems to create a reliable signature.
- **Background Noise:** Introduce background noise when speaking, as it can interfere with the clarity of your voice. However, be cautious not to make it too excessive, as it may also hinder communication.
- **Speak Softly or Whisper:** Lowering your voice or whispering can make it more challenging for voice recognition systems to capture distinct features of your speech.
- **Use Voice Modulation Software:** Consider using voice modulation software that can alter your voice in real-time. These tools can adjust pitch, tone, and other characteristics to make your voice sound different.
- **Employ Text-to-Speech Tools:** Convert your spoken words into text and use a text-to-speech tool to generate the audio. This introduces an additional layer of abstraction, making it harder for voice recognition systems to identify your unique vocal characteristics.
- **Limit Vocal Samples Online:** Be cautious about sharing voice

recordings online, as these can be used to create voiceprints. If possible, avoid participating in voice-activated systems that store your voice data.

• **Disable Voice Recognition**

Features: Turn off voice recognition features on devices and applications when not needed. This limits the opportunities for your voiceprint to be captured and stored.

• **Use Voice-Changing Apps:**

Explore voice-changing applications that can modify your voice in real-time. These apps can be used during voice communication to add an extra layer of protection.

The Social Media Addiction

While it is essential to be mindful of the online presence and take precautions against potential risks, here are some additional counter-measures to minimize the risk of critical leadership profiling through social media:

• **Limit Personal Information:** Be cautious about the amount of personal information you share online. Minimize details about your work, location, and daily activities to reduce the risk of potential exposure.

• **Review Privacy Settings:** Regularly review and adjust the privacy settings on your social media accounts. Limit the visibility of your profile to only those you trust, ensuring a more controlled online environment.

• **Be Mindful of Connections:** Exercise selectivity in connecting with others on social media. Be cautious about the people you connect with, avoiding individuals you do not know or trust to mitigate security risks.

• **Use Separate Accounts:** Consider creating separate accounts for personal and professional use. This practice helps compartmentalize your online presence,

enhancing privacy and security.

• **Change Usernames and Handles:** Periodically change your usernames and handles to make it more challenging for anyone tracking your online activity. This proactive measure adds an extra layer of protection.

• **Use Virtual Private Networks (VPNs):** Employ VPNs to mask your IP address and enhance online privacy. This makes it more difficult for someone to trace your online activities back to your physical location, bolstering overall security.

• **Rotate Devices:** Avoid consistently using the same device for all online activities. By rotating between different devices, you make it harder for someone to correlate your online presence, adding an element of unpredictability.

• **Regularly Audit Online Presence:** Conduct regular audits of your online presence. Search for your name and assess the information that is publicly available to proactively manage and control your digital footprint. This practice enables better awareness and security.

Stay Safe – The Precautions

In conclusion, adopting a forward-looking approach is imperative for the sustained protection of biometric data, critical leadership, and the overall integrity of military, intelligence, and security operations. The way forward involves implementing comprehensive security measures, incorporating continuous risk assessments, and conducting regular security audits to stay ahead of evolving threats. An essential component of this strategy is an awareness campaign, particularly emphasizing the individual profiling of critical leadership through biometric

signatures in the cyber and electromagnetic spectrum domain of social media. Additionally, stakeholder training plays a pivotal role in enhancing the understanding of these risks and fostering a culture of vigilance. **Furthermore, effective regulation of communication and data storage systems is indispensable to ensure data security and prevent unauthorized access or pilferage.** By embracing these measures, organizations can establish a robust defence against emerging threats, thereby safeguarding sensitive information, critical leaders, and the overall integrity of their operations.



Col (Dr) VKT Mishra

Col (Dr) VKT Mishra (Retd), from the Corps of Signals is a Fellow of IETE and a Cyber Electronic Warfare Subject Matter Expert with over three decades of experience in EW. He had commanded an EW battalion and served in EW establishments for over a decade including holding of a Senior Faculty assignment in EW Wing, MCTE. He has also been the Commander All Arms Wing at MCTE. A member of Mhow Analysis and Research Society presently, he is a Professor of Practice in MediCaps University, Indore, and visiting faculty in EW Wing at MCTE Mhow.

EDGE COMPUTING

In the last couple of decades, Network Centric Warfare, has been at the centre of many discussions. As technology marched ahead, the transformation of warfare towards network-centricity has been inevitable. The large amount of data from sensors, shooters and computing power as well as reliable networks required to handle warfighting pose immense tech challenges. Edge Computing provides one of the possible ways to handle these complex requirements. Realising its importance in future battlefields, we decided to have a tete'-a-tete' with Brigadier Subhash Katoch (Retd), our Tech Wizard.



Edge Computing (image credit spec-india.com)

So, Subhash, what is Edge Computing?

Edge Computing is the process of bringing information storage and computing abilities closer to the devices that produce that information and the users who consume it. Traditionally, applications have transmitted data from smart devices like sensors and smartphones to a central data centre for processing. However, the unprecedented complexity and scale of data have outpaced network capabilities. By shifting processing capabilities closer to users and devices, edge computing systems significantly improve application performance, reduce bandwidth requirements, and give faster real-time insights.

What then are the benefits of Edge Computing?

You will be amazed to learn that there are many benefits, like

- Reduced latency / increased speed. In many industries, technology demands almost instant

transfer of data. Take the example of a piece of robotic machinery on a factory floor. If a production incident makes it unsafe for that robot to keep operating, it needs to receive that information as fast as possible so it can shut down.

- Improved data security. With Edge Computing, the majority of data is processed and stored locally. Any information that needs to be sent back to the data centre can be encrypted before transmission. Enterprises also use edge computing to comply with data sovereignty laws, such as the General Data Protection Regulation (GDPR), by keeping any sensitive data close to the source.

- Increased productivity. Enterprises improve operational and employee productivity by responding more quickly to information. By analysing data collected at the source, organisations can improve areas of their facilities, infrastructure, or equipment that are underperforming. Edge Computing can be teamed with Artificial Intelligence (AI) and Machine Learning tools to derive business intelligence and insights that help employees and enterprises perform more productively.

- Remote data collection. It is challenging to collect data from places with unreliable connectivity and bandwidth. Establishing compute and

data storage capabilities at the network edge helps enterprises collect and transmit data from distant oil fields, industrial zones, and offshore vessels.

- Reduced costs. Sending large quantities of data from its origin to centralised data centres is expensive because it requires more bandwidth. The Edge Computing model allows you to decrease the amount of data being sent from sites to data centres because end users only send critical data. Depending on how much data your business sends and processes, this could significantly save operating costs.

- Reliable performance. Edge Computing often takes place in remote areas where internet connectivity is weak. By setting up an Edge Computing environment, enterprises ensure that their operations reliably process, analyse, and store data. This significantly reduces the chances of suffering from operational downtime caused by network or connectivity disruption.

So, Edge Computing is widely in use in the Industrial Sector?

Yes, the high speeds and low latency of data transfer, combined with the relative ease of installing Edge devices, have seen Edge Computing being widely used across industries. Some examples are-

- Manufacturing. The proliferation of Internet of Things (IoT) devices such as sensors and gateways has made Edge Computing systems prevalent in the manufacturing industry. Manufacturers utilise Edge Computing solutions to enable automation, collect data on-site, improve production efficiency, and allow rapid machine-to-machine communication.

- Autonomous vehicles. Autonomous vehicles like self-driving cars are fitted with several IoT sensors that

collect large amounts of data every second. They require real-time data processing for instant response and cannot rely on a remote server for split-second decision-making. Additionally, autonomous vehicles interact more efficiently if they communicate with each other first, as opposed to sending data on weather conditions, traffic, accidents, or detours to a remote server. Edge Computing is critical technology for ensuring their safety and ability to accurately judge road conditions.

- Energy. Energy companies use Edge Computing to collect and store data on oil rigs, gas fields, wind turbines, and solar farms. Rig operators commonly deploy Edge AI to detect hazards and optimise and inspect their pipelines. Edge Computing helps the industry improve operational efficiency, keep its workers safe, and forecast when maintenance work needs to be undertaken.

- Healthcare. Edge devices monitor critical patient functions such as temperature and blood sugar levels. Edge Computing allows the healthcare sector to store this patient data locally and improve privacy protection. Medical facilities also reduce the data volume they send to central locations and cut the risk of data loss.

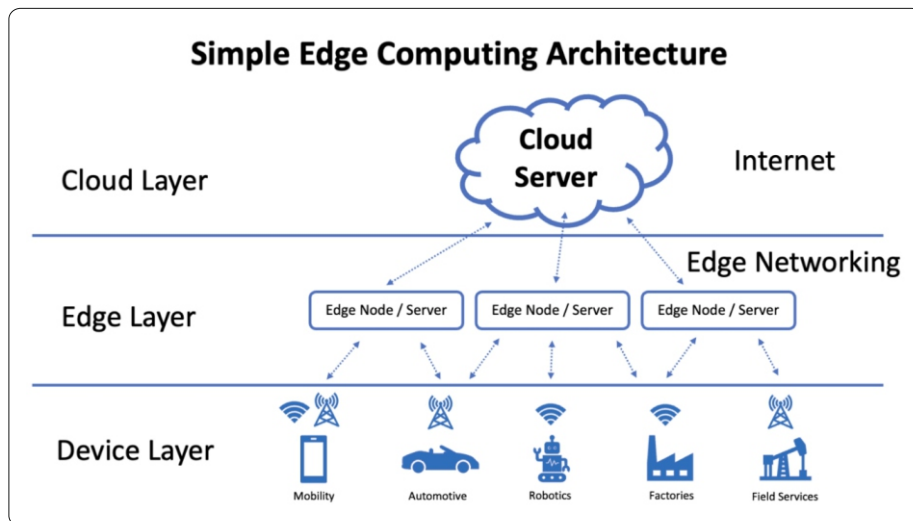
- Agriculture. Edge Computing has made precision agriculture a reality. By deploying sensors and cameras in fields, farms can collect real-time data on soil conditions, weather, crop growth, and pest infestations. This data is processed locally, allowing for immediate adjustments in irrigation, fertilizer selection and pest control.

I know that Edge Computing can be of great use in the defence sector too. Can you amplify?

The concept of Network Centric Warfare (NCW) has been adopted as a military doctrine by most countries worldwide. The idea is that battlefield advantage can be gained through a network of robustly connected forces to improve information sharing, which in turn improves situational awareness and decision-making responsiveness, dramatically improving mission effectiveness. Modern Defence Forces need a Common Information Grid (CIG) as the primary communication framework to support NCW operations. The CIG is a wide interconnected, end-to-end set of information capabilities for sensing, collecting, processing, storing, disseminating and managing information on demand to warriors, policy makers and support personnel.

In a network centric environment consisting of a geographically dispersed and interconnected system of systems, the collection, storage, processing and dissemination of information represents a major technical challenge. The use of cloud and Edge Computing in a military context, combined with use of real-time data connectivity enabled by common protocols and standards, offers great potential to effectively address these hurdles. Another set of concerns relate to the sheer volume, variety and velocity of data produced by network centric military applications that have grown exponentially. This poses many challenges with respect to how to manage, process and share the data in systems containing Edge networks, limited computing resources, limited network bandwidth where connectivity to centralised command and control systems is not always guaranteed.

The cloud computing paradigm



Edge Computing Architecture (image credit wipro.com)

works effectively till the tactical edge, such as on the battlefield where mission requirements are dynamic and fast changing, and where the need for computing power is great but network communications are much more challenging - specifically, due to intermittent connectivity with the core networks, limited network bandwidth and high network latency.

Edge Computing or small clouds at the Edge, address the limitations of cloud computing at the tactical edge. Cloudlets consist of servers and communication equipment that are deployed on the battlefield, typically hosted on a vehicle or other platforms in the proximity of the troops. They offer computational offload capabilities to mobile forces, forward data staging for a mission, provide data filtering for streams intended for dismounted users and also are a collection point for data heading to the cloud or other battlefield Edge nodes. Tactical Cloudlets can continue to be used even if disconnected from the core network.

In effect, you are implying that Edge Computing is imperative for the modern battlefield.

Yes, in the modern battlefield full of sensors, long-range precision weapons, drones, robotic systems and an intense ever changing environment, Edge Computing will enable:

- Real-time Data Analysis:

Military operations generate vast amounts of data from sensors, drones, satellites, and other sources. Edge Computing allows for the processing and analysis of this data right at the source (the "Edge"), enabling real-time decision-making without relying on distant data centres.

- Reduced Latency:

Edge Computing minimises data transmission delays by processing critical data locally. This is crucial for applications like remote drone control or autonomous vehicles, where split-second decisions can be a matter of life or death.

- Enhanced Security: Armed Forces deal with highly sensitive data that needs to be protected from cyber threats. Edge Computing can provide an additional layer of security by processing data locally, reducing the risk of data breaches during data transmission to centralised servers.

- Improved Bandwidth Management: In remote or hostile environments, network bandwidth may be limited or unreliable. Edge Computing reduces the dependency on a constant connection to a centralised server, allowing critical tasks to continue even when network conditions are suboptimal.

- Edge Devices for Surveillance: Surveillance cameras and sensors at the Edge can process data locally, identifying potential threats, and transmitting only pertinent information to central command centres. This reduces the burden on network infrastructure and allows for faster threat detection.

- Autonomous Systems: Edge Computing is essential for autonomous systems such as Unmanned Aerial Vehicles (UAVs) and autonomous ground vehicles. These systems can process sensor data in real time, making independent decisions without human intervention.

- Military Wearables: F-INSAS or Future Infantry Soldier As a System where soldiers can wear Edge devices like smart helmets that provide real-time battlefield data, navigation assistance, and communication capabilities without the need for centralised infrastructure.

- **Ruggedised Hardware:** Edge devices used in defence applications would need to be ruggedised to withstand harsh environmental conditions, ensuring they remain operational in extreme situations.

- **Scalability:** Edge Computing solutions can be deployed in a scalable manner. New Edge devices can be added as needed, making it adaptable to changing mission requirements.

- **Redundancy:** Edge Computing can provide redundancy in case of central server failures. Critical functions can continue to operate independently at the Edge even if central systems are compromised.

In summary, Edge Computing empowers the Armed Forces to process, analyse, and act on data quickly, securely, and efficiently in the field, contributing to improved situational awareness and mission success.

What advances do you foresee coming up in this field in the coming years?

Maturing technologies are making the Edge more efficient, reliable and easier to manage:

- **5G** makes Edge implementations seamless by guaranteeing the transmission of critical control messages that enable devices to make autonomous decisions. This last-mile technology connects the Edge to the internet backhaul and ensures that Edge devices have the right software-defined network configurations to do the right things.

- **IoT** and connected devices are unique data sources that need to be secured and registered in the cloud. Edge will reside near or on these data sources.

- **Containers.** Containers are packages of software that contain all the necessary elements to run in any environment. They virtualise the operating system and run anywhere, providing a

standardised deployment environment for developers to build and package applications. Containers can be deployed on various hardware, regardless of device capabilities, settings and configurations.

- **Service and data mesh** provide a way to deploy and query data and services distributed across containers and data-stores across the Edge. These meshes present a single interface that abstracts away the routing and management of services and data interfaces. This critical enabler makes possible bulk queries for entire populations within the Edge, rather than on each device.

- **Software-defined networking** allows users to configure the overlay networks. It also makes it easy to customise routing and bandwidth to determine how to connect Edge devices to each other and to the cloud.

- **Digital twin** is a critical enabler that organises physical-to-digital and cloud-to-Edge. The twin allows data and applications to be configured using domain terms around assets and production lines rather than database tables and message streams. Digital twins allow domain experts (rather than software engineers) to configure applications to sense, think and act on the Edge.

- Other technologies like **AI and blockchain** are also making Edge more powerful. For example, when AI acts on data at the Edge, it reduces the need for centralised compute power. Edge also makes blockchain better as more reliable data leads to greater trust and less chance of human error.

Data can be captured and relayed directly by machines in real-time, and the increased use of sensors and cameras on

the Edge means more and richer data will become available to analyse and act on. Edge is also leading a revolution in automation, moving from systematic processes in closed, controlled environments like factories to complex performances in open, uncontrolled environments like war fighting and agriculture.

Wow, these are indeed disruptive changes which will alter the way we operate in the future. Your inputs will undoubtedly give greater insight to our future warriors. Thank You.



Brig Subhash Katoch

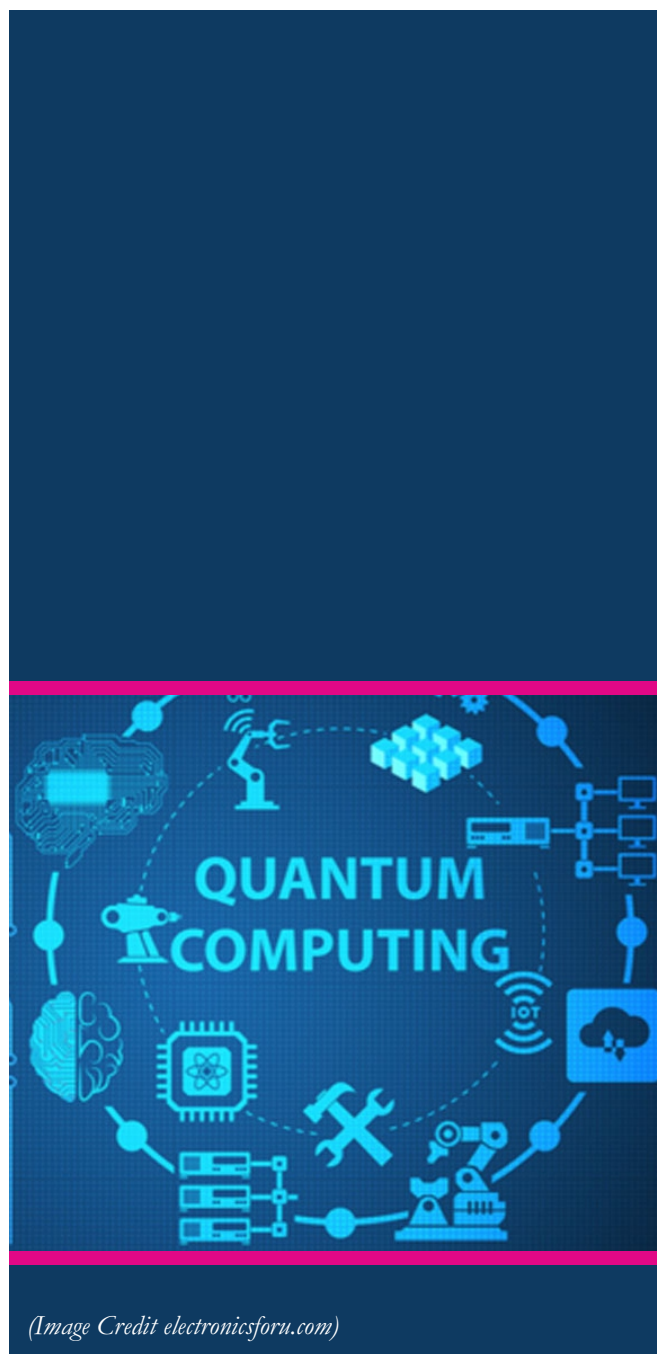
Brig Subhash Katoch (Retd) is a highly qualified professional with comprehensive experience in military telecommunication technologies, data networks, cyber security, data science and analytics, decision support systems, automation, EMI/EMC testing and compliance. He holds a MBA from FMS, Delhi University, and is an M.Tech. (Computer Science and Technology) from IIT, Madras. He is also a Fellow of the Society of EMC Engineers, India and is on the Guest faculty for 'Business Intelligence & Business Analytics' at Faculty of Management Studies (FMS), Delhi University since 2014.

QUANTUM TECHNOLOGY AND MILITARY OPERATIONS

FROM THE LAB TO THE BATTLEFIELD

In today's ever-evolving landscape of modern warfare, technology has consistently played a pivotal role in shaping the strategies and capabilities of military forces around the world. From the Industrial Age to the Information Age, each era has brought forth innovations that have redefined the way conflicts are fought and resolved. As we stand at the precipice of a new era, quantum technology is poised to usher in a revolution that could transform the very nature of warfare itself. It is envisaged to be 'emerging' & disruptive both. In this article, we will delve into the disruptive power of quantum technology and how it stands to reshape the battlefield, from secure communication channels and unbreakable codes to ultra-precise navigation and intelligence gathering.

As a young boy, I was always fascinated by gadgets, technology and scientific advances. I joined the Corps of Signals, and my knowledge in the field of electronics and communications got a fillip. As I understood the intricacies of electromagnetic spectrum, cryptography and computers, my passion in technological advances was further enhanced during a course at the Military College of Telecommunications (MCTE) at Mhow. MCTE has taken a lead in the domain of Quantum Technology by establishing the first Quantum Tech Lab in the tri-services. Quantum Technology and its amazing capabilities fired up my zeal. **So what is Quantum Technology?**



Bastions of Quantum Tech

- **Fundamentals: Unravelling the Quantum World.** Quantum technology might sound like science fiction, but at its core, it is built upon a few mind-bending principles of quantum mechanics that are as real as they are astonishing. Based on these concepts the domain is divided into 3 main heads – Quantum Computing, Quantum Sensing and Quantum Communication.
- **Quantum Superposition: A Tale of Schrödinger's Cat.** Imagine a cat in a sealed box with a vial of poison.

According to quantum mechanics, before we open the box and observe the cat, it exists in a state of superposition – simultaneously alive and dead. This concept, famously illustrated by Schrödinger's cat, is a fundamental property of quantum particles. In quantum technology, superposition enables the processing of multiple pieces of information at once, leading to the creation of incredibly powerful quantum computers.

- **Quantum Entanglement: The Einstein-Podolsky-Rosen Paradox:** Entanglement is the phenomenon where two particles become so intimately connected that the state of one instantly influences the state of the other, regardless of the distance separating them. Think of it as having two coins that always show the same side, no matter how far apart they are. This concept forms the basis for quantum teleportation and secure quantum communication, allowing for un-hackable connections even in the most hostile digital environments.

- **Quantum Uncertainty: Heisenberg's Microscopic Mystery.** Heisenberg's Uncertainty Principle states that you can never simultaneously know both the position and momentum of a particle with absolute precision. This concept is akin to trying to precisely measure both the speed and location of a race car as it zooms around a track. Quantum uncertainty has profound implications for quantum sensors, enabling incredibly precise measurements in various fields, including navigation and detection of stealthy threats. Understanding these quantum principles is the key to unlocking the potential of quantum technology in military applications, allowing for secure communication, navigation, and computational capabilities that were once deemed impossible.

- **Qubits : The Marriage of 0 and 1.** Qubits may be perceived as the ultimate jugglers, seamlessly blending 0s and 1s in a way that classical bits can only dream of. This unique property allows quantum computers to perform complex calculations exponentially faster than classical counterparts. It is like having a calculator that can solve equations as fast as you can type them, redefining the boundaries of computational power.

- **No Cloning Theorem.** The information of one quantum particle cannot be replicated or cloned onto other particle. Every quantum particle is unique in nature. It gives an immense advantage in making hack-proof communication channels be it optical fibre link or free space optics links.

- **Measurement.** To observe a quantum state, it needs to be disturbed. Simply put, one cannot observe the contents in a box without opening it. This principle also is a key factor in designing paradigm shifting secure communication links.

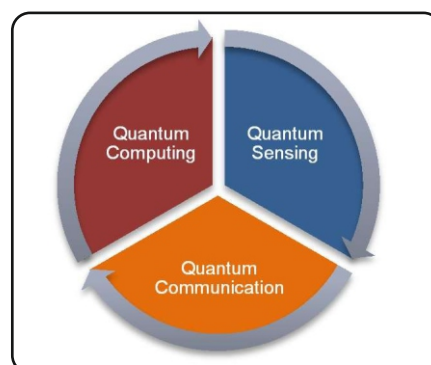
Quite confusing to those not well-versed in physics and electronics, but let us look at the potential military applications of quantum technology. **Why? Because this cutting-edge field will not merely fit into the future of**

warfare; it will redefine it. To understand the profound implications of quantum technology on military strategy, I intend to examine specific applications that will shape the future of warfare.

Potential Military Applications

QKD: The Quantum Seal on Your Messages. In an era where data breaches are commonplace, securing communication channels is of paramount importance. Quantum Key Distribution (QKD) offers a gigantic leap in this domain. Imagine sending a top-secret letter to a trusted recipient. In the world of classical encryption, one would use a traditional lock and key to secure the message. The risk here is that if an eavesdropper intercepts your message, they might be able to obtain the key and unlock the letter. Now, enter the quantum world. With QKD, instead of a physical lock, you and the recipient share a quantum-generated secret that can be used as a key to unlock your message. This quantum key is established using the bizarre properties of quantum mechanics, making it theoretically impossible for an eavesdropper to intercept it without leaving a detectable trace. In essence, QKD provides an unbreakable seal on your messages, ensuring that your communication remains secure, even in the face of the most determined adversaries. This is the essence of QKD, where quantum mechanics ensures unbreakable encryption, a game-changer for secure military communication.

Quantum Computers: Solving the Unsolvables. Imagine managing a colossal jigsaw puzzle with an astronomical number of pieces. A











 <p>Calculates with qubits, which can represent 0 and 1 at the same time</p>	 <p>Calculates with transistors, which can represent either 0 or 1</p>
 <p>Power increases exponentially in proportion to the number of qubits</p>	 <p>Power increases in a 1:1 relationship with the number of transistors</p>
 <p>Quantum computers have high error rates and need to be kept ultracold</p>	 <p>Classical computers have low error rates and can operate at room temp</p>
 <p>Well suited for tasks like optimization problems, data analysis, and simulations</p>	 <p>Most everyday processing is best handled by classical computers</p>

Figure 1 : Comparing Quantum & Classical Computers (Quantum Computers aspects listed in left column)

classical computer might take centuries to solve it, but a quantum computer can solve it in seconds. The 'unsolvable' puzzles in military simulations, cryptography, and optimization problems suddenly become tractable. Quantum computers open doors to innovations that will reshape the landscape of warfare and problem-solving on a grand scale. By understanding these additional concepts of qubits, QKD, and quantum computers, we gain a further insight into how quantum technology is poised to redefine military applications in communication, encryption, and data processing. The comparison between Classical & Quantum computers is shown in Figure 1 above.

Quantum Networks: The Highway of Quantum Information. Quantum networks are the futuristic information highways that revolutionize data transmission. Traditional networks are like congested city streets, where your data can get stuck in traffic or intercepted by snoopers. Quantum networks, on the other hand, resemble wide-open, high-speed expressways with no traffic jams. Data packets, represented as quantum bits or

qubits, can travel instantaneously and securely from one point to another. It's similar to sending messages via teleportation, ensuring swift and tamper-proof communication, much like characters in science fiction who can instantly transport from one place to another without being intercepted.

Quantum Cyber Security: The Unhackable Digital Vault. Quantum cyber security acts as a virtually impenetrable digital vault for sensitive information. Picture it as a treasure chest that only opens when the rightful owner approaches. Quantum encryption keys can't be stolen without detection, providing a level of security equivalent to a mythical guardian

protecting your secrets. It's like having an enchanted lock on your digital treasure, ensuring that only the chosen key can unlock the secrets, while any unauthorized attempt to breach it would be instantly noticeable.

Quantum Sensors: The Epitome of Precision. Quantum sensors embody the epitome of precision, akin to finely calibrated instruments in a virtuoso's hands. These sensors are analogous to rulers with the capacity to measure with atomic-level precision or compasses that steadfastly point true north, never faltering. They possess the remarkable ability to detect minute variations in physical attributes, such as magnetic fields or gravitational forces, with unparalleled accuracy. Picture a magnifying glass for the unseen realm, providing military forces with the means to navigate with unerring precision and the ability to unveil concealed threats that would otherwise elude notice.

Quantum RF Antennas: The Guardians of Secure Communication. Quantum RF antennas serve as the guardians of secure communication, cloaking sensitive information in a shroud of invisibility. Traditional antennas broadcast information like a public address system in a bustling room, susceptible to eavesdropping by any passer-by. Quantum RF antennas, however, employ the enigmatic principles of quantum entanglement to create a secure channel. They envelope your message in an impenetrable veil, ensuring that only the intended recipient can decipher it, while eavesdroppers encounter naught but incoherent noise. The effect is much like having a private conversation in a soundproof chamber, rendering your communication invulnerable to prying ears.

Quantum Artificial Intelligence – Machine Learning (AI-ML): The Savants of Tactical Insight. Quantum AI-ML represents the savants of tactical insight, transcending the capabilities of conventional

AI. It would process data with a rapidity that leaves traditional AI systems in the dust and represents the peak of the fusion of Quantum Technology with current AI-ML domains, but this is yet to fructify. In the complex realm of warfare, this quantum leap in analytical prowess would reshape the landscape, endowing commanders with a decisive edge.

Envisioning Quantum Advancements in the Indian Army

Quantum technology presents a captivating realm of possibilities for the Indian Army, having the potential to redefine the landscape of defence and national security, underpinned by a suite of sophisticated technologies that transcend the boundaries of imagination. An envisaged Quantum Tech enabled battlespace may be visualized as depicted in Figure 2 below.

Augmenting Command-Control Systems. In the not-so-distant future, quantum-enhanced command-control systems will emerge as the backbone of military operations. These systems will empower commanders with unprecedented real-time insights, akin to wielding a panoramic, instantaneous view of the battlefield, enabling more agile and informed decision-making. Quantum computers are expected to play a significant role in augmenting Command & Control (C2) systems by providing an accurate and precise output by applying effectiveness of quantum computation over data gathered from classical communication channels, human intelligence, Intelligence-Surveillance-Reconnaissance (ISR) data & satellite imagery. Complex algorithmic calculations quickly performed by quantum enabled C2 system will be an extremely efficient tool of quantum technology.

Quantum Sensors. Quantum

sensors will stand as the vanguard of precision, elevating the art of reconnaissance and threat detection. Analogous to instruments of unparalleled accuracy, they will decode the subtlest environmental cues, providing military strategists with tactical advantages previously deemed unattainable. Quantum gas sensors have been tested and proved potent in detection of gases like CO₂ & Methane. With accurate calibration these sensors have successfully detected precise human presence. As instruments of unrivalled finesse, quantum sensors establish a new standard for precision and situational awareness in military operations. Quantum technology based radars theoretically claim to nullify the supremacy of the stealth jets. In the context of the Indian Army, the Positioning, Navigation & Timing (PNT) services can become precise to millimetre or even less, even in the scenario of a GPS denied environment.

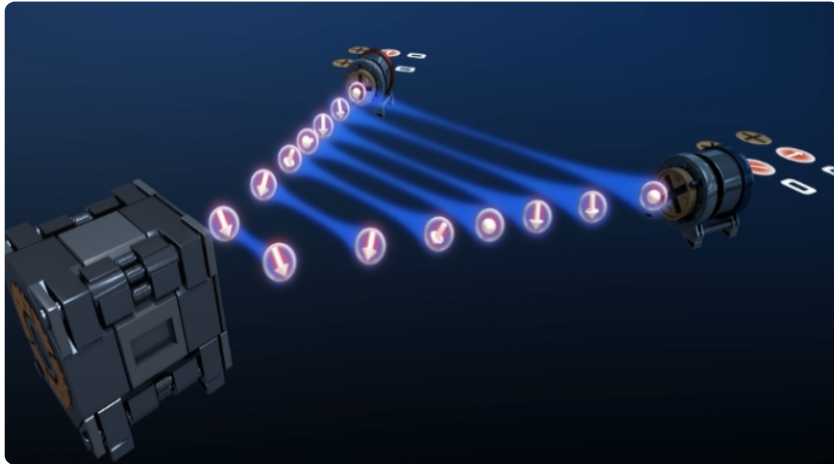
Quantum Imaging: Enhancing Situational Awareness. The evolution of

quantum imaging bestows upon the Indian Army a quantum leap in situational awareness. Much like a grand tapestry, quantum imaging stitches together high-resolution data, providing a nuanced and comprehensive view of complex terrain and dynamic situations. It grants soldiers and commanders a unique vantage point to navigate terrain with uncanny precision and to assess situations with a level of clarity that transcends the current boundaries of perception. Low Light vision device will be very effective in target detection, classification and identification and will potentially counter adversaries' camouflage or other target-deception techniques. Quantum imaging will enhance capabilities of aviation helicopter pilots while carrying out landings in dusty, foggy or smoky conditions.

ISR: Quantum-Powered Stealth and Precision. Quantum technology promises to revolutionize the ISR capabilities of the Indian Army. This



Figure 2. Quantum Enabled Battlespace (Image Credit NATO Modelling and Simulation Centre of Excellence)



Quantum Key Generator

transformation entails the capacity for more agile and discreet intelligence gathering. Quantum ISR is akin to equipping intelligence operatives with a cloak of invisibility as they unobtrusively gather critical information from the shadows. Quantum computers with improved processing will analyse the Big Data from ISR sensors and resources for enhanced situational awareness. This also includes the involvement of quantum-enhanced machine learning and quantum sensors/imaging. Quantum ISR transcends the traditional bounds of reconnaissance, offering a nuanced and sophisticated approach that will shape the future of military intelligence.

Synergized Quantum Operations. The concept of Synergized Quantum Operations heralds a quantum leap in the realm of military coordination and execution. It embodies a transformative approach where quantum technologies converge to orchestrate and optimize military actions with unprecedented precision, efficiency, and synergy. Future combinations of optical and free-space channels will interconnect various end

nodes such as drones, planes, ships, vehicles, soldiers, command centres. In order to achieve a high degree of precision for the C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) systems, quantum clocks will deliver accurate synchronisation of various data and actions in the battle area including radar, electronic warfare, command centres, weapon systems, etc.

MCTE: Pioneering the Quantum Frontier for Military Excellence

Our efforts at MCTE, Mhow have been focussed on indigenous development of user end security through our own efforts and achieving network security through collaboration with industry & academia.

Proof of concepts in quantum computing has also gained traction. In a short span, MCTE has been able to bring the lab on the national map and has published multiple research papers in international forums. The impetus is laid on field army solutions.

The current military scenario is marked by an intricate web of interconnected networks, sophisticated cyber threats, and a constant race for supremacy in areas like communication, intelligence, and cryptography. **In this digital age, the advantages of speed, precision, and security have become paramount, and the military that can harness the potential of emerging technologies gains a distinct edge in any conflict.** The fusion of quantum innovation with the resolute spirit of the Indian Army ushers in a paradigm shift in defence capabilities. The applications of quantum technology for the Indian Army, as expounded throughout this article, herald a future where military operations are underpinned by precision, security, and unparalleled sophistication. The emergence of Synergized Quantum Operations offers a transformative approach where quantum technologies converge to orchestrate and optimize military actions with unprecedented precision, efficiency, and synergy.



Captain Vishwas Sharma was commissioned into Corps of Signals in June 2019. The officer is a B.Sc and Tech graduate in IT and Telecom from Jawaharlal Nebru University. He has served in a Corps Signal Regiment and was involved in Post-Quantum Cryptography projects at Military College of Telecommunication Engineering, Mhow.



Captain Vishwas Sharma



5G TECHNOLOGY

On 27 September 2023, Techfest AVINYA was organized at Military College of Telecommunications Engineering (MCTE), Mhow. Several students from local schools visited the Techfest to give an impetus to their learning experience. One of the inquisitive students asked us about 5G and how does it differ from 4G, 3G, etc. So let us glance through 5G networks and how they benefit the Armed Forces.

We recalled the evolution of mobile communication technologies as we responded to the young boy's query. We elaborated that 1G introduced voice calls in the 1980s, while 2G in the 1990s brought text messaging. The early 2000s witnessed the emergence of 3G, which enabled limited multimedia and internet data access. Then, 4G LTE arrived in the later years of the first decade of this century, providing high-speed data connectivity and enabling the use of various devices for dynamic information access. With the advent of 5G networks, mobile communications are on the brink of a significant transformation. This new era will be characterized by high-density connections, large data volumes, extremely high speeds (20 times faster), remarkably low data transfer latency (10 times quicker), and improved power efficiency. The shift from traditional handset – to – handset communication to machine-to-machine communication will be a hallmark of 5G technology. This transition will not only

support voice and digital conversations but also facilitate the real-time exchange of data, a defining feature of the Internet of Things (IoT), telemedicine, the operation of smart cities, and the performance of autonomous vehicles. Furthermore, 5G is expected to drive progress in IoT, Artificial Intelligence (AI), and Augmented Reality (AR) applications.

For the young students listening to us attentively that day, we amplified that 5G, the fifth generation of wireless technology, brings a host of key features that distinguish it from its predecessors. Some of these are:-

- **Ultra-High Speed.** 5G networks are designed to be significantly faster than 4G. They offer peak download speeds of up to 20 Gbps (gigabits per second) and peak upload speeds of 10 Gbps. This translates to much quicker downloads, streaming, and web browsing.
- **Low Latency.** 5G has extremely

low latency, reducing the delay in data transfer. Latency is expected to be as low as 1 millisecond, making it ideal for real-time applications such as online gaming, autonomous vehicles, and remote surgeries.

- **High Device Density.** 5G is built to support a much higher density of connected devices. This is crucial for IoT, where a multitude of sensors and devices need to communicate simultaneously.

- **Enhanced Capacity.** 5G offers a substantial increase in network capacity. This means that it can handle a higher volume of data traffic without slowing down, which is essential for handling the growing demand for data-intensive applications.

- **Security Features.** 5G incorporates advanced security features to protect against evolving cyber threats and safeguard sensitive data, which is increasingly important in our connected world.

Parameter	4G	5G
Maximum Data rate	1 Gbps	20 Gbps
Use Experienced Data Rate	10 Mbps	100 Mbps
Network Latency	10 ms	1 ms
Maximum Mobility support	350 km/h	500 km/h
Maximum Devices supported per square km	1 million	1 billion
Bandwidth	20 MHz	100 MHz

Comparison between 4G and 5G performance parameters

The key enabling technologies in 5G wireless communication include a variety of advancements and innovations that make 5G networks faster, more reliable, and capable of supporting a wider range of applications compared to its predecessors. 5G utilizes Low Band (Sub 1 GHz), Mid band (1 - 6 GHz) and mmWave band (typically 24 GHz onwards). But it particularly exploits mmWave band to provide significantly higher data rates and capacity. However, mmWave signals have limited ranges and are sensitive to obstructions. Hence sophisticated antenna technologies like Massive Multiple Input Multiple Output (mMIMO) and Beam forming are used to focus radio signals in specific directions, increasing signal strength and reliability for connected devices. It helps optimize network performance and achieve high signal quality.

5G networks use Network Function Virtualization (NFV) for virtualizing network infrastructure and implement them as software. Further, 5G networks use Network Slicing to customize logical networks for different applications. Multi-Access Edge Computing (MEC) reduces

real-time.

- **IoT and Sensor Networks.** 5G based IoT can connect a vast number of sensors and devices on the battlefield, providing real-time data on everything from equipment status to environmental conditions. This data is crucial for situational awareness and decision-making.
- **Smart Soldier.** The integration of 5G into a soldier's equipment and operations can bring about a wide range of benefits. Smart soldier concept can be leveraged using 5G technology to enhance the capabilities, safety, and efficiency of military personnel on the battlefield.
- **Smart Military Bases.** 5G can be used to create smart military bases and camps with interconnected systems for security, energy management, and logistics. This enhances the overall efficiency and security of the base.
- **Autonomous systems.** 5G enables more precise and responsive control of autonomous systems. This is particularly valuable for surveillance, reconnaissance, and target acquisition missions.
- **AR and VR.** 5G can support AR and VR applications for training and simulation purposes. Military personnel can train in realistic environments, improving their readiness and effectiveness.
- **Remote Maintenance and Repairs.** With low latency and high bandwidth, 5G can facilitate remote diagnostics and maintenance of military equipment and vehicles, reducing downtime and maintenance costs.
- **Logistics Management.** 5G can improve the tracking and management of military supply chains, ensuring that resources and equipment are deployed efficiently and securely.
- **Cyber Security.** 5G networks come with advanced security features, making them more resilient to cyber threats. This is essential for

latency for real-time processing in IoT and AR/Virtual Reality (VR) applications, making 5G versatile for various use cases.

5G technology has significant potential in defence applications, offering a range of capabilities to enhance military operations and communication. Some of the key uses of 5G for defence include:

- **Enhanced Communication.** 5G networks provide fast and reliable communication for military personnel in the field. This includes voice communication, video conferencing, and data transfer, ensuring that troops can share critical information in

protecting sensitive military data and communications. However robust SAG-approved encryption algorithms need to be ported on 5G networks for defence usage.

- **AI and Machine Learning.** 5G can support AI-driven applications for data analysis, predictive maintenance, and decision support. Machine learning algorithms can process vast amounts of data quickly, helping with threat detection and intelligence analysis.

- **Tactical Edge Computing.** 5G allows for Edge Computing, which means processing data closer to the source, reducing the need to transmit data to distant data centres. This is valuable for real-time decision-making on the battlefield.

Despite their inherent security features, 5G networks are susceptible to Electronic Warfare jamming and electronic threats from nearby transmitters. Challenges in deploying 5G technology in the military include limited signal penetration through obstacles, the need for extensive tower infrastructure due to short BTS coverage, high infrastructure costs, complex spectrum allocation, and security and privacy concerns due to the increased attack surface.

A global scan of 5G adoption in various world armies reveals a growing trend toward integrating this advanced technology into military operations. The United States military has been actively exploring 5G applications. The US Department of Defence (DoD) has initiated projects to harness 5G for improved communication, real-time data sharing, and the integration of autonomous systems for both tactical and strategic operations. They have also been partnering with commercial carriers to establish 5G test beds. Similarly, China is making substantial investments in 5G

technology for its military. The People's Liberation Army (PLA) is incorporating 5G into various aspects of its operations, including surveillance, logistics, and command and control. China's focus on 5G is part of its broader modernization efforts. In addition, NATO countries and various other nations are exploring the use of 5G for military operations.

India embraced 5G technology development with emphasis on promoting innovation, self-reliance, and national development. In March 2018, India allocated Rs 224 Crores for the **'Indigenous 5G Test Bed'** to develop 5Gi technology, a modified 5G standard, aligning with the Prime Minister's vision. Developed collaboratively, 5Gi includes innovative features, such as the Low Mobility Large Cell (LMLC) concept, aimed at improving rural coverage. Concurrently, the Indian Army established a 5Gi Defence Test bed at MCTE for military Research &

Development and enhanced communication capabilities.

The future is characterized by mobility, wireless connectivity, and intelligence. Every sensor and platform is evolving to incorporate smart features, infusing them with a degree of intelligence. This evolution involves the collection and manipulation of vast amounts of data, with the aim of enabling these devices to make autonomous decisions. Therefore, the significance of 5G technology cannot be overstated. It will deliver real-time surveillance and ensure resilient and uninterrupted communication, meeting the demands of commanders at both tactical and strategic levels. Lastly the strategic importance of 5G cannot be understated, as it enhances national security and defence capabilities while reducing dependence on foreign technologies.



Lieutenant Colonel K Tony Joseph was commissioned into the Corps of Signals in September 2007. The Officer is a BTech graduate in IT and Telecom from Jawaharlal Nehru University and MTech in Communication Systems from IIT Madras. The Officer has served in two Mountain Divisions, Air Formation unit, EW brigade and performed Instructional duties. The Officer was awarded AOC-in-C Commendation Card in 2016 and GOC-in-C Commendation Card in 2023 for exemplary service.



Lt Col K Tony Joseph

Captain Pooja Sharma was commissioned into Corps of Signals in September 2019. The officer is a B.Sc graduate from University of Rajasthan, Tech graduate in IT and Telecom from Jawaharlal Nehru University and MA from University of Rajasthan. The officer has completed her post graduate diploma in Cyber Security from IISc Bengaluru. The officer has served in an Infantry Division Signal Regiment.



Captain Pooja Sharma

MOVING TO 6G

THE NEXT TECH RACE

The demand for wireless connectivity and Quality of Service (QoS) has grown exponentially over the last few decades. A new paradigm of wireless communication, the sixth-generation (6G) system, is expected to be implemented between 2027 and 2030 with the full support of Artificial Intelligence (AI).

Emerging technologies such as AI, terahertz communications, three-dimensional networking, quantum communications, unmanned aerial vehicles, cell-free communications, integration of wireless information and energy transfer, and big data analytics will assist the 6G architecture development in guaranteeing the QoS. 6G would prove to be a key enabler for any hyper connected military force having a multitude of sensors, robots and autonomous vehicles with sophisticated AI. It will enable real-time analytics, provide commanders solutions or courses of action based on the influx of data and cut latency.

Emerging Communications Landscape

Over the last three decades, mobile communication networks have undergone significant revolutionary development. The 5G mobile network is already implemented in most parts of the world. Approximately 65 % of the world's population is expected to access the 5G network by the end of 2025¹. The continuous progress of the 5G mobile communication system is constantly revealing significant restrictions to this network. Its original principle was to empower the Internet of Everything (IoE). However, due to limited capacity, the 5G system is unable to achieve a fully intelligent and automated network that enables IoE as a service². Several emerging applications and sectors have rapidly grown to include virtual augmented reality (VAR),



(Image Credit Who is Danny/Adobe Stock)

three-dimensional (3D) media, AI, machine-to-machine (M2M) and Brain to Machine (B2M) communications, enhanced mobile broadband (eMBB), etc. These developments require Tbps-data rate and ultra-low latency, which cannot be met even with the new frequency bands of the 5G system. The increase in industrial automation and the transition from Industry 4.0 to Industry X.0 will further increase massive connectivity far beyond the specifications

¹ I. Shayea, M. Ergen, M.H. Azmi, S.A. Çolak, R. Nordin, Y.I. Daradkeh Key Challenges, Drivers and Solutions for Mobility Management in 5G Networks: A Survey, IEEE (2020), pp. 172534-172552

² S.J. Nawaz, S.K. Sharma, S. Wyne, M.N. Patwary, M. Asaduzzaman Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future IEEE (2019), pp. 46317-46350

that 5G was originally planned for. Increased connection density will further raise the demand for enhanced energy efficiency, which is not possible in 5G.

Global mobile data traffic is expected to increase by 55 % per year between 2020 and 2030³. The anticipated traffic growth will generate 5,016 exabytes (EBs) of monthly data by 2030. The rapid development of data-centric and automated systems may eventually overtake the capacity of 5G and existing mobile networks. 5G will reach its limit by 2030, prompting the development of new paradigms to overcome the challenges in previous mobile network generations. The 6G infrastructure will be extremely complicated due to massive connectivity. As far as military applications are concerned - gathering intelligence, visualizing combat operations, and delivering precise logistical support have been identified to be fit areas for 6G intervention. The US and China have commenced exploring the potential of 6G technology and its vastly superior bandwidth, extremely low latency, and high connectivity properties and expect that the future of combat will be autonomous (based on Internet of Military Things,

IoMT) and reliant on data driven AI for modernised militaries.

6G Technologies: Features and Promises

To meet the 6G targets, overcome the limitations of 5G and support new challenges, mobile communication systems in 5G and beyond must be enhanced with new and sophisticated features. The features of 6G mobile technology go beyond the intelligence, reliability, scalability, and security of ground mobile networks. They will empower satellite and undersea communication integration to form a ubiquitous mobile network, in line with the need to have a truly global wireless network presence⁴. The 6G mobile network is expected to attain high practical standards that meet the performance requirements of IoE, VAR, 3D applications, AI, M2M and B2M communications, eMBB and their supplementary technological directions. It is expected that the 6G network will

provide a 100x increment in energy and volumetric spectral efficiency compared to the 5G network. The 6G network will enhance the 5G system lag by introducing a novel set of technologies that include: a THz-band operating system, ubiquitous AI, massive network automation, intelligent network environments, ambient backscatter communication, internet of space things (IoST), Massive Multiple Input Multiple Output (MIMO) cellular networks, and human-to-human (H2H) and Brain-to-Machine (B2M) communication⁵. Three upcoming features are also expected to change future mobile networks, but they will not be mature enough for 6G. These features are quantum communications, the internet of nano things (IoNT), and the internet of bio-nano things (IoBNT)⁶.

The 6G target is to provide global coverage. AI applications will distinguish 6G from previous generations. Although it is still in its

³ F. Tariq, M.R. Khandaker, K.-K. Wong, M.A. Imran, M. Bennis, M. Debbah *A speculative study on 6G* IEEE Wireless Communications, IEEE(2020), pp. 118-125

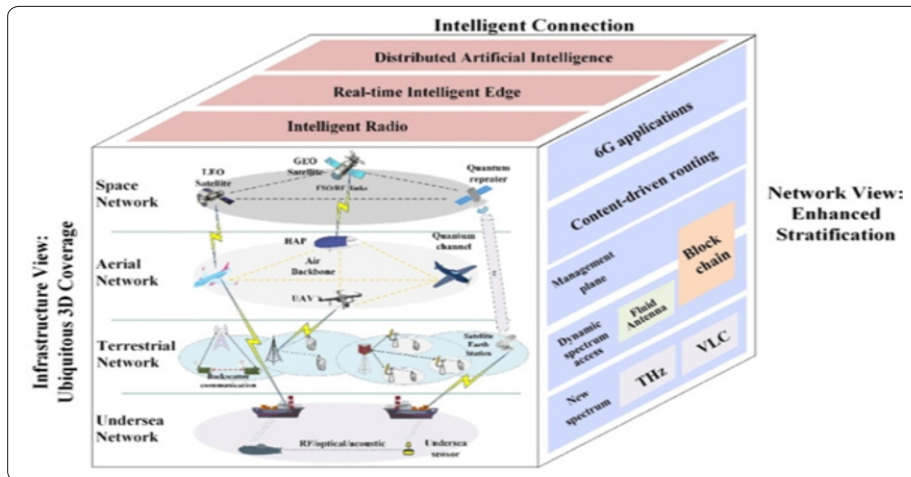
⁴ I.F. Akyildiz, A. Kak, S. Nie *6G and beyond: the future of wireless communications systems* IEEE Access, 8 (2020), pp. 133995-134030

⁵ I.F. Akyildiz, A. Kak *The Internet of Space Things/CubeSats: a ubiquitous cyber-physical system for the connected world* Computer Network, 150 (2019), pp. 134-149

⁶ E.C. Strinati, S. Barbarossa, J.L. Gonzalez-Jimenez, D. Ktenas, N. Cassiau, L. Maret, et al. *6G: The next frontier: From holographic messaging to artificial intelligence using subterabertz and visible light communication*, IEEE Veh. Technol. Mag., 14 (2019), pp. 42-50 Google Scholar



Department of Telecom forms Innovation Group for 6G Technology (image credit toppersnotes.co)



Global coverage and use case scenario of 6G (Source: 5G 6G O-RAN on Linked-in)

early stages, the autonomous 6G network is expected to serve as the backbone of 6G technology. High transmission rates are indicated by the THz frequency. Because of 6G, latency will be in the range of 10–100 μ s, connectivity density will be in the range of 10 million devices/square km and traffic capacity will be in the range of 1 Gb/s/square metre. Spectrum efficiency and energy efficiency will exponentially increase compared to 5G. 6G promises an unlimited wireless connection. It will be a communication network that will host numerous systems such as communication, metering, storage, computing, control, Global Positioning System (GPS), radar, imaging, and navigation.

The Playground for 6G Technologies

To understand the importance of 6G technology, it is relevant to examine where 6G will be used. In addition to phones, it is estimated that the density of mobile communication devices will increase. Higher quality devices, such as wearable devices, integrated headsets, and implantable sensors require more

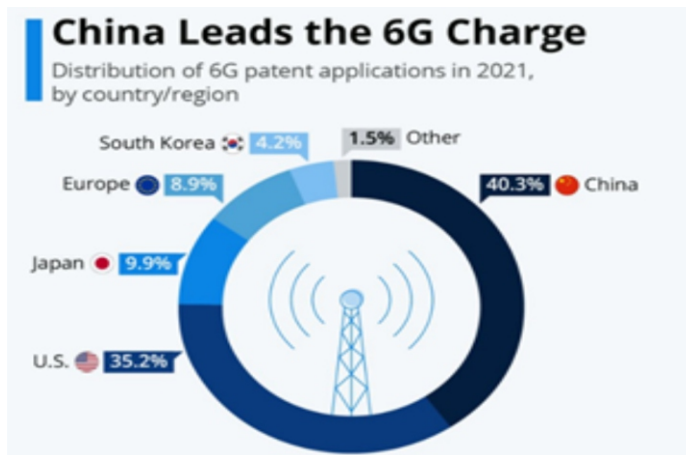
advanced environmental conditions, and these conditions are only available in 6G. 6G technology will be effective in undeveloped rural areas as well as in busy and developed cities. This large-scale communication network will be enabled by terrestrial, airborne, and satellite communications. 6G technology must participate in Industry 4.0. Building and factory automation, production, e-health, transportation, agriculture, surveillance, and smart networks all require 6G for enhanced reliability, latency, and broad bandwidth. Another contribution of the 6G generation will be the transfer of the five senses (taste, smell, touch, vision, and hearing) to users. This transfer will

include a neurological process that will be made possible thanks to wireless brain-computer interactions. The system, known as the brain-computer interface (BCI), will be used to establish a connection between the brain and other devices connected to this system. AI, virtual reality, 3D media, and IoE-based systems are based on 6G. 6G will be much more secure than current generations. The defence industry will also benefit from 6G technology since high data rates in wireless connections are required for UAVs. Submarines are also included in the concept of global coverage. This is crucial since most of the world is covered by water.

Geopolitics of 6G: The Next Tech Race

Washington has already started to sketch out the 6G battle lines. US telecommunications standards developer known as ATIS (Alliance for Telecommunications Industry Solutions) launched the Next G Alliance (NGA) in October 2020 to “advance North American leadership in 6G.” The alliance’s members include technology giants like Apple Inc, AT&T Inc, Qualcomm Inc, Google and Samsung Electronics Co. The alliance reflects the way the world has been fractured into opposing camps as a result of 5G rivalry. The US has demonstrated that it has the ability to seriously handicap Chinese companies, as in the case of ZTE, which almost collapsed after the Commerce Department banned it for three months in 2018 from buying American technology. Japan, Australia, Sweden and the UK which are part of NGA have shut out Huawei from their 5G networks which hampers Huawei’s 6G ambitions. But, Huawei is welcomed in Russia, the Philippines, Thailand, and other countries in Africa and the Middle East.

In December 2020, the European Union also unveiled a 6G wireless



China Leads the 6G Charge (Source: Cyber Creative Institute, Nikkei Asia)

project led by Nokia, which includes companies like Ericsson AB and Telefonica SA, as well as universities. Notwithstanding the above developments, as of Aug 2021 the state of patent applications filed are given in Figure 2 above.

The Ministry of Communications in India has evolved a Bharat 6G Vision Document in March 2023 highlighting how India can realize its mission of becoming a global leader in this field. The Technology Innovations Group has set up six task forces to explore the major pillars of the 6G Vision. These task forces will look into their respective areas covering Multi-platform Next Generation Networks, 6G Spectrum, 6G Devices, International Standard Contribution and R&D Finance. The Bharat 6G mission is divided into two phases: Phase 1 (2023-25) and Phase 2 (2025-2030). In Phase 1, support will be provided to explorative ideas, risky pathways, and proof-of-concept tests. Further, ideas and concepts that show promise and potential for acceptance by the global peer community will be adequately supported to develop them to completion, establish their use cases and benefits,

the processing power of the human brain. Many applications of THz wireless will enable novel cognition, sensing, imaging, communications, and positioning capabilities that will be used by automated machinery, autonomous cars, and new human interfaces, all enabled by the ultra-wide bandwidth and ultra-short wavelength at THz which appears to be a promising

and create implementation IPs and testbeds leading to commercialization as part of Phase 2.

Way Ahead

The 6G in THz frequency spectrum range will support a large number of promising applications as computing power concurrently grows to approach

spectrum for future wireless communications. Simultaneous imaging and sensing with location capabilities may be enabled by the move to above 100 GHz. THz positioning will support centimetre level accuracy and may also support imaging, even in non-line of sight (NLOS) environments. Challenges such as power-efficient devices, cost-effective integrated circuit solutions, and practical phased arrays that may be interconnected with minimal loss loom as impediments to 6G and THz product development, and offer open research and development problems that are being investigated by DARPA and other global research agencies. Today, the most important limitation that must be addressed is the economic factor. A global technological revolution such as 6G can be defined as a high-scale, costly business. 6G technology can be cost efficient if integrated with the 5G infrastructure. Making neutral hosting and location-based spectrum licensing would possibly reduce the total cost by 50%.



Colonel (Dr) Dinesh Kumar (Retd) is an alumnus of Defence Services Staff College, Wellington and holds a PhD in Information Technology (Cyber Security). With more than three decades of experience in the Corps of Signals including tenures as a Senior Faculty in Military College of Telecommunications Engineering, Mhow. He is a Subject Matter Expert in Emerging Military Technologies and Cyber Security at military institutions and a Professor of Practice at IPS Academy, Indore. He is a member of Mhow Analysis and Research Society, a Central India based think tank.



Col (Dr) Dinesh Kumar

EVOLVING WEAPONS AND SYSTEMS

Transient Nature of Disruptive Technologies

The ongoing Russia – Ukraine and Israel – Hamas conflicts have propelled new tactics, weapon systems and counter-measures onto the battlefield. Innovations too have been made as the Russians erected a netted canopy over the tanks to defeat drones and other top attack loitering munitions. In this report, we throw light on some of the emerging weapons and systems.

The Israeli Defence Forces (IDF) and the Israeli military industrial complex has been at the forefront of innovation and a constant technological evolution, leading to some of the most advanced systems in the world. The Iron Dome Counter Rocket Artillery and Mortar (C-RAM), the Trophy Active Protection System (APS), the Drone Dome Counter Unmanned Aerial Vehicle (C-UAV) systems and the B-Net Software Defined Radio (SDR) are some such examples, which have significantly impacted the battlefield.

The Iron Dome, for example, very successfully addressed the threat of rockets, providing not only security, but also political flexibility to the Government of Israel. Had the rocket strikes been effective, they would have been compelled to retaliate, as all governments need to pander to public perception. The Trophy APS afforded advanced protection to Israeli Armour during ground offensives. Similarly, the Drone Dome C-UAV system now addresses an emerging and potent threat.



Iron Dome Air Defence System in action in Israel, a US Made Tamir missile being fired

But there is no perfect system, and this is why I prefer the term ‘evolving technologies’ to ‘disruptive technologies’. I intend elucidating on these systems.

Iron Dome C-RAM System

The Iron Dome detects, assesses and intercepts aerial threats. The system radar first detects a threat, and then carries out an assessment of whether the threat will be effective, in terms of where it is expected to land. This is done by estimating the trajectory of the airborne threat. It then intercepts only those threats that are assessed to be effective.

The system is designed to achieve a hit probability of more than 90%. The design may itself have been capable of achieving a higher hit probability, but was curtailed to 90%, so as to optimize cost and effect. It is an all-weather system, capable of simultaneously handling multiple targets. The interception itself is carried out by a missile with a proximity

fuse, thus detonating the target warhead in the air.

Israel follows a multi layered approach to Air Defence, catering for short, medium and long range aerial threats. The systems are highly networked and optimized, facilitating command and control and optimization of resources. Therefore, all systems, including the Iron Dome, can function as a stand-alone system or as part of a multi-layered Air Defence System.

Since its introduction in 2011, the Iron Dome has been highly successful, with thousands of successful intercepts. So much so, that rocket attacks, for some time now, have just been a show of fireworks in the sky.

The technology was indeed disruptive. The impact was not just tactical, it was strategic. **So why was it that Hamas terrorists still manage to strike?** The answer lies in the fact that Hamas could manage to find a counter – in this case, tactical rather than technological. Over a period of time, Hamas kept amassing rockets, to be unleashed at a future date. Ironically, this happened without the knowledge of IDF, or other agencies across the world

The solution that Hamas found was to increase the number of rockets to such a degree that the Iron Dome simply got overwhelmed. **Never before had so many rockets been fired near simultaneously.** The deployment of the Iron Dome in terms of the number of systems and missiles was based on the threat assessment. The system did not envisage thousands of rockets being fired within a short span of time.

While the system has proven to be highly effective, there lies a difference between effectiveness and efficiency. It must be kept in mind that a smart missile is used to intercept a 'dumb' threat. The cost

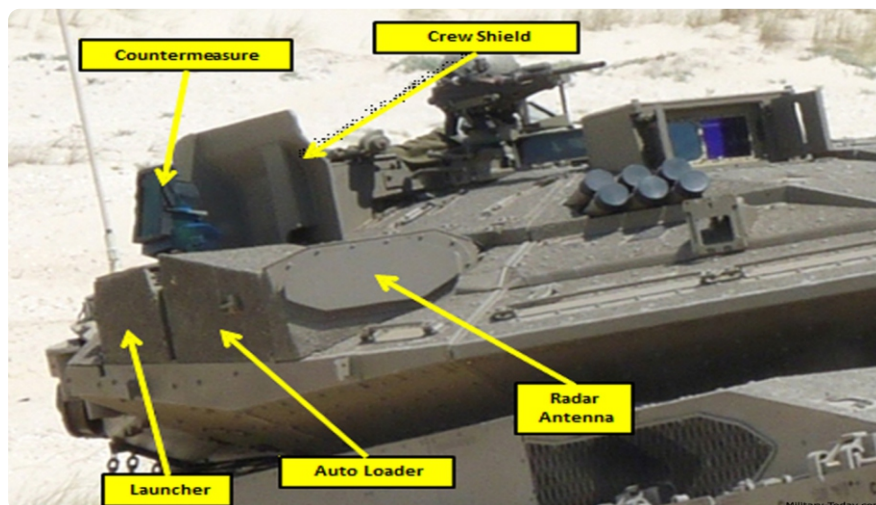
difference between these two is exponential. By some estimates, a single missile costs more than 100 times the price of a rocket. As the number of rockets increase, the number of interceptors also goes up correspondingly. It is also for this reason that India, though impressed with the system, did not seriously consider procurement. The effectiveness was impressive, but the efficiency was questionable, especially in the context of India, where such a threat was not assessed, and where the area to be protected is also very vast. Of course, when it comes to defence of the land, and the saving of lives, as in the case of Israel, cost may be an insignificant contributor to decision making.

There is no doubt that the IDF would have learnt their lesson, and we will in the near future see further development of the system. **Perhaps directed energy could be one solution. From disruption to evolution.**

Trophy APS

The Trophy is the only combat proven system in the world today. The system was developed to overcome an operational challenge of the threat that Armoured Fighting Vehicles (AFVs) faced during land manoeuvres, especially in and around built-up areas. Trophy provides a hemispherical protection around the vehicle. It is indeed highly complex technology, in that an incoming threat is detected, then assessed to be actually homing towards the vehicle, and finally intercepting and neutralizing this threat.

The detection is carried out primarily by radar, and system algorithms then assess whether the threat is indeed likely to be hitting the vehicle. If not, it is ignored. If the threat is indeed likely to hit, then it is intercepted at some distance away from the vehicle, by means of firing a countermeasure. The entire cycle is carried out automatically, without crew intervention.



Trophy Active Protection System on a battle tank (Photo courtesy military-today.com)

The interception itself is designed so as to minimize collateral damage, allowing dismounted troops to operate in the vicinity, subject to a safety zone. The system is platform-agnostic, and can be integrated to any platform, and can simultaneously handle multiple threats. In fact, if one looks at a combination of APS, Remote Controlled Weapon Station (RCWS), 5th Generation ATGM and advanced electro-optics, both the lethality and survivability of any platform can increase exponentially.

Trophy counters only Chemical Energy (CE) threats. The system was designed for this purpose, as the defined operational requirement was against CE threats only. CE threats would include High Explosive Anti-Tank (HEAT) rounds like Anti-Tank Guided Missiles and Rocket Propelled Grenades (RPGs).

Why was Trophy a disruptor?

Look from the point of view of a tank commander heading into hostile territory, especially into towns or cities. The threat here is not as much enemy tanks, but more from shoulder fired RPGs, that are readily available. The buildings enable the firer to shoot and scoot. Now imagine the tank moving into Gaza City with the confidence that these threats would be taken care of by the APS, then one will understand why the system has been instrumental in saving so many lives.

The system was developed resulting from a stated operational necessity of armour operating in and around built-up areas. Tank to tank battles, however would involve Kinetic Energy (KE) projectiles, which the system so far does not address. In India, the operational requirement for Trophy includes protection against KE projectiles, as tank to tank battles are expected to be more predominant than operations in built-up areas. The necessity of an APS, however, on all future

armoured platforms, is indisputable, and the Indian Army is actively pursuing APS programmes.

Drone Dome C-UAV System

If one has to single out a single technology that is actively shaping the battlefield today, it would undoubtedly be unmanned aerial vehicles (UAVs). Recent conflicts across the world have proven the threat from UAVs on the battlefield. UAVs are not just a battlefield reality today, they are also potent terror threats. Most air defence systems are not fully capable of engaging these threats, due to the small Radar Cross Section (RCS) and the accuracy required for engagement.

The challenge for an effective counter UAV system is the accuracy and specificity required. The system is required to not only detect and neutralize UAVs, but very often achieve this in an environment that does not interfere with non-hostile aerial systems. Take an airport, for instance, where there is substantial aerial traffic. The system needs to detect the threat amidst all the traffic, assess and classify the threat, and finally engage it. All this while causing nil or minimal interference to other friendly aircraft.

The first step in a counter UAV system is detection, which can be done by one or a combination of three means. This includes radar, electro optic sensors and homing on radio frequencies within the entire applicable frequency spectrum. The most reliable of these is the radar, provided it has the ability to pick up a target with very low RCS and velocity. The system then needs to identify and track the target. Finally, the target needs to be neutralized, which could be either by soft kill or hard kill, or both.

Soft kill involves rendering the target inoperative, in that it can no longer navigate and propel itself to a pre designated point, and cannot be guided to do so by the control. Typically, this would involve jamming the signals to and from the target, including GPS frequencies. Once again, the challenge is to be specific in this jamming, such that friendly systems in the area are not affected. There could even be means of acquiring control of the system through hacking.

Hard kill would involve the physical destruction of the target. Although technically possible, it is difficult to do so by means of firing. The more reliable option is to use directed energy. In the case of the Drone Dome C-UAV, this is done by means of laser.

Most nations are alert to the threat of UAVs, and are in the process of developing / procuring and deploying C-UAV systems. India itself is well alert to the operational necessity, and all three services are actively pursuing C-UAV programmes.

B-Net SDR

Wikipedia defines SDR as *'a radio communication system where components that conventionally have been implemented in analog hardware (e.g.*

mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software on a personal computer or embedded system. While the concept of SDR is not new, the rapidly evolving capabilities of digital electronics render practical many processes which were once only theoretically possible.'

A typical SDR will consist of an RF Card, an analog to digital converter, and a processor. The processor carries out all functions that were earlier done by electronic circuits. Each SDR is programmed to transmit and receive communication protocols, referred to as waveforms. To this, layers of encryption can be added.

Since waveforms are typical to the SDR, there are sometimes concerns over interoperability, in that one family of SDRs may not necessarily communicate with another, unless protocols are exchanged. Since waveforms are proprietary, this is a challenge, and this is an aspect that has to be kept in mind during induction of SDRs.

The SDR has revolutionized military communication just as cellular phones have revolutionized communication in general. Radios are no longer just a means for voice communication, they can now transmit and receive data that has redefined the scope of situational awareness. Apart from just point to point communication and multi point communication, SDR can also be embedded in systems allowing for much higher command and control.

Most SDR are capable of establishing Mobile Ad-Hoc Network (MANET) implying that typical line of sight communication is a thing of the past. Apart from unprecedented network capacity, the SDR also provides for Electronic Counter Counter Measures (ECCM). The B-Net SDR also has Multi Channel Reception (MCR) technology that enables exponentially enhanced network

capacity in terms of data rates, number of users, and minimal delay. In India, the SDR has already been inducted partially, and more programmes are being pursued in this field.

Transience of Disruptive Technologies

One major lesson learnt from the ongoing conflict in Gaza is the impermanence of disruptive technologies. **The disruption is only temporary. It is only a matter of time when a counter will emerge.** More often than not, these counters will be technological, a tandem warhead to beat Explosive Reactive Armour (ERA) being one such example. But ever so often, the counter is in the form of evolving tactics. Notably, India has been a master at these kinds of 'improvisations'. The modifications to Precision Guided Munitions during the Kargil conflict to enable engagement in high altitude, the modified range tables and fuses used in rarefied high altitude firing are some examples. We have been forced to 'do more with less' so often, that improvisation is almost second nature to us. It is even encouraged at all levels, to find solutions to mostly minor operational or logistics problems.

Evolving Technologies and a Defence Industrial Base

Military technologies are ever-evolving, and most nations devote significant time and resources towards this end. The effort for research and development is continual. For each technology that turns out to be disruptive, there will be a counter at some point of time.

In the Indian context, specifically of 'Aatmanirbhar Bharat', there has been a recent shift towards indigenisation. Most

programmes today stipulate not just substantial indigenous content, but also Indian design. But self-reliance, especially in defence manufacturing, cannot be achieved in a day, or even in the short or medium term. There has to be a phased approach, starting from manufacturing in India, and culminating in Indian design.

For now, it does not appear that Indian industry is capable of developing technologies that can be considered disruptive. We are just emerging from the Public Sector monopoly, and it will take some time before Indian industry reaches that kind of capability. There is always the option of acquiring designs, but most foreign Original Equipment Manufacturers will be loathe to transfer design rights. They would, however, be willing to transfer technology for licenced manufacture. That should be a viable start point. Simply manufacturing. **Once they start manufacturing, the design will come. Just give it time.**



Col Manish Sarin

Colonel Manish Sarin (Retd) was commissioned into 2/8 Gorkha Rifles in 1991. He commanded the same unit, 'Sikand Aite', and then took premature retirement in 2012. After retirement, he has worked with Rafael Advanced Defence Systems, Israel as Senior Director, Land Systems. He is now an independent advisor on defence procurement issues.

NAVY'S INNOVATION IMPETUS: CONVERTING SPRINT TO A MARATHON

Indigenization in the defence industry requires tremendous 'cutting of corners', hand holding and close interaction between the users and the developers. Rate of infusion of new technology also has to be accelerated, and innovations have to be nurtured on a suitable platform.

SPRINT is one such initiative from the Navy which succeeded in launching 75 viable innovations in the first year. This article critically examines the SPRINT initiative with an aim to recommend long term policy and organisational changes that will help sustain the thrust over a long term.

During its annual seminar 'Swavlamban' in October 2023, the Naval Innovation and Indigenisation Organisation (NIIO) showcased products developed under the acronym 'SPRINT' (Supporting Pole-Vaulting in R&D through iDEX, NIIO & TDAC) initiative. SPRINT, by all accounts, has been an unparalleled success with some observers in the print and social media describing it as "magical". One commentator even suggested that the success of SPRINT can make an interesting case study for any business school!

Innovation, however, is an ongoing and never-ending process. It is not something that can be done once and then forgotten. To use a seaman's term, a Navy cannot rest on its 'innovation' oars. It is important that the small beginning made be converted into a long term, institutionalised mechanism that can repeatedly replicate the results.

To provide unprecedented thrust to *Atmanirbhar* Bharat during the 75th year of Independence, and provide 'acceleration' in induction of disruptive defence technology as a part of the *Amrit Mahotsav*, the NIIO proposed in 2022 that the time to 'leapfrog' to keep pace with the fast-changing technology is over. The need now is to 'pole-vault' to greater heights.



Autonomous weaponised boat swarm developed by Sagar Defence (photo credit X @NewsLADN)



Autonomous Armed Swarm Boats Under The SPRINT Scheme (photo credit currentaffairs.adda247.com)

To achieve this, a collaborative project aptly named 'SPRINT' was started with problem statements for the industry being unveiled by the Hon'ble Prime Minister during the inaugural NIIO Seminar 'Swavlamban' in July 2022. An MoU was signed between the NIIO and the Defence Innovation Organisation (DIO) – a Section 8 'Not for Profit Company' of the Ministry of Defence (MoD) - which steers the iDEX initiative. The iDEX, NIIO and TDAC (Technology Development Acceleration Cell) – the innovation arm of NIIO collaborated on '*pole-vaulting*' R&D support for disruptive technology. Aimed at developing at least 75 Indian products for the Indian Navy before 15 August 2023, the acronym **SPRINT** was selected for the initiative. To enable funding support for start-ups, MSMEs, universities and even individual innovators, the existing procedures of iDEX were to be used. NIIO was to frame the problem statements and handhold the selected firms so as to meet the goal.

The reasons for the success of NIIO and SPRINT include a top-down thrust; a very high level of delegation of decision making; trusting the Indian start-ups and seeing them as '*partners*' not '*vendors*,' and, close coordination between DIO and NIIO. One factor which has not been discussed sufficiently but which had an important role to play was the very structure of NIIO.

With the setting up of NIIO in 2020, the Indian Navy had signalled its intention of moving beyond mere import substitution in the field of defence manufacturing. The Navy, which has always championed '*indigenisation*' with impressive results, was specifically focusing on '*innovation*'. A dedicated, small and nimble organisation named the TDAC was also simultaneously set-up to focus on this aspect.

Innovation demands a different mind-set. For innovation, '*out-of-the-box*' thinking is required. This may need challenging the status quo and an examination of the rules to see where they need to be amended instead of just following them. Innovation, by its very nature, is risky, while our procedures largely tend to be risk averse. **The first lesson that must be learnt for innovation is of risk taking.** The officers posted to TDAC therefore had to be carefully chosen based on a demonstrated innovative mind-set rather than on any other criteria. The fact that the organisation was set up with a '*willingness to fail*' is possibly the biggest factor behind the success that has been achieved till now. This was facilitated by a number of factors including an unconventional organisational structure which depended not only on officers posted to it, but also on a number of '*volunteers*' who were collaborating online. Out-of-the-box thinkers in the Navy were identified and permitted to directly communicate with Naval Headquarters on matters concerning innovation. This thirty-plus strong team of young officers helped create a flat hierarchy-less entity more akin to a start-up than a conventional military organisation.

Successful innovation in the defence sector is as much about technology as it is about processes and policies. Whilst the same may be true in any field, in the field of defence especially even for successful development of technology, the aspects of induction and integration of the innovative solutions are as important as the technical innovation per se. Therefore, having officers from diverse backgrounds and from different branches in TDAC was a good decision.

Another step that, in hindsight, worked well was the formal MoU between NIIO and DIO for SPRINT. At the time of launching SPRINT, the need for an MoU between the NIIO and DIO was debated. One view was that since the two organisations are supposed to work together as it is, there should be no need for a separate MoU. The counter logic was that the MoU simply reiterates the existing procedures, delineates responsibilities and lays down timelines. The MoU was also largely worded with generic '*motherhood and apple-pie*' statements that no one could object to. The firm details were to be worked out at the working level between identified Points of Contact (POCs) at NIIO and DIO. The fact that an MoU had been signed provided a clear roadmap on what needed to be done and, more importantly, committed everyone to timelines. An ambitious project such as this would probably not have been feasible without focused attention at all levels.

There were discussions in the months preceding SPRINT on the need to bring in the aspects of procurement into the framework. It is of little use developing technology and then trying to find means of quickly inducting it. The traditional procurement timelines are not really suited for start-ups - which need immediate financial support in terms of orders once the product has been suitably trial evaluated. The timelines need to be in weeks and months and not in years.

The April 2022 amendments to Chapter III of the Defence Acquisition Procedures (DAP) were used to good advantage by the SPRINT initiative. Through these amendments, the section on innovation has been virtually written anew with all old clauses being removed and substituted with more user-oriented ones. These were applicable to iDEX cases and similar leeway has subsequently been extended to TDF (Technology Development Fund) cases as well.



Hon'ble Prime Minister launched the 75 challenges for the start-ups/ MSMEs as a part of the 'SPRINT' initiative, in July 22 under the Swavlamban programme (photo courtesy www.pib.gov.in)

A unique feature of SPRINT – over and above the iDEX procedures -- was the willingness of the Navy to indicate the Minimum Order Quantity (or MOQ) upfront at the time the challenge was launched. This proved to be a game changer. Industry is quite willing to invest in R&D provided they have a good degree of assurance of orders. Our procurement procedures did not explicitly permit this MoQ being specified, but they did not explicitly prohibit it either! The amended DAP included a clause that no quantity vetting or justification of scaling is necessary for initial procurement up to delegated financial powers. Therefore, as long as the MoQ was within the delegated powers, no rules were being broken. The Navy committed that under SPRINT, the initial procurement shall be undertaken, subject to successful trials, as specified at the time of launching the challenges. This enabled small firms and start-ups to raise capital from non-governmental sources and Venture Capitalists (VCs) as well. This

very specific 'requirements' for a product that does not, as yet, exist. Solving a problem as expressed by the users can be much better undertaken in consultation with the developers and the final product may actually turn out to be very different from the one initially envisaged. Flexibility is important. The provision for automatic conversion of the demonstrated capability of the product that clears the single stage composite trials into QRs is a bold new addition to the DAP that will show results in the years to come.

The selection of the problem statements was crucial. The emphasis was on 'sensors' and Artificial Intelligence based applications. Radars, sonars, blue green lasers for underwater applications (both detection and communication), space communication and Electronic Warfare systems are some of the fields which were included. There were many challenges for firefighting as well. Autonomous and remotely manned systems of various kinds (airborne, surface and sub-surface) for different purposes were also envisaged and successfully developed. Autonomous, weaponised boat swarms and heavy lift UAVs are just two applications. These would have been considered beyond the capability of start-ups by many. The fact that a large number of start-ups responded to the challenges, and, also that products are already being inducted after successful trials is testimony to the fact that Indian defence industry is changing.

The stated aim of developing at least 75 products was not only met but surpassed. Quite a few 'global firsts' were also developed under the initiative and many more are in the pipeline. Acceptance of Necessity

initial procurement – though of limited quantity – has two advantages. From the user perspective it permits comprehensively experimenting with the products before larger orders are placed. From the industry perspective it ensures that genuine effort is rewarded. The appetite for risk in the private sector and VCs will always be higher than in any government entity. By giving assurance of orders, the Navy signalled its intention of supporting start-ups not only in development but for induction as well.

Developing 'high-risk, high-return' category of disruptive innovation requires a shift away from a 'Qualitative Requirement' (QR) based approach to a 'Problem Definition Statement' (PDS) based problem-solving approach. It is difficult, if not impossible, to envisage

(AoN) for 12 products worth nearly Rs 1500 crore has already been accorded. A few products have already been inducted. What should be done to ensure that the momentum is further built upon and that the gains made are consolidated?

Firstly, the difficult decision about the way ahead for the organisational structures would need to be taken. It is true that the success of NIIO in innovation is to a very large extent due to its unique organisational structure. This structure allows for greater flexibility and adaptability, and has enabled the Navy to quickly adopt new technologies. The 'willingness to fail' embedded in the organisation certainly helped encourage risk-taking and experimentation, which is critical for innovation. However, in the long term such an organisation can become a victim of its own success. This should not be allowed to happen. The expectations from the NIIO will be higher in the years to come and the leeway provided to the organization hitherto has to be maintained. A fine balance will need to be worked out between institutionalising what has worked and permitting 'mavericks' to think and act differently.

Secondly, close monitoring would need to be ensured as the technology demonstrated moves from the 'innovation' to the 'production' stage. Demonstrating a capability through a prototype is very different from meeting large orders and providing adequate lifecycle support. Once again, the skill sets required may be very different. As the SPRINT winners go on to expand their capabilities, they too would need to look at conformists in addition to mavericks. The production capacity would need to be ramped up (or in some cases set up anew) and additional manpower hired for providing support at multiple locations. This would also need infusion of capital.

Lastly, mere placing of orders (even up to the MoQ) by the Navy may not suffice if a change in the ecosystem is to be brought about. The orders by the Navy for the successful products will certainly be placed, but these products must also be promoted for use by other Services and agencies as may be applicable. Quite a few of the products are 'dual-use' and can have numerous civil applications as well. Agencies such as the police, fire services, railways, Defence Public Sector Undertakings and disaster relief forces (both at the state and central levels) can straight away benefit from some of the products, as can the merchant marine. The export market needs to be tapped as well. Of course, the quality of the products will speak for themselves, but a concerted campaign to spread awareness may be useful. The novelty of the innovations implies that many users may not be able to visualise the utility till the capability is

practically demonstrated. Most of the start-ups involved are small firms which may not have the reach or the wherewithal to fully realise their potential. Inter-ministerial coordination and a 'whole of government' approach may help. If the innovation blitzkrieg is to be replicated, it is imperative that the products developed and their potential utility be suitably highlighted at every available forum.

In the final analysis SPRINT, with its emphasis on collaboration, innovation, and industry engagement, represented a transformative initiative in India's quest for self-reliance in defence technology. The hand-holding required by these start-ups does not end here. This is just the beginning. The success of SPRINT must be replicated, be built upon and be surpassed through even more innovative initiatives. **The SPRINT must become a marathon.**



Commander Ishant Panwar, an alumnus of the Indian Naval Academy, Ezhimala, was commissioned in the Indian Navy on 04 July 11. The officer specialises in Naval Armament Inspection and has done B.Tech in Elec. and Comm. Engg. and has a M.Sc. Degree in Military Technology from Military Institute of Technology, Pune. The officer has served in various Naval establishments like Contollerate of Naval Armament Inspection, Visakhapatnam and Directorate of Naval Armament Inspection at Naval Headquarters, New Delhi. He also worked with DRDO in strategic projects/ missile systems at Hyderabad. The officer is currently posted at TDAC under the newly created NIIO.



**Commander
Ishant Panwar**

NORTH TECH SYMPOSIUM

When any weapon or equipment passes muster with the Indian Army, it generally indicates to other countries that the equipment is a 'good buy'. This perception is primarily because the Indian Army tests the equipment in diverse and extremely challenging terrain and weather conditions. And, the Indian Army invariably tests the equipment in the high altitude, rugged Himalayan Mountains of the Northern Command. The Northern Theatre is not just a test bed, but is a live battleground. Equipment induction into the Northern Theatre is therefore a vital necessity.

In the recent past, imaginative and offensive exploitation of technology has challenged the status quo in the battle field. In the coming years, the existing and emerging technologies will fundamentally change future border management, operations and national security. To match the operational requirements with advances in weaponry and new technologies, it was **imperative to bring the users, the developers, the manufacturers and the researchers together onto a single platform – close to the actual operational area.**

The annual North Tech Symposium organized under the aegis of Headquarters Northern Command provides such a platform where the requirements of modern equipment for the Northern Command in particular and the Indian Army in general are synergised with the capabilities and product



Lt Gen Upendra Dwivedi, Northern Army Commander witnessing the equipment on display at the Symposium



Lt Gen MV Suchindra Kumar, the Vice Chief of Army Staff discussing equipment aspects with a vendor representative

availabilities from the industry and the academia.

So, What Transpires in this Symposium?

Various Army Officers engage with **Academia and Industry** persons to identify unique/ customized solutions to meet the operational requirements of the Northern Army. **The Original Equipment Manufacturers/Vendors** showcase their existing products and discuss possible new product designs and their launch. The Symposium also promotes inclusive **Aatmanirbharta in Defence Production and Technology** Proliferation by encouraging start-ups and Micro, Small and Medium Enterprises (MSMEs). Thus, the platform creates an effective eco-system for **knowledge diffusion** on contemporary Defence technologies and enhances the **technological knowledge threshold** of the participants through joint Army - Industry – Academia participation.

Indigenisation

Under the '**Aatmanirbhar Bharat**' campaign, the Defence sector has been identified as one of the key focus areas for indigenous production. Defence Aatmanirbharta has received the desired thrust through policy changes in Foreign Direct Investment, Budget reforms and by introducing a positive indigenisation list. The Indian Army too has converged its focus and aligned it to the national aim of self-reliance through indigenisation.

For the first time since its inception in 2005, the North Tech Symposium was held in a civil establishment viz **IIT Jammu** from 11 to 13 September 2023. The potential and capabilities of the academia and the industry (Society of Indian Defence Manufacturers (SIDM)) were on display together at the IIT Jammu campus. IIT Jammu is one of the 23 IITs in India and

specializes in Communications and Cyber Applications, Artificial Intelligence & Machine Learning, Renewable & Sustainable Energy, Biomedical Research, Catalysis and Synthesis. This premier institution also has an MoU with Northern Command for pursuing Research & Development (R&D) projects. **SIDM** was formalized in 2017 under the umbrella of the Confederation of Indian Industries (CII), and plays a proactive role as an advocate, catalyst and facilitator for growth and capability building of the defence industry in India. **SIDM** helped by synergizing the participation of its members during the North Tech Symposium 2023. The Indian Army representatives from Delhi, and all commands pan India, the private sector, start-ups, Defence Public Sector Undertakings, R&D Organizations & Academia engaged concurrently, over the three day event. The North Tech Symposium witnessed participation by 183 industry partners comprising 30 large, 104 MSMEs and 49 start-ups.

Highlights

The Symposium was inaugurated by Lieutenant General MV Suchindra Kumar, Vice Chief of Army Staff. Many other dignitaries visited the Exhibition to include General Anil Chauhan, Chief of Defence Staff, Lieutenant General Upendra Dwivedi, Northern Army Commander, Shri Manoj Sinha, the Lieutenant Governor of Jammu & Kashmir and Brigadier BD Misra (Retd), the Lieutenant Governor of Ladakh. Shri Rajnath Singh, the Hon'ble Raksha Mantri and Dr Jitendra Singh, Minister of State graced the event on 12 September 2023. Other major activities were as under:-

- An **Exhibition** of latest products by

over 200 industry participants on various technologies with special encouragement to start-ups.

- **Product launches** typical to the requirements of the Armed Forces.
- **One on One Structured Interaction** with industry representatives and the academia to bridge the gap between requirement and capabilities.
- **Technical Seminar(s)** to invigorate fertile minds through exchange of novel ideas and concepts.
- **Ideas and Innovation Display** by students and the Army with due recognition and awards.
- **Military Equipment Display** by the Armed Forces to acquaint general public, industry and academia and to foster nationalistic fervour.

During the three days, more than 10000 persons (Army officers, NCC Cadets, students and faculty of IIT Jammu and other Universities, colleges and schools around Jammu and Udhampur) visited the exhibition.

So What has been the End Result?

The Symposium made the participants more aware of the dynamic operational challenges in the Northern Theatre, has added practical nuances in the minds of the academia and has stimulated the innovative potential of our young entrepreneurs - Start Ups. All these take-aways will energise the brains involved in our defence industry – undoubtedly our defence industrial base will improve in capability, product designs and delivery of quality weapons and equipment.

■ Lt Gen JS Sandhu (Retd) *Editor*

TIRANGA ATOP 28

HIGHEST POINTS / PEAKS

'Har Shikhar Tiranga', an audacious and patriotic expedition, aspired to hoist the Indian national flag on the highest peak or point of every state across India.

As India celebrated 'Azadi Ka Amrit Mahotsav' and G20 Presidentship, I thought about the vast differences in the terrain obtaining in each state. An idea sprouted – why not lead an expedition to the highest points or peaks in all the states. I am heading the National Institute of Mountaineering and Adventure Sports (NIMAS) at Dirang in Arunachal Pradesh, and so could conduct this expedition with mountaineers at our Institute. I discussed the proposal with the Ministry of Defence, and we decided to start with a test phase to cover the States in North East India. Thus the 'Har Shikhar Tiranga' Mission was launched - a remarkable tribute to India's unity, diversity, and mountaineering excellence.

Since we were in Arunachal Pradesh, we started by proceeding to Arunachal Pradesh's Mount Gorichen (6505 metres), which we summited on October 16, 2022. The other Northeast India's six states' highest points were also completed as part of the test phase and the feasibility of the mission was confirmed. The team was confident enough to make plans for a pan-India expedition, taking due permissions from the Ministry of Defence. My experience made a huge difference in planning and execution, resulting in a unique first in the field of mountaineering.

'Har Shikhar Tiranga' Mission then resumed its journey, after being flagged off at Dirang by Shri Pema Khandu, Arunachal Pradesh's Chief Minister, also the Vice President of NIMAS, on 25 May 2023. The team tackled Himachal Pradesh's highest mountain, Mount Reo Purgyil (6818 metres) and then moved in June 2023 to Uttarakhand. The team climbed the formidable Mount Kamet (7756 metres) and then began the journey to the plains and coastal states. We ended the mission with a very technically challenging mountain, Mount Jongsong (7462 metres) in Sikkim on October 2, 2023.



Upper Photo. The team climbing up towards Mount Jongsong in Sikkim Lower photo. The team atop one of the highest points with local volunteers who joined up at each place

The Government of India had also launched the 'Meri Maati Mera Desh' campaign as part of 'Azadi Ka Amrit Mahotsav'. The Hon'ble Prime Minister Shri Narendra Modi presided over the programme in October 2023, marking the culmination of the campaign's 'Amrit Kalash Yatra' at Kartavya Path in New Delhi. 8500 Amrit Kalash containing soil from every nook and corner of the country were brought to Delhi. This included soil collected by the 'Har Shikhar Tiranga' team from the highest points of all the 28 states.

So, what were the significant aspects of the Mission? This was the first ever such expedition in India, wherein a team climbed the highest mountain or point of all the Indian states, covering more than 30000 kms in one year. The mission's primary aim was to instil a profound sense of respect for our national identity and the significance of the 'Tiranga', our national flag, across the entire nation. The campaign's significance extended beyond adventure; it aligned with the celebrations of India's 75th year of Independence and the G20 Presidency. It resonated with Prime Minister Narendra Modi's 'Meri Maati Mera Desh' campaign, as the team actualised the vision of a unified celebration of India's soil.

The motivation of the team also came from the ground support and adulation of the public. Often it surprised the team as many people used to wait for the expedition members. More than 1000 adventure enthusiasts joined this mission from various states. This is the highest number of participants in a single mission. It was also the first time ever that the highest peaks of four Himalayan states (Arunachal Pradesh, Himachal Pradesh, Uttarakhand and Sikkim) were climbed within a span of one year and by a single expedition.

Mission 'Har Shikhar Tiranga' created a wave of nationalism across the entire

country and received an overwhelming response everywhere. The expedition also gained the support of mountaineering legends like Ms Bachendri Pal, Captain MS Kohli, Santosh Yadav, Arunima Sinha, as well as celebrities like Anupam Kher, Gaurav Chopra, Darshan Kumar, and Mohit Raina. They propagated the campaign by posting messages on their social media accounts. Support from the Ministry of Defence was extremely beneficial and it emphasised the campaign's national importance.

Any major difficulties faced? I continually faced an administrative challenge of securing of forest permissions, particularly in ecologically-sensitive areas. During these phases, my long experience and clarity of focus kept 'Har Shikhar Tiranga' going.

Nature had also set its own test for us. In a dramatic twist, the team was caught amidst the cloudburst in Sikkim, leading to a delay in our return. But the determined members survived all these difficulties and physical and mental tests with their trademark resilience and bravery. Eventually, Team NIMAS returned with the news of Mission 'Har Shikhar Tiranga', successfully accomplishing its ambitious goal.

This Mission also stood out for several reasons, one of them being settling the historical debate concerning the highest peak in Himachal Pradesh. The Tiranga team conclusively identified Mount Reo Purgyl as the highest peak. This discovery not only puts an end to a long-standing debate, but also solidifies the peak's status in the Indian mountaineering community.

The arduous expedition involved long hours of travel, wading through tough terrain, heavy rains, snow, leeches, and even sensitive Naxal areas. Mission 'Har Shikhar Tiranga' was an epic journey that symbolised India's unity, diversity, and indomitable spirit. It celebrated love for nation, adventure, and the commitment to overcome challenges, exemplifying the belief that we are stronger together.

In a nutshell, this pioneering expedition to 28 Indian states, traversed all these states in one year, with a record-breaking participation of over 1000 climbers, and scaled the highest peaks of four Himalayan states within a year.



*Colonel Ranveer Singh Jamwal, SM, VSM** is a decorated officer and a distinguished mountaineer of international repute who has been awarded with the National Adventure award, Indian Mountaineering Federation Gold Medal and various other civil and military awards. He is the only Indian to climb the highest mountain of all seven continents along with three Everest summits. He holds three Asian records and four Indian records and has done more than 75 mountaineering expeditions. He is presently the Director of National Institute of Mountaineering and Adventure Sports (NIMAS), which is the only adventure institute in the country mandated to conduct certification courses in all three verticals of adventure (Land, Aero and Aqua).*



Col Ranveer Singh Jamwal

SMARTER WAYS TO INVEST IN REAL ESTATE

Real estate investing refers to the purchase of property, land or any immovable as an investment to generate income rather than using it as a primary residence. While it can also be for long-term capital appreciation purposes, for the limited purpose of this article, we are exploring Real Estate as an Investment option to generate regular returns.



What are Real Estate Investments?

Any land, building, infrastructure, and other tangible property that is usually immovable but transferable. If real estate investments are not done wisely, then it may lead to poor returns or depreciation of the investment value.

Drawbacks of Real Estate Investing

High Cost. The biggest disadvantage of real estate is the high capital investments. To get started with real estate investment, you need to have down payment. You will have other expenses as well like Registration Fees, Property Tax, Stamp Duty etc.

Long term Investment. To see good returns, one needs to hold the property for a long term, and this might change as per the location of the property. At times, the property value may take years to appreciate. Real estate investing is essentially a part of long term strategy.



Methods of Investing in Real Estate

Legal Issues. Investing in real estate is very tedious as it involves a lot of paperwork and cumbersome legal formalities.

Liquidity constraints. A major constraint is liquidity. Readily finding buyers and sellers is very difficult. Rental income also causes problems if you don't have a good tenant.

Maintenance Cost. Maintenance cost is an important fact to look into while buying a property. This will vary as per the location. There would be higher maintenance costs in larger cities.

Property Tax. Property tax varies depending upon the jurisdiction in which the property is located. An investor should also consider the tax while valuing the property, as property tax can potentially wipe out a large chunk of the profit.

An Easier Way to Invest in Real Estate

Not everyone has cash on hand to buy a home or property for investment purpose. Financial real estate investing gives the investor an easier option to enter the real estate market. Some of the alternatives are Fractional Investing or Real Estate Investments Trust (REITs). Fractional real estate investing is worth considering.

What is Fractional Ownership?

Ownership itself dictates our sole right over any property. But Fractional Ownership, as the name suggest, is the concept of owning just a fraction of any property rather than being the exclusive owner with the rightful benefits. Over the past few years, the real estate market in India has undergone significant changes, transitioning from a disorganised and unregulated state towards a more organised and regular one. With many regulations such as RERA, GST and recently REITs, Fractional Ownership platforms for real

estate investments have gained the trust and interest of investors.

Fractional Ownership is bringing a change in the Indian real estate sector by democratizing investment opportunities and granting all the retail investors access to the high value commercial real estate. This investment model is gaining popularity because of the potential for high returns, ease of tracking and also the diversification benefits. According to a report of Knight Frank, the market size of fractional ownership in India was USD 5.4 billion in 2020 and is projected to reach USD 8.9 billion by 2025, growing CAGR by 10.50%.

How does fractional ownership work?

The multiple owners who intend to buy big ticket commercial property create a group among themselves or through a financial ownership platform – an investing strategy in which the cost of acquisition of real estate is split between different investors. They invest in the securities issues by a special purpose vehicle established by financial ownership of the property. Such a special purpose vehicle purchases the

real estate property on behalf of the investor. Purchase would depend on the offering provided by the platforms. The property can be purchased by the individual in the form of a defined share, say 10% of the shareholding or built up area, say square feet basis etc.

Who regulates the investment?

Securities and Exchange Board of India (SEBI) has recently proposed to bring such Fractional Ownership of real estate as micro, small and medium REITs under the SEBI (Real Estate Investments Trust of India) Regulations.

You Need to Know

Fractional ownership is partial ownership in large commercial properties. The amount of ownership is based on the ticket size or the minimum amount of share one wants to hold. The minimum amount generally would be Rs 25 lakhs and can be invested through fractional ownership platforms. The good part is that retail investors can take part, but fractional investment is currently not





governed or monitored by SEBI. But, as per recent announcements, SEBI has allowed a separate regulation for smaller REITs. Many of the fintechs have evinced interest in being brought under this SEBI regulation for greater transparency and client adoptability. Investments are allowed in developed and under construction properties.

Why Fractional Ownership?

Lower Entry Barriers. Generally investing in real estate requires significant upfront capital. But Fractional Investment Ownership allows you to enter with lower capital. While the investor can enter with a smaller financial commitment, fractional ownership allows the individual to participate in the lucrative commercial real estate market and enjoy potential financial rewards that come with it.

Passive Income. Fractional ownership also provides passive income through rental returns. The investor earns a proportional share of the rental income generated by the property, thus providing an additional regular income. This attracts retail investors who want a regular income.

By investing through Fractional Ownership, the investor can gain a stake in institutional grade properties. Fractional Ownership enables individuals to tap into advantages typically reserved for institutional investors. Through this pathway, individuals can generate attractive returns.

Hassle Free Management. Investing in real estate comes with various administrative burdens, such as tenant management, paper work, property management, maintenance etc. Fractional ownership gives a relief to the investors from these responsibilities. The professional property management company will manage all the operational aspects, ensuring that investors enjoy benefits of real estate ownership without any hassles.

Current Players in Fractional Ownership in India

While fractional ownership is gaining ground due to the high ticket size of real estate and with digitalisation, the platforms offer seamless opportunities to invest quite easily in this asset class. Multiple fractional ownership platforms (FOP) have come up in recent periods in India such as Smartowner, Strata, hBits, Asset Monk, YieldWiseX (earlier known as myRE Capital). These are tech enabled platforms and offer seamless online investments to investors.

Fractional Ownership Vs REIT – Which is More Beneficial?

REIT is a lot like Mutual Funds. Just as mutual funds pool money from investors and invest them in government bonds, direct equity stocks, etc, REITs pool money and invest in profitable real estate on behalf of the investors. Such properties are leased out to business organisations through which the part owner gets his share of the capital. But in REITs you cannot choose the property to invest in.

Fractional Real Estate Investing on the other hand happens as

per your choice. Fractional ownership platforms list the properties in their platforms which investors are welcome to check out. Based on the market price of each property, the minimum ticket size or fractional estate investment is decided. Finally based on the ticket amount you can choose how many portions can be bought or owned.

Major Differences:

- Fractional Ownership allows you to identify and invest in multiple properties in different locations. REITs present a set portfolio with a fixed number of assets in it.

- Fractional Ownership allows liquidity and you are free to sell your share anywhere you want. Non – traded REITs are also illiquid, which means there may not be buyers or sellers in the market available when an investor wants to transact. In many cases non – traded REITs cannot be sold for some minimum years. However there are some listed REITs that do not suffer from liquidity constraints.

- The minimum value set for investing in Fractional Ownership is usually upwards of Rs 25 lakhs. However in the case of listed REITs, being a retail product the minimum investments are much lesser.

- Fractional Ownership can purchase properties that are under construction or not in use presently. But REITs must have at least 18% of their investments in income – generating properties.

Things to Keep in Mind When Investing in Fractional Ownership

- **Extensive Market Research.** Fractional Ownership is something new in India, only a few companies have provided the opportunities to invest in Commercial Real Estate. It is better to do your own research and figure out if the company is worth investing in.

- **Get the best deal.** Searching for

the property with the highest return or minimum investments is a fairly easy task compared to other factors like evaluating the current market price of that property. Experienced investors know how to select a property where they don't pay more than the market price of the property.

- **Check for Customer Oriented Solutions.** Look for the business which gives a good deal with good returns in a long term perspective.

Risks Involved in Fractional Ownership

Fractional ownership of real estate, also known as co-ownership or shared ownership, involves two or more individuals or entities owning a piece of property jointly. While fractional ownership can offer a way to invest in real estate with lower costs, there are risks involved like:

- **Disputes Among the Co – owners.** Co-owners might have different opinions on how the property should be managed and how it should be used, when to sell and how to maintain. Dispute among the co-owners may lead to time consuming, costly and sometimes may result in the need for legal intervention.

- **Liquidity Risk.** Generally investing in Fractional Ownership of real estate is not very liquid, and it is up to the fractional owner to find a buyer if he wants liquidity.

- **Limited Control.** As a co-owner you will have very limited control on decision making. Every decision would need the approval of all the co-owners; there might be delay in decision making and execution.

- **Market Risk.** Like any other investments, the value of the property might fluctuate based on the market conditions. Hence it may result in loss at

times when you are planning to sell your share.

- **Management Risk.** Depending on the management structure of the Fractional Ownership, there is a risk that the property may not be managed properly or the managing company has a conflict of interest.

In Conclusion, Fractional Ownership of real estate is a new idea in the Indian real estate industry, which has created a novel potential for individual investors. High ticket commercial real estate holdings have become more accessible to investors, who can profit from investing in properties with high returns potential. But, the investors must do a detailed check of the facilitator and then be careful about the pitfalls.



Babu Krishnamoorthy

Babu Krishnamoorthy has spent the past 25 years as a financial adviser and entrepreneur, and is the Chief Sherpa at Finsherpa Investments Pvt Ltd. A money coach, he helps people dream big and achieve life goals.

He helps them plan and execute their financial plans in a manner that is predictable. He loves meeting people and spends his spare time reading non-fiction & is an amateur runner (with over 15 half marathons and one full marathon completed).

He has authored many books including "Unlock Secrets to A Wealthy Life". He is available at Babu.k@finsherpa.com (www.finsherpa.com)

NINE TAKEAWAYS FOR 2024

From India's Top Wellness Experts

Do we ever stop to think about what sets wellness experts apart? In my quest to learn more about preventive and holistic healthcare, I founded the Radiant Wellness Conclave in 2015, as a platform for thought leaders and stalwarts to share their experiences and advice. The result? A treasure trove of ideas to transform not just your health, but also your life. The most recent edition of the Conclave, held in September 2023 in Chennai, was no different. As we begin 2024, I'd like to share nine key takeaways from our nine experts – each on a different dimension of wellness. Happy New Year!



Social Wellness:

Dr Anbumani Ramadoss, *Politician*

The biggest advantage we have in India is the concept of a family system, which is lacking in the rest of the world. We can fall back on our families for support regarding emotional or intellectual or physical issues. As a former Health Minister, I would also like to point out that India has a huge native system of medicine – it encompasses Ayurveda, Siddha, Yoga, Naturopathy and many other streams. Even though I'm a 'modern medicine' doctor by qualification, I believe we have to merge both and get the best out of both these systems. In China, 60 per cent of medical clinics follow TCM or Traditional Chinese Medicine, which is hugely popular and successful. Only 40 per cent use modern medicine. We need to introspect along the same lines.





Intellectual Wellness:
Dr Palanivel Thiagarajan,
*Minister of Information Technology
and Digital Services, Tamil Nadu*

The beginning of intellectual wellness is curiosity. Anyone who wants to know 'why' or 'how', or even 'why not', is someone whose brain is constantly ticking. Sometimes we seek knowledge for knowledge's sake, but mostly it is for an understanding of our communities, families, societies, how they all fit together, and hopefully to apply that knowledge as we go through life. A close second to curiosity, is the notion of empathy. While applying for a job in Wall Street, New York, I was asked, "What is the most important attribute of a trader?" I answered 'Empathy', and the interviewer said I was absolutely right. Every time you interact with somebody, if you put yourself in their shoes, you're in a much better position to transact. Empathy also makes you capable of lateral, out-of-the-box and creative thinking. At some level you have to be physically and mentally well to pursue the luxury of intellectual wellness. You have to have equanimity, a sense of gratitude and community, a sense of well-being in the human network. Those are all building blocks to intellectual wellness.



Health Wellness:
Dr Shriram Nene,
*Cardiovascular and Thoracic
Surgeon & Healthcare Innovator*

In India, heart disease is the number one killer among all non-communicable diseases. How do you prevent that from happening to you? Firstly, identify your risk factors. If you have a first degree relative with heart disease, especially if they're less than 50, your likelihood of getting it is 4 –

10 times higher. The second is lifestyle. Certain things will put you at risk; sedentary nature, smoking and metabolic syndrome - while we've shifted from an agricultural to an industrialised society, but we are eating the same as what we did when we were farming! Thirdly, activity is only about 20 per cent of the equation in keeping you normal, but it helps release endorphins, among other benefits which cause you to be on the right track. Lastly, be positive and social. In Italy there are cities which have an abnormally high life span. When experts studied why, it wasn't because they had superhuman genes or a different diet. In many cases they had high social networks. In India as well, we have a deep social network but it's slowly getting fragmented. So if you live in a nuclear set-up, create your base of 3 a.m. buddies! Stakeholders can bring the level of awareness and access up in the metros and more importantly in the rural areas, where 70 per cent of the population live. India is an old culture, but it's a young country with a median age of 28. We have an opportunity to change the plot and dialogue.



Emotional Wellness:
Revathi,
Actor & Director

Life today is very tough. It is taxing mentally, psychologically and physically. Everyone is working more than 20 hours and people don't have a social life. When I was young, my father would be home by 5.30 p.m, and we would visit neighbours and friends, children had time to play together through the week, and one was not constantly put into different classes and tuitions. I definitely feel that schools need a session on emotional wellness to tell children how to cope with all of this. Another important aspect of emotional wellness is sleep. When you don't have enough, then burnout happens quickly, and there is a lot of emotional pressure. Lastly, sometimes I think we invest too much into certain aspects of life. We need to prioritise, understand where to invest and where to step back. There is absolutely no 'have to' for anything!





Mental Wellness:
Faye D' Souza,
Journalist

‘Enough’. Let’s focus on this word. *‘Atelophobia’* is the fear of imperfection - that you are not enough and not worthy of love. Women will especially understand it. *‘Am I successful enough?’ ‘Do I have enough money?’ ‘Will my kids be happy?’* With social media, these questions have been thrown over to the world. For me, it all started when I walked out of a job as a television news

anchor, choosing my integrity instead. In the aftermath, I had crippling anxiety, so I took the help of a therapist. During my session, I had to sit down and decide what I wanted to be when I *‘grow up’*. Do I want to be a journalist? Is there anything else I want to do? What do I want my contribution to society? I focussed on the word *‘dignity’*. Because, when you work in television, there’s no dignity for the anchor, for the guest who’s speaking or even the audience. I regularly see a therapist now, and I recommend it to everybody. Like we talk to a doctor for our physical health, we have to have someone who understands us mentally. After balancing my life, a miracle happened last year that I didn’t expect. In spite of being told my whole life I couldn’t have children, I was blessed with a baby. Perhaps it was the Universe’s way and God’s way of telling me, that I am enough.



Technological Wellness:
Raju Venkatraman,
Entrepreneur & Founder of
Medall Healthcare Pvt Ltd

With the power of Artificial Intelligence (AI), we will be able to personalise medical care to individuals in the future. We can come up with predictive algorithms using AI. We are not talking about replacing the doctor, but rather giving them a lot more data to make smart decisions. Early diagnosis can not only cut costs, but can also improve the probability and quality of life. Also, drug discovery takes 10-15 years to get a molecule out. I see that happening in 1-2 years because of the data sets available. We can prevent things like sickle-cell anaemia and cystic fibrosis because we now know the genes and these can be edited over time. Ageing genes have also been identified, that can slow down ageing and increase lifespan and health span. Digital doctors will also help. In fact, I hope 5G works as fast as it should in rural India as this could benefit the 200 million people who don’t have accessible doctors, even if they have other healthcare facilities.



Physical Wellness:
Major General Vikram Dev Dogra,
AVSM, - Three-time Winner of the
Ironman Challenge

I’ve always believed in mind over matter. Only if you can dream it, can you achieve it. If your mind says no, then your body’s not going to say yes. You have to use techniques to keep yourselves motivated. The mind is always wanting to quit. But the more I trained and the more my body hurt, the better I felt. When you do physical activity, endorphins make you feel happy. Self-discipline is what sees you through any situation and you must also be mindful of physical activity. As I started training, I learnt this. For instance, people are of the opinion that if you’re going for a run, you can listen to music to keep you entertained. But if you do that, you’re not being mindful and you’re not in the

moment. If you're running, you should do it because you enjoy it. So I used a technique called the breathing technique, also used in meditation. I would synchronise the fall of my feet with my breathing. How does it work? For three steps you exhale, and for the next three steps you inhale. Follow that rhythm continuously. Once this rhythm sets in, after say half-an-hour (if you're going on a long 20 km run!) you actually get very mindful about it.



Occupational Wellness:
**Lieutenant General
Devraj Anbu**

Occupation isn't the right word to describe service in the Armed Forces. It's not a regular 9-to-5 job. A soldier is at work 24 x 7. It is a home away from home. Yes, the Army takes care of every other aspect of wellness – physical, social, intellectual, spiritual, financial. The soldier is groomed to be able to focus on the task at hand. Inspiring leadership is crucial. When that is there, everyone in the Armed Forces is ready to make sacrifices.



**Lieutenant General
JS Sandhu:**

Of course, it isn't easy. Everyone is afraid. As Field Marshal Sam Manekshaw said, "The only guys who aren't afraid are the Gorkhas". But it is getting over fear which gives you that extra courage. You're a leader and commander and you've got men in front of you looking to you for inspiration. If you display fear, you'll lose your battle. The thought of your unit's self-esteem carries you across that threshold. That courage comes from within and you face it. What sustained me personally during those times was prayer.

Financial Wellness:

Priya Goutham,

Co-Founder – Two Trees Workspaces

and Cretium Business Solutions,

Head - Mentorship National FICCI Flo Start-up Cell

(in conversation with start-up entrepreneurs

Moinak Banerjee, Nimisha J Vadakkan and

Suryanarayanan Paneerselvam)



For a company to be sustainable, other than money you get from investors, you have to be profitable over time, which will make it last and grow. You have to make profits from day one. All of us should understand finances and not rely on anyone else. Be in control of your own finances, always. Please be particular about parting with your shares, even if it's 1%. Venture Capital Funds help to scale and one should reach out appropriately. Bootstrap mentality for start-ups is a must. Pick up the business and cover the ground. When you know you've made a mistake, it is important to course correct. Keep your ear to the ground for technological changes that could impact your business. Have a balanced work-life.



Dr Renuka David, MBBS, PGD (MCH), USA-PhD (HC) is the Managing Director of Radiant Medical Services and an alumnus of the Coimbatore Medical College. She has been a frontier doctor, working extensively with women and young adults in urban, rural and tribal India. She has also been a contract doctor with the Indian Army for three years. Dr Renuka dons many avatars as an entrepreneur, doctor, professional speaker, television show host, TEDx speaker and wellness expert. She is the Founder-Curator of the immensely successful Radiant Wellness Conclave.



Dr.Renuka David

*For medical queries, please email:
ask@drrenukadavid.com*

BATTLE OF NARRATIVES

IMPACT OF INFLUENCE OPERATIONS

Influence Operations are tailored actions to shape perceptions of targeted individuals (people, military, policy makers, international community, etc) to achieve larger political, economic, social, military or a combination of these objectives. This article discusses the effect of dominant narratives on warfighting and national governance.



Gaza City after Israeli air strikes, October 2023

Putin is evil! Russia is a dangerous threat to the global community! This was the narrative being spewed from many Western media channels in March - April 2022, after Russia's 'special military operation' commenced in Ukraine. I realized that the Western story was more pronounced, more widespread, more visible. The Russian side of the conflict was not catching traction. In essence, the global narrative is largely controlled by the US and Western European nations, because the "media giants" are based there. Nothing new, as this Western control has been a feature of the last century plus. Not worrisome, as long as the truth is portrayed, but invariably the truth is distorted in tune with the hidden interests behind this Western curtain.

Come October 23, and we see **Information Warfare** (or influence operations in my perception) in full steam. Different media channels play on "good Israelis" vs "bad Hamas" story lines, dependent on the ownership patterns or location of these channels. Al Jazeera castigates the Israelis for the wanton

destruction in Gaza and their disproportionate response, while the Israelis have deftly deployed many innocent Jewish victims, influencers and analysts who describe the horrors perpetrated by Hamas. Tunnels under hospitals in Gaza are shown to counter the allegations of targeting healthcare facilities. Videos and audio tapes affect the perceptions of the audience, and Palestinians give out the number of innocent children, women and elders killed in Israeli air strikes. The Hamas are terrorists is one narrative, the other narrative calls them freedom fighters. **Interestingly, the Western media giants control over the narrative has been diluted by social media** – Instagram reels, TikTok videos and YouTube shorts have deluged the younger generation and the situation in Gaza becomes clearer. Israeli justification is countered by excesses in Gaza over the past couple of decades, and perceptions are altered. The information war influences the global community and calls for restraint and peace become shriller, so the warring sides agree to a temporary truce.

This article is not about who is right and who is wrong. It is about bringing forth **the power of narratives**, the influence that they have on military operations, on the duration of campaigns and the type of operations. Military leaders must realize that influence operations are a vital part of contemporary conflicts and confrontation. The **"Just Cause"** for the war is constructed through electronic, social and print media; each side tries to take the moral high ground. Around two decades ago, the US Government painted Saddam Hussein black, the media highlighted the Weapons of Mass Destruction (WMD) danger. The Iraq War became a *just intervention* by the Western powers, and Saddam Hussein was neutralized. The WMD narrative was just a tool for

the desired regime change. The truth was not material, information warfare willingly uses 'hoax' stories if convenient.

Information warfare is not a recent phenomenon, but has been around in past wars too. In the Second World War, propaganda was the term used to vilify the enemy and to justify and encourage domestic efforts in the war. The Reich Ministry of Public Enlightenment and Propaganda was established in 1933 under Joseph Goebbels, who wrote *"The essence of propaganda consists in winning people over to an idea so sincerely, so vitally, that in the end they succumb to it utterly and can never again escape from it."* The Nazi Government used radio, press, books and all forms of communication media to promote their nationalist ideology, to highlight national pride and to paint the Russians as 'inhuman beasts'. The West is repeating that portrayal today – the dangerous Russian Bear!

Realising the value of such propaganda, the BBC World Service foreign language broadcasts continually attempted to influence the German people during the War. Leaflets and postcards with subversive messages were dropped on German towns regularly. The tools used by Britain were effective. Goebbels, who committed suicide later, wrote, *"Enemy propaganda is beginning to have an uncomfortably noticeable effect on the German people.....British broadcasts have a grateful audience."*

During the Kargil operations, Indian media swayed the nation with patriotic fervour, and boosted the morale of the soldiers on the icy mountains. National sentiment is a powerful entity which multiplies the intangible capabilities in battle. The Israeli Army fighting in Gaza also has such a national sentiment adding to their calibre. The perception of being morally right gives greater strength to a fighting unit; the Hamas fighters derive their moral cause from Islam and its radical

interpretation. The breaking down of the moral high ground in the Vietnam War influenced the American audience and the American soldiers; they returned to the Homeland defeated. Long duration conflicts also cause fatigue and slowly denude the justness of the campaign – Operation Enduring Freedom in Afghanistan also reached such culmination, and the justness of the intervention is forgotten.

Influence operations are not a marginal part of sub-conventional operations, but play a major role. Pakistan has been indulging in information warfare in Jammu and Kashmir (J&K) for over three decades, targeting the mind-set and perceptions of the *Awaam* therein. They have employed proxies (armed and unarmed), political groups, the Bar Association, teachers, funding, etc to drive their agenda. The Inter Services Public Relations (ISPR), the publicity organ of the Pakistan Armed Forces hired hundreds of young persons to prepare "social media content" and broadcast it into J&K. Video clips and audio notes influence the perceptions of young gullible minds easily. These influences fuelled the agitation and stone pelting in Kashmir in the last decade plus. Like the *Intifadeh* in Palestine, the street protests are an intrinsic part of the proxy war. Pakistani agencies continue to recall the grievances against the Dogra rulers before independence, and link it to the religion card. The 2020 Edition of *Pakistan Army's Green Book* emphasizes the criticality of engaging with India in the information domain.

Influence operations are not limited to war alone. The global strategists realize that it is easier to safeguard respective national interests by ensuring "friendly" Governments in

possible conflict zones. Regime change is a preferred method, and mass agitations can be engineered to topple inimical Governments. The internet, global connectivity, social media and financial access enable such insidious campaigns. Democracies are also vulnerable, and there are credible allegations that the Russians influenced the US Presidential Election in 2016, in favour of Donald Trump. Veles, a small town in Macedonia, Greece was the epicentre of political disinformation targeting the American voters in 2016. Many youth in the town were paid to route 'hoax stories', these stories generated more clicks and views. Some stories read as *"Pope Francis endorses Trump"*, or *"ISIS calls upon Muslim voters to vote for Hillary"*.

Another striking example is the Chinese attempt to influence the Taiwan elections. The ruling Democratic Progressive Party is disliked by Beijing, and the Chinese have used military intimidation and media channels to bat for Kuomintang, a friendlier party. China has successfully infiltrated the Taiwanese business and media community, who regularly repeat pro - China bytes. These influence initiatives are dovetailed with the military harassment of Taiwan. Chinese fighter jets violate Taiwanese airspace routinely on an almost daily basis – 1737 airspace violations were reported in 2022, vis-à-vis just 20 violations in 2019. Chinese fishing vessels also enter Taiwanese territorial waters at will and several military exercises have been conducted around Taiwan in the last couple of years. The message being delivered by the pro - China lobby is that USA will abandon Taiwan, when push comes to shove, during any military action by China. The



The front page of *The Guardian*, the day after Russia's Special Military Operation in Ukraine commenced

media and TV channels were given free access to Xinhua media content (text, photos and videos) for six months. Many stories started appearing in Pakistani media on the benefits of CPEC; many positive stories about Chinese assistance to Pakistan added to the influence operation! So, narratives have a noticeable impact.

Considering the forthcoming elections in 2024, India is undoubtedly a significant target for information warfare. We will have to remain watchful about the '*misinformation – disinformation – malinformation*' campaigns which will run. The dedication and fortitude of the sentinel on the borders should not be compromised by powerful wheeler-dealers in the national capital.

intimidation is clear, the psychological effects of such messaging must be understood – *weaken the enemy's mind before the blow*. The Chinese are indeed masters in the art of winning without fighting. We too need to be vigilant.

Influence operations are also executed in friendly allies. The Chinese sought to reshape the information environment in Pakistan by setting up a "*nerve centre*", ostensibly to counter negative stories about Chinese interests in Pakistan (which are circulating in Pakistan). Beijing proposed setting up a "**CPEC Rapid Response Information Network**" and Beijing wanted significant control over Pakistan's domestic information environment. They planned to feed their narrative to Pakistani think tanks, academia, media, etc. Expectedly, Pakistan was wary about the Chinese plan. But the wily Chinese don't give up easily. Xinhua, CGTN and other Chinese media channels started Urdu and English language services in Pakistan; all Pakistani

What lies ahead in the battleground? In future, information warfare will have a greater effect in conflicts and confrontation. Artificial Intelligence will assist in deep fake videos, innumerable false reports would appear credible, true pictures and facts may be jammed, satellite imageries can get doctored too, hacking would be done of the communication networks. Decision makers may get confused about the actual situation in battle, and faulty decisions could lead to blunders. Our young leaders will have to be trained to judge the facts correctly. In the non-military arena, influencers are becoming more trustworthy than traditional media. During war, paid influencers may propel harmful content on to their followers. The fault lies with the regular electronic media channels - they have lost credibility having sacrificed truth at the altar of bias, channel ownership guidance and for TRPs.

To sum up, we have to be incisive to sift the bias and truth in the content being trolled. Young military leaders should be able to perceive the '*misinformation – disinformation – malinformation*' designs being projected. **Three parameters be kept in mind – Who is giving this story? What is their bias and interest? What is likely to be the true picture?**

Let us remember that influence operations are a weapon/tool, being used consistently, continually in war and peace – we need to be careful of inimical forces in this **Information Age**.

Lt Gen JS Sandhu (Retd) Editor

THE MADRAS SAPPERS AT SILKYARA TUNNEL



201 Engineer Regiment of the Madras Sappers, commanded by Colonel Dhirender Joshi deployed a column for the Silkyara Tunnel Rescue Operation in November 2023. The column fabricated rescue contraptions, made a modified circular casing for the evacuation of the workers, and fabricated the casing for vertical drilling. In the photo above, after the successful rescue, the Sappers with General V K Singh, Minister of State for Road Transport and Highways and Shri Pushkar Singh Dhama, Chief Minister Uttarakhand.

ARTICLES FOR PUBLICATION

Readers interested in contributing articles/poems/cartoons/humour/anecdotes for publication may kindly email to chiefeditor@medalsandribbons.com. Some of the authors of content selected for publication will be suitably remunerated, between Rs 1000/- to Rs 5000/-, depending on the length and content value. The decision of the Editor would be final in this respect.

• • •

The views expressed in this magazine are those of individual authors, and not necessarily of the Editorial Team or management. No part of this publication may be reproduced or transmitted in any form without permission from the Editor.

Any queries related to the magazine may be raised on www.medalsandribbons.com or may be mailed to info@medalsandribbons.com

Visit us at www.medalsandribbons.com Follow us [f](#) [t](#) [i](#)



RADIANT

GROUP OF COMPANIES

Varied Business Interests - One Mission.... Redefining Excellence



**RADIANT CASH MANAGEMENT
SERVICES LTD**



**RADIANT
PROTECTION FORCE PVT LTD**



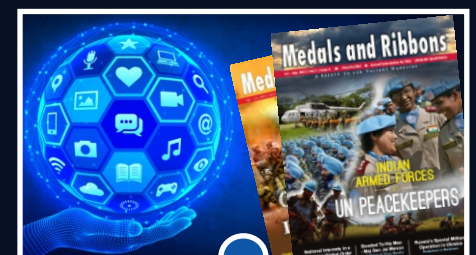
**RADIANT
BUSINESS SOLUTIONS PVT LTD**



**RADIANT
MEDICAL SERVICES PVT LTD**



**RADIANT's
CSR INITIATIVES**



**RADIANT CONTENT CREATIONS
PRIVATE LIMITED**

Regd. Office : No.28, Vijayaragava Road, T.Nagar, Chennai - 600017
Ph: 044 28155448 / 6448 / 7448. Fax: 044 28153512

Corporate Office : No.4/3, Raju Nagar, 1st Street, Okkiyam Thuraipakkam,
Chennai - 600096. Ph: 044 4904 4904

www.radiantgroups.com