Pragyan Conclave 2020

Changing Characteristics of Land Warfare and its Impact on the Military

04-05 March 2020

Manekshaw Centre, New Delhi

Director, CLAWS : *Lt Gen (Dr.) VK Ahluwalia, PVSM, AVSM**, YSM, VSM (Retd)*

Seminar Coordinator : *Col Anuraag Singh Rawat, SM*
Dr.Jyoti M Pathania

S R Written by : *Col Anuraag Singh Rawat, SM*
Dr.Jyoti M Pathania
Ms Kanchana Ramanujam

Rapporteur : *Ms Anashwara Ashok, Mr Vishakh K Valiathan,*
Ms Tejusvi Shukla, Mr Mohak Gambhir
& Mr Alakh Ranjan

Editorial Board : *Col Himanshu Kataria, SM*
Col Pradeep Mehta

Pub Manager : *Ms Shreya Das Barman*
Web Manager : *Mr Raghunandan*

Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi – 110010
Phone: 011-25691308; Fax: 011-25692347
Email: landwarfare@gmail.com; website: www.claws.in

Printed in India by
Delhi Area Printing Press
Delhi Cantt
New Delhi – 110010

*'Pragyan'(**प्रज्ञान**),derived from the Sanskrit word 'Pragya'/'Prajña' ('**प्रज्ञ**' in Devanagari script), is composed of two words - the prefix "pra" meaning 'before' or 'foremost' and "gya" (or "jna") meaning 'knowing'. 'Pragyan' could be understood to mean an insight, understanding, judgement and intelligence.*

However, 'Pragyan' does not merely denote knowledge, but wisdom that is gained through critical analysis and reasoning. In fact, ***it is the purest and the highest form of intellectual discourse and understanding****. This word has been used many times in ancient Indian texts such as the Yoga Sutras of Patanjali, the Vedas and the Upanishads, to refer to 'consciousness', 'intelligence' and so forth.*

True to this, the Pragyan Conclave is a biennial forum, organised by the Indian Army and the Centre for Land Warfare Studies (CLAWS). The Conclave will include domain experts from across the globe to discuss and deliberate on a particular theme related to defence, security and strategy.

SEMINAR REPORT

CONTENTS

S No	Contents	Page No
1.	**Commonly used Abbreviations**	V
2.	**Executive Summary**	04-18
3.	**Objectives and Modalities**	22-23
4.	**Inaugural Session** • Keynote Address • Inaugural Address • Award Presentation to Winners of Field Marshal Manekshaw Essay Competition on National Security	26-33
5.	**Session I: Evolving Warfare – An Insight into the Changing Realm** • Opening Remarks • Sub-Theme 1: Military Futures - Prospects and Possibilities • Sub-Theme 2: Changing Character of Conflict - Imperatives of Transformation • Sub-Theme 3: Trends in Warfare - Concept of Victory and Strategic Conquest	36-46
6.	**Session II: Technological Revolution – A Seminal Change** • Opening Remarks • Sub-Theme 4: Salience of Information Warfare in Multi-Domain Operations • Sub-Theme 5: Cyber as a Tool of Warfare - Paradigm Shift • Sub-Theme 6: Drivers: Space Command to Space Force • Sub- Theme 7: AI and Robotics - From Concept to Delivery	47-59
7.	**Special Address**	64-66
8.	**Session III: Transformation in the Battlespaces** • Opening Remarks • Sub-Theme 8: A New Strategy for the Changing Era • Sub-Theme 9: Firepower - The Impact of Long Range Vectors & Precisionary • Sub-Theme 10: Special Forces - A Force Multiplier for Land Operations • Sub-Theme 11: The Nuclear Environment to Include the Impact of Hypersonics	70-82
9.	**Session IV: Hybrid/ Sub-Conventional Warfare** • Opening Remarks • Sub-Theme 12: Operations in a Grey Zone Environment • Sub-Theme 13:Technology and Urban Warfare • Sub-Theme 14: Rise of Non-State Actors • Sub-Theme 15:The Salience of Technology and Social Media in Hybrid Operations	83-95
10.	**Closing Remarks**	98-100
11.	**Concept Note**	106-109
12.	**Programme**	112-113
13.	**Bio Data of Guest Speakers, Chairpersons & Panellists of the Sessions**	116-123

Commonly used Abbreviation

S No	Word	Abbreviation
1	Fourth Industrial Revolution	4IR
2	Intelligence, Surveillance and Reconnaissance	ISR
3	Non-Contact Warfare	NCW
4	Anti-Access/Area Denial	A2/AD
5	Israeli Defense Force	IDF
6	Information Warfare	IW
7	Divisional Information Manoeuvre Group	DIMG
8	Advanced Research Projects Agency	ARPA
9	Defense Advanced Research Projects Agency	DARPA
10	Joint Surveillance and Target Attack Radar System	JSTARS
11	Defence Space Agency	DSA
12	Indian Space Research Organisation	ISRO
13	Lethal Autonomous Weapons System	LAWS
14	Ballistic Missile Defence	BMD
15	Special Forces	SF
16	Liberation Tigers of Tamil Eelam	LTTE
17	Long-Range Patrol	LRP
18	Nuclear Posture Review	NPR
19	Hypersonic Glide Vehicle	HGV
20	Lashkar-e-Taiba	LeT
21	Tactical Nuclear Weapon	TNW
22	Chief of Defence Staff	CDS
23	Department of Military Affairs	DMA
24	Artificial Intelligence	AI
25	Islamic State	IS
26	Integrated Battle Group	IBG
27	Improvised Explosive Device	IED
28	National Security Agency	NSA
29	Anti-Satellite	A-SAT
30	Technology Experimental Satellite	TES
31	Ship Submersible Ballistic Nuclear	SSBN

MANEKSHAW CENTRE

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

General

War, as we have known it, is changing and changing rapidly. The Fourth Industrial Revolution (4IR) fuelled by the fusion of technologies, aided by concepts exploiting these, is being practiced by State and Non-State actors, which is altering the very way we fight. Technological advances are driving the 'changes in the character of warfare' leading to some scholars even challenging the Clausewitzian theory of 'unchanging nature of warfare'.

Many believe that while the nature in terms of the victor imposing his will on the vanquished, the organised violence, the blood and gore is constant and unchanging, the character keeps on evolving and changing with respect to how wars are fought in terms of weapons, technology and strategic context. Technologies such as AI-driven targeting, automation and intelligence, surveillance, reconnaissance (ISR) are impacting the character of war, while the unchanging nature of force and violence will manifest in newer forms.

There is a rapid geo-political, economic and social change taking place in the world with technology playing a major role in it. While Clausewitz attributed the change in the character of conflict to three factors, namely capabilities, circumstances (geo-politics) and motives; the competition and confrontation between nation states vis-à-vis the fast-diminishing natural resources, could very well be the crucial, fourth factor.

While hard power will always remain relevant and will have to be leveraged in accordance with the changing strategic context, the Armed Forces need to keep pace or stay ahead of the change. However, warfare evolves faster than war-fighters do and the Armed Forces, being conservative by nature, often prepare not only for the last war, but very often, for the wrong war.

Complexity and ambiguity have crept into present-day conflicts as compared to wars fought three decades back, with geo-strategic realities and spaces being altered without altering the state of peace. There is a blurring of lines between what is equated to regular and irregular military activities and conventional & non-conventional activities.

Today, the battlefield is everywhere –land, space, social media, the human cognitive-domain and so forth. Consequently, everyone is a warrior, not just the uniformed personnel. Hence, warfare is becoming less and less military i.e. shades of grey have crept where the adversary tries to achieve geo-political and territorial ends without overt military aggression and crossing the threshold of open warfare. These grey zone operations are a national and institutional challenge which needs a whole-of-government approach, infact, a whole-of-nation approach. A strategy to counter grey zone challenges must focus on political and bureaucratic adaptation and building the resilience of civil societies. Additionally, apart from the conventional and nuclear domains, deterrence needs to be built in the grey zone too.

Armies need to re-tool and re-structure for modern combat, given that information is the new Center-of-gravity and data – a critical raw material and a new strategic resource. The digital battlespace is re-defining the traditional boundaries and there is a need for incorporating the

power of the digital network and space assets into the armed forces and the complete metamorphosis of the nation's security horizon, outlook and responsibility. Networks have to be created and protected seamlessly as well as integrated across agencies and forces. The challenges of the digital world would extend to the industrial ecosystem too and thus it is important to develop capacities in that critical domain.

Consequently, the Armed Forces need to be prepared for the conduct of overt, covert and outsourced operations, in the backdrop of the fact that the qualitative technological advantage between States or between the State and Non-State actors is eroding and would continue to erode further. Multi-domain operations which would seamlessly and concurrently integrate effects across multiple domains and create multiple dilemmas for the adversary, would have to be carried out. Through multi-domain operations, the adversary could be overwhelmed by acting faster, deceiving, disrupting and dominating the narrative.

The concept of 'Victory' is also changing and cannot be defined using the logic of World War II, since 'Victory' no longer rests on the ability to inflict massive destruction, but on the ability to wrest popular support from one's opponents. It could be defined as an outcome or descriptive statement of the post-war situation, or as an aspiration driven to accomplish specific objectives through the use of force. The rise of non-state actors and transnational criminal networks has also not only necessitated a nuanced approach to achieving 'Victory', but also fuelled the postulate of a narrowing space for all-out conflicts.

Ancient Indian strategic thought could be used to create contemporary templates for modern, geo-political competition. Predicated on the sheer majesty of power and guile, the Kautilyan view in strategic policy espouses an outward orientation, a calibrated power projection and influence which can be effectively employed in today's environment.

In the Indian context too, due to the exponential change in technology and its cascading impact, there is a need for taking a wide-angled view of the changed dynamics that necessitate a comprehensive transformation of the Indian Armed Forces and the wider defence ecosystem in India, in order to be future battle ready. The rationale behind keeping massive funds locked up in large inventories needs to be revisited with the need for a 'restructured, ready-to-wage military instrument' emerging as being the requirement of the time. The chaotic and unpredictable nature of conflict notwithstanding, it is for the professionals to make reasonable assessments so that policy, resource and planning process can be aligned.

Evolving Warfare – An Insight into the Changing Realm

Warfare is evolving, especially given the emergence of grey zone, hybrid and urban warfare and to keep pace, one needs to adapt to the changing conceptual, structural and cultural, military needs and sensibilities, as also adjust to the skill and speed at which the transition is being made. The world has moved from foot-soldiers, to elevated platforms, to network-centric platforms, to knowledge-based warfare, further now to Non-Contact Warfare (NCW). In the present time, the battlefield is everywhere, thus we need to be always prepared.

Military Futures – Prospects and Possibilities. Military futures is entirely imaginable, if not completely predictable, Gen Billy Mitchell's prescient words, espousing the cause of

airpower at sea, predicted events which unfolded nearly 20 years later. There is a need for change of the strategic mindset, as the mindsets of traditional, western-style militaries are crucibled in distinct thresholds of war and peace. Adversaries, both state and non-state, have exploited this oversimplified conceptual and legal framework of war and peace by waging a battle in the virgin terrain– that of the sub-threshold space. In today's 'Information Age conquests', military vile & guile and not brute force, can be used to secure competitive advantage and thus the indirect approach characterised by strategic subversion and tactical deniability will reap rich dividends. There is a need to doctrinally shift major focus to the sub-threshold space, develop an entirely different and elevated set of attributes and skill sets to operate & regain and seize the initiative in that domain. Additionally, acquiring and inducting the capabilities and technologies that the digital forces of tomorrow would need will require deepening the engagement with the private sector. Due to India's budgetary constraints and the issue of live and active, unsettled borders, 'continentality' will continue to prevail over India's national security outlook. However, 4IR demands comprehensive transformation - in concept & outlook, structure & culture and from mere jointness to full spectrum integration.

Changing Character of Conflict – Imperatives of Transformation. There can be no real transformation sans change in organisational and operational concepts, since transformation is not just related to technology. Not all transformation is positive or necessary and if a force is relevant to the threats being faced, transformation may not be required, since it is risky and expensive.Knowing when to transform, is one of the biggest challenges in the transformation process. Initially, concept and reality are nearly the same and there is no need to transform. However, the relevance-gap i.e. the gap between concept and reality, increases as time and environment change, exacerbated by a denial to acknowledge this gap, till there is a major surprise/loss/incident that brings out the need for transformation. In addition, when the adversary catches up with own military revolutions, it also necessitates a new revolution. For Israel, the present day relevance-gap is a strategic challenge since its enemies have been able to take advantage of the proliferation of new technologies and have transformed from terrorist organisations to basically near-peer adversaries with the ability to carry out their own anti-access/area denial (A2/AD). Transformation in the Israeli Defense Force (IDF) is stuck, with the relevance gap having increased, however, bringing tactical mobility back to the land battlefield may ensure successful transformation. Another difficulty is managing transformations and innovations which falls between services and the IDF is trying to strengthen the joint level with new organisations, that will be able to manage these. While there is a tendency sometimes to stretch old concepts to solve new problems, without new concepts actually being generated, the ability of a military to meaningfully change is intimately connected to its ability to understand the broad technological potential of the time and through that application, to understand warfare in a new way.

Trends in Warfare – Concept of Victory and Strategic Conquest. War is a social construct to unleash violence, which is direct, intentional, organised, sanctioned, regulated and sometimes, ritualised. Trends in warfare have been dictated by technology, concepts, threats and other factors and while the 'Hundred Years War' witnessed a manifestation of national identity and loyalty to the Nation State, the Industrial Age saw the advent of refined weaponry and technology giving rise to new tactics. World War I saw the tedious trench warfare, while German biplanes brought in the third dimension, World War II witnessed

armoured sweeps with synergistic air support, the use of nuclear bombs, while the Cold War saw the race for supremacy in the new domain – the outer space. Post the invention of computers and internet, the cyber domain has become the latest domain for future battles. The Fourth Industrial Revolution (4IR) will have a major impact on international security and while the set of natural resources critical to strategic industries would change, their use as a geo-economic tool would be repeated. The greatest impact of AI on conflict may be socially mediated. Algorithmically driven, social media connections funnel individuals into transnational, but culturally enclosed echo-chambers, radicalising their worldview. In today's environment 'Victory' should be considered within the context of the political aim and war and victory is about statecraft, rather than only hostilities. Clausewitzian understanding of military victory is a condition where the enemy's ability to enter battle and resist or resume hostilities is destroyed, however this may be a thing of the past. Complexities of defining victory in counter-insurgency warfare get compounded due to the non-state composition of the adversary and the difficulty in using metrics to indicate progress towards a stated goal in such an environment. Strategic successes cannot be achieved by military force alone and victory does not mean the defeat of the opponent's military capabilities, but the successful resolution of the deeper problems which lie at the root of the conflict.

Technological Revolution – A Seminal Change

The world is witnessing a high intensity of information and cyber warfare due to four faultlines i.e. no consensus on the applicability of international law, dispute over control of the root servers, non-attributability of the cyber attacks and no clear definition of what constitutes a cyber war. With a million attacks per month, India is the second most-attacked country in the world and what makes 'cyber deterrence' very difficult is the fact that it requires 'persistent presence' in the cyber domain of the adversary.

Salience of Information Warfare in Multi-Domain Operations. The increasing number of domains, the ability to conduct cross-domain operations and the proliferation of technology and communications has brought in radical changes that provide both threats and opportunities. While hard power remains relevant, the ability to use the information domain to disrupt, attack the homeland and undermine social cohesion makes information warfare (IW) a vital facet of constant competition and warfare. Key aspects to IW in UK are a joint doctrinal concept, achieving information superiority and then leveraging the information advantage achieved. The 6th Division, which prepares the army's Information Manoeuvre and Unconventional Warfare forces, has a concept of 'Information Manoeuvre', which, at its heart, is about fusing and synchronising multiple information-centric capabilities in one Division under one command. Information Manoeuvre allows the UK to generate options to mitigate risk and seize opportunities in the era of constant competition. The aim of preventing the adversary from dominating the perceptual landscape and gaining operational surprise in the grey zone is achieved by persistent, worldwide engagement, both physical and cyber, through collecting intelligence and challenging the adversary's incremental gains in the physical, virtual and cognitive spaces. Enemy propaganda and covert operations are exposed and technical intelligence is gained to build the battle picture further. This is then followed by shaping the environment for offensive information operations. In an environment above the threshold of conflict, the Divisional Information Manoeuvre Group (DIMG) is deployed and

it delivers stand-off decision-advantage to the commander. It counters threat by looking at how the adversary is gathering intelligence and uses cyber and electromagnetic activity, influence operations, networks and multi-domain ISR. This is enhanced by a reach-back deep into the UK, to the specialist Reserve Officers. The battle-winning advantage by the DIMG is gained by leveraging all multi-domain assets. UK believes that IW is an absolutely critical factor of multi-domain operations and its doctrine of information manoeuvre implemented through the 6th Division provides it with great advantage.

Cyber as a Tool of Warfare – Paradigm Shift. In US, the earliest use of computer networks commenced under the visionary guidance of JCR Licklider, in the early 1960s with the Advanced Research Projects Agency's (ARPA's) use of the Semi-Automatic Ground Environment computer system, that was designed to link 23 air-defence sites to coordinate tracking of Soviet bombers and the Pentagon's 'command and control' programme. Vietnam War was actually the first demonstration of a'network-centric warfare' and a computer network combined air and land operations to fight the Viet Cong insurgents. Post-Vietnam, the Pentagon decided to take the sensors and networking capabilities developed for counter-insurgency and apply them to land warfare, against the Soviet conventional advantage in Europe, which eventually gave rise to the concept of Joint Surveillance and Target Attack Radar System (JSTARS). In Kosovo, US' Defense Advanced Research Projects Agency (DARPA) came up with an idea of distributing combat capabilities across a network called the Future Combat Systems, however in Iraq (2003), where home-made bombs proved deadly for the US forces, they realised that they could never have enough information to make up for armour. The US battled insurgency in Iraq, using the Real-Time Regional Gateway – designed to pull together many feeds of information ranging from intercepted phone calls to information on bomb attacks and after analysing that data, identify insurgent-networks and predict attacks in real time. As far as the IS was concerned, it was an entirely different problem compared to the insurgencies in Iraq and Afghanistan. 'Operation Glowing Symphony' was the biggest cyber operation carried out by the US Cyber Command, that involved attacking the IS' information networks with malware and other tools and preventing IS members from communicating and posting propaganda, thus focusing on countering propaganda. However, what seems to be lacking in US, compared to the post-Vietnam situation, are visionaries who can think about how to take the last 20 years of cyber research that was applied to counter-insurgency and adapt it to the national security challenges that the United States and its allies face today, whether in land warfare, or any other area of national defence. There is thus, a need to have a different viewpoint on how we use the computer network and what are we defending against, to optimise the cyber warfare capabilities.

Drivers – Space Command to Space Force. Militarisation of space, is the use of satellite technology for navigation, reconnaissance, communication and various other aspects of intelligence-gathering. It is legal and not against any treaty or rule. Weaponisation, on the other hand, is using militaristic means to prevent the adversary from using his/her satellite-network. India at present could be considered a 'second-rung space power', however, it could become a 'smart (space) power' by incorporating both hard power and soft power elements into its space capabilities. The focus of the Indian space programme has never been military and the policy remains the same even today, however some mid-course correction is ensuring that India's space policy now has commercial and strategic aspects too. In this regard, while India does not have a well-articulated, military spaceprogramme, she does have assets in

space with direct, military or dual-use relevance. Investments have been made from a military perspective in remote sensing, communication and navigation satellites. From a militaristic perspective, India's space capabilities could be termed as 'rudimentary plus'. The space architecture, so should be structured with Space Command and Space Force to cater for the need to have a distinction while looking at space from the perspective of deterrence and that of a force multiplier.Thus, the Space Command can look at the use of satellites as a force multiplier while the Space Force would look at the deterrence value. In this regard, a model with three agencies – an agency with a civilian space-agenda, Space Command/Defence Space Agency (DSA) and Space Force could be a way forward. The role of the Indian Space Research Organisation (ISRO) should remain intact and it should continue to do its job, while investing further in technology development, especially in the area of launch vehicles. The other agencies being recommended, should plug-in as per the requirements. The safety of space assets is the job of the military as a net security guarantor aiming for full spectrum dominance. Thus, there is a paramount need for India to be proactive in developing an 'Indian Space Defence Force' which is in line with its future requirements and stated policies.

AI and Robotics –From Concept to Delivery. Modern logic or inferencing is a better means of disrupting the loop in battles compared to computational power and the human prefrontal cortex (PFC) plays a pivotal role in inductive reasoning and drawing inferences. However, humans are being rapidly replaced by AI due to sight and processing-related limitations, lack of pure logic in decision-making and it not being humanly possible to process information in an efficient time-bound manner. In the context of network-centric warfare, real-time situational awareness gets undermined because of the cyber constraints, thus the need of the hour is to make autonomous systems which cannot be penetrated, since even having a link could lead to hacking. It is also becoming rather simple to weaponisethe existing, autonomous drones and as such, one has to be prepared for Lethal Autonomous Weapons System (LAWS). There are myriad ways in which drones could be used today and swarm bots are becoming increasingly popular for a plethora of reasons including the fact that defensive measures against swarm attacks cannot be carried out manually and one needs to install autonomous systems. Cyber attacks today have moved from hacking to farming. If a nation is using hardware, software and even networks which are not indigenous, it is susceptible to this technique and is in a very precarious situation. In the Armed Forces, there is a need to have specialist officers, with experience across various platforms and with vertical and horizontal growth, thus ensuring optimal delivery in this field. While people may be averse to using robots, they could assist in the tactical, strategic, as well as the civilian space by eliminating the need for avionics, crew safety, logistics etc. Not only can robots be replenished, but they are also economical and the law regarding them is at present vague too. While adequate caution needs to be exercised with regard to the use of robots and LAWS, they have become a necessity. There is an emergence of a new AI-enabled species and a pure PFC, unlike the human brain which has the emotional part in addition, which will help find the best solutions to most of the problems, including the military ones.

Transformation in the Battlespaces

Warfare before the 21stcentury, was intimately linked to statecraft, with an identified adversary and quantified threat, while the 21st century battlefield is multi-domain with shades of grey. Technology will dominate the multi-domain battlespace, however there is unlikely to

be a linear extension of the present trends, keeping in mind the disruptive technologies that are being pursued with great focus. Precision-fire at longer ranges and pinpoint targeting are replacing massed attacks and firepower, respectively and the manifestation of kinetic war has and would undergo profound changes. The future battlespace for network-centric warfare will be defined by inter-connected physical, informational and cognitive battlespaces. In the aerospace dimension, AI-based technology will dominate the battlespace, with a combination of optionally-manned aircraft operating along with autonomous drones and swarms. Keeping the centrality of the human dimension in modern conflicts, there is a need to develop military leaders with the skills, vision, steadfastness and comprehensive understanding of the challenges that modern warfare would present, as also, the endurance, strength of character and mental resilience to meet the conditions that modern warfare would impose.

A New Strategy for the Changing Era. While the contours of the change in the character of warfare are broadly understood, the difficulty lies in the army's ability to adapt to that change in terms of organisational structures, thought processes and doctrines. Some aspects impacting the changing character of warfare in future will include the ' man-machine interfaces' and the position of the human with regard to the decision loop and the fact that war will no more be restricted to soldiers alone, with the actions of the military becoming very transparent. In addition, use of cyber and networks including data, both military & personal and prosecution of Hybrid Warfare through a combination of economics, politics, diplomacy, military, state, non-state actors and so forth, will also impact the change. In preparing for future conflicts, one needs to plan for the war one would be forced to fight and not which one wishes to fight; the latter is based on one's own capabilities, weapon systems and doctrines. The salience of doctrine, when planning for operations, should not be pushed in the background due to the lure of technology, since merely relying on technology without organisational structures, concepts and a doctrine never works. Another aspect that needs to be deliberated is the issue of 'integrated low-cost systems versus a monolithic, complex platform' as well as an urgent requirement for integrating numerous small systems. Information War has become a game changer and it is not only the non-state actors, but the states too who are engaging in propaganda and fake news. Wars are fought on Facebook and Twitter and victory is defined by who gets more 'likes'. When engaged in real war, it will become difficult to match the illusion that one has created in the virtual space with what is happening on ground. There is also a lack of joint functioning in the cyberspace with different arms looking at different aspects thus maybe necessitating the requirement of a Cyber Corps. The training methodologies, standards and systems need to be in congruence with the requirements of the future battlefields, thus the need and methodology to invest in the military human-capital should be dictated by the importance of understanding the wars one will get engaged in.

The Impact of Long - Range Vectors & Precisionary. The destructive nature of war has not changed and as such, if non-kinetic operations do not enable one to deliver kinetic effects, one will not remain competitive. Some trends in technology that are going to re-shape how fires are delivered are range, automated fusion, multi-sensor active-seeker munitions and defensive measures. In the next decade, the range of artillery could double across most systems, however, beyond the range of 40 km, these systems will need precision munitions. Automated fusion i.e. fusing of information from multiple sensor-streams will occur, thereby reducing the human burden of analysis. Modern defensive measures like highenergy lasers,

Ballistic Missile Defence (BMD) system and high frequency microwaves will quantumly increase the potency of the defensive measures. If we look at the high economic aspects of engaging the adversary with precision munitions, then relevance of conventional fires and the fact that without a significant conventional-fires capability, one can simply be overwhelmed, is clearly brought out. A target can be engaged with massed conventional artillery when it is manoeuvring upto 40 km, beyond which artillery systems, having a total range of 70 Km, will require precision munitions. Thus, there would be a stretch of 30 km, where one will have significant levels of precision to engage the target, but only a limited stockpile of them. Hence, the challenge for the force is in crossing that 30 km gap and getting into the 40 km conventional space without being decisively engaged and losing the critical enablers. At the operational level, there are large depots and concentration of munitions and material and these create fixed points to defend or 'defensive nodes', whilst also fixing most of one's available defensive capabilities. These nodes however cannot be targeted by the adversary without risking the exhaustion of the limited stockpile of precision munitions. The primary task at the onset of hostilities will not necessarily be heavy contact between manoeuvre elements; rather, pushing into the 30 km space with relatively small force-packages and recce forces, UAVs and potentially autonomous systems, essentially trying to map out the enemy's Center screen for their 'reconnaissance-strike complex' and then to start causing attrition to them. Additionally, hypersonics make all of one's critical nodes vulnerable and the speed at which it comes, gives the target no reaction-time. Given that the entire battlefield is held at risk, the art in beating the threat of hypersonic weapons would lie in how to operate in a way that does not present the adversary with opportunities that it cannot resist.

Special Forces - A Force Multiplier for Land Operations. As an outfit, the Special forces (SF) is sophisticated, highly trained, motivated and capable of operating in all terrains and weather conditions using unconventional tactics, techniques and modes of employment. The SF is an operational force multiplier with an ability to engage in significant deep operations in the operational framework and engage in decisive engagements in adverse conditions to change the tide of war. The battlefield is becoming increasingly information-dense and technologically driven tending to non-contact battles, which has necessitated organisational and doctrinal changes in the SF. In the Sri Lankan context, the necessity for the Sri Lankan Army to re-organise and re-structure occurred in response to the then principal terrorist threat–the Liberation Tigers of Tamil Eelam (LTTE) and led to the raising of Sri Lanka's SF. In response to the increased threat by LTTE, Sri Lankan military experts decided to maximise the use of small team operations leading to the formation of Long-Range Patrol (LRP) teams in the mid 1990s to neutralise targets of strategic nature. Two major missions conducted by the LRP teams were the neutralisation of Shankar – LTTE's second-most-important leader and in-charge of LTTE's air-wing and neutralisation of the LTTE air threat. The physical use of SF even in the contemporary, digitised battlefield, can have strategic impact like in the missions to neutralise Osama bin Laden and Abu Bakr al-Baghdadi. Operating in a technologically driven battlespace has put tremendous pressure on maintaining operational secrecy, which is the core value of SF operations. Besides, technological advancement of the adversary hinders the effective employment of SF. The vulnerabilities have to be addressed with doctrinal changes and increased utilisation of technology. Some of these will include keeping abreast with the latest developments in their fields and situational awareness, integration with horizontal and vertical stake holders, ensuring friendly access to the Electro-Magnetic spectrum while denying it to the adversary, focusing the capability development of

small groups on technology, as well as revising communication and other technical equipment to be above the standards of the adversary and modernising the weapons and ammunition used by the SF. All these should be incorporated when modifying the operational philosophy. The SF will thus be equally relevant in the technologically advanced, digitized battlefield conditions and will be a force multiplier for any theatre commander in the present and future battlefields.

The Nuclear Environment to Include the Impact of Hypersonics. Asia is the most nuclearised zone in the world, with seven nuclear powers in the vicinity, namely, India, China, Pakistan, Russia, Israel, North Korea and also the US owing to its extended responsibilities. As far as the US goes, the majority of its present infrastructure is over 40 years old which has necessitated modernisation. It has already modernised the command-and-control systems, infrastructure, launch systems, warheads and the weapons have grown from first generation to fourth generation, making them more accurate and at least three to five times more potent. The US in its Nuclear Posture Review (NPR) of 2018, has added a clause regarding the necessity of having a flexible-response capability i.e. low-yield nuclear weapons and it has been put into effect as per open sources. Russia developed a triad by the 1960s and modernisation had been going on at a very fast pace. While the hypersonic glide vehicle (HGV) has been inducted into the Russian nuclear forces in very small numbers, nuclear-powered underwater drones and nuclear-powered cruise missiles are under development. A situation of mutual vulnerability has been created, with the Russians and the Chinese feeling that the US has a better BMD-capability and the US feeling that those countries have a system (HGV and Multiple Independent Targetable Re-entry Vehicles) which can penetrate it. This mutual vulnerability has infact led to strategic balance. China has concentrated both on conventional as well as nuclear strengths, developing missiles and possibly has the HGV capability too. China's White Paper clearly states that they have a policy of 'No First Use', however, the problem is that China's ballistic missiles are for dual-use and there is a threat of miscalculation. In the India-Pakistan context, the two, essential differences between the nuclear weapons of India and Pakistan, firstly is that while India's nuclear weapons were meant to deter any country from using nuclear weapons against her. Pakistan's were purely anti-India. Secondly, while India's nuclear programme was more-or-less indigenous; the Pakistani nuclear arsenal has been developed as a result of a 'beg-borrow-steal programme'. India, at the moment, has the military capability and a strong political will, both of which add to credible deterrence against any country. Overall, as long as mutual vulnerability stays, no one is likely to use nuclear weapons as everyone realises its dire consequences.

Hybrid/ Sub-Conventional Warfare

Hybrid war has emerged as the cardinal challenge for the immediate future. Conceptually, it is premised on avoiding the strength of the adversary and striking the weakness. Deterioration of the social fabric of the country also provides a fertile ground for the prosecution of hybrid war. Collaboration between agencies in a hybrid warfare environment and communication especially leveraging social media, are both of utmost importance. The preparedness for hybrid warfare is a national effort which cannot be left to Army Commander's Special Financial Powers fund alone. The world is witnessing a new age driven by AI, nanotechnology, quantum sciences & genetic engineering and characterised by individuals

with augmented capabilities – or the 'Cyborg' era. This will have an impact on the competition for influence and power i.e. politics.

Operations in a Grey Zone Environment. War has many definitions and military doctrines all around the world are designed to respond to these definitions, but modern combat goes beyond the sensationalism of hi-tech weaponry which shadowed the broader concepts of social, political and cultural issues. The emergence of grey zone warfare, which seeks to bridge the chasm between war and peace or between routine statecraft and an all-out war, can be attributed to breakdown of national institutions, exacerbated by social media and resurgence of revisionist states using methods beyond the realm of conventional war. In order to develop response-options, there is a need to distinguish between wars that use force and those which do not. In this regard, hybrid war is not synonymous with grey zone war. The principal difference between hybrid warfare and grey zone warfare is that conventional operations necessarily constituted a part of the former and not of the latter; however, grey zone conflicts could escalate to a conventional war is a separate issue. Grey zone is a concept of gaining strategic advantage over an adversary with a breadth of operation that could only be limited by imagination. Some basic characteristics of grey zone warfare are its non-military nature, protracted emergence using proxies, non-attributability, use of legal and political justifications etc. To effectively respond to grey zone operations, it is essential to first identify the ambit of grey zone operations, which is not easy as operations could constantly be scaled up, scaled down, stopped, re-started and new elements added. Subsequently, proportional, commensurate, timely and limited-natured responses must be crafted to the adversary's grey zone operations. The strategy against grey zone operations must be based on the understanding of the essentially opportunistic, gap-seeking character of grey zone operations. In this regard, aspects of transparency, deterrence, political and bureaucratic adaptation and resilience of civil societies assume importance. While militaries have kept upgrading their conventional preparedness, these may be of only limited use in a grey zone conflict, thus it is time to prepare for the more probable and frequent conflicts – those in the grey zone.

Technology and Urban Warfare. By 2030, two-third of the world population is expected to be living in cities. Conflicts to will become more urbanised and technology will play a major role. The two main challenges to the conduct of military operations in urban areas is understanding the urban environment, as also being aware of how to operate in the same. South Asia, as a region, is multi-ethnic, multi-religious, multi-lingual and full of complexities. It is a fragile region due to political instability, corruption and poor governance, as also, being home to more than 22 UN-designated terrorist entities. Meanwhile, the geo-political realities of South Asia are changing and aiding this shift are the changing geography, new regional structures and power rivalry. Geography in the region is changing, with mountains which were barriers flattening, so as to speak, with strategic communication networks being constructed and thus there is connectivity not just in the physical sense, but also in terms of ideas, values, culture and technology. The old, regional structure is changing, with the growing Chinese interest in South Asia and its attempts to access the Indian Ocean. In addition, the menace of terrorism in the region is increasing and there is a need for a collective, South Asian resolve to fight it. Finding the technological safeguards to the potential threat of terrorists using technology in the urban environment in India and the rest of South Asia will be a real strategic challenge and vulnerability in the years to come.

Terrorists, in fact, use the internet for a variety of purposes including fundraising, operational planning & propaganda and the techniques used by terrorists are becoming more and more sophisticated. This includes the use of more advanced communication systems, drones and smart gadgets. The region offers unprecedented opportunities for security-related cooperation, however there is a need for a core, strategic, geo-political mechanism to formulate reliable, intelligence-based assessments and forecasts for South Asia.

Rise of Non-State Actors. The LeT is the most-favoured terrorist group of the Pakistani State and the group formed a part of the Order of Battle for the Pakistan Army as it is different from every other militant or terrorist organisation on Pakistan's pay-roll. The LeT is at odds with Deobandi organisations who are the largest cluster of terrorists in Pakistan. The difference between LeT and the Deobandis is that the LeT has hierarchical structures that reflect the State's relationship with them, while the Deobandi groups have a very flat organisational structure and operate like a network-of-networks. In addition, the Deobandis are inherently sectarian and these groups were joining the IS to kill Shias and Alawites even before the Caliphate was declared. The LeT is anti-sectarian and anti-communal while operating inside Pakistan, firmly opposing the Deobandis' practice of declaring Muslims takfir and thereafter, Wajib-ul-qatl. The LeT has two missions – da'wah (proselytism) and jihad and the former was crucial to the domestic politics of this organisation. In India, while jihad may be the priority, in Pakistan it is da'wah and the selected recruits are used to tap into the rest of the family for support. The motivation to join the LeT, can be visualised as a three-dimensional space where one dimension was geography because the angle of the Partition was brought in, the other was personal aspiration and finally there was devotion. Mothers have a very important role and there is a different kind of motherhood that is being promoted. Persuading the mother is pivotal to the recruitment process and the LeT is putting in a lot of effort into cultivating mothers. The LeT today, is ripe for leadership-decapitation and there is also a possibility that the JeM would probably replace the LeT in the operations for the time being, given Pakistan's own efforts to defeat the Pakistani Taliban, as also, the peace deal in Afghanistan. Finally, sub-conventional deterrence is very important to Pakistan despite its Army and the nuclear deterrence, thus India also needs to start talking about sub conventional deterrence and not limit its options to conventional deterrence.

The Salience of Technology and Social Media in Hybrid Operations. 'Unrestricted warfare' is a term which may be more suitable than hybrid or grey zone warfare to describe what is happening today. While grey zone and hybrid warfare seem to suggest a beginning and an end, unrestricted warfare suggests no limits of morality, scruple, value, or on instrumentalities that may be employed. It looks at indeterminate timeframes, omnipresent battlefields and blurring of distinction between the civilian and the war-fighter. When we talk of terrorism and social media, the assessments are largely hysterical, lacking sobriety, information and understanding. There is a need to distinguish between the message and the medium and it is the message which is the most powerful component, along with the social and the political contexts which also play key roles. The importance of social media is often exaggerated because it is not understood properly and it presents as much an opportunity for the adversary as for the defender. Terrorists use the social media to propagate their cause by twisting news, however fake news is not a crisis of social media it is just being carried by social media and there is a comprehensive, enveloping ecosystem of political falsification that adds fuel to fire. Given the scale of social media, controlling it might look daunting at

first sight, especially if our response mechanisms remain primitive. However, control is already being exerted by the social media platforms themselves. Monitoring of the digital presence of terrorist groups can actually prove to be a force multiplier for the states and research organisations. There is a need to understand the nature of the content and narrow the gap between the pace of technological transformation and one's reactions. This has to begin at the level of policy, which is most difficult, since adaptations by professional organisations cannot occur overnight. There is a need to change the reaction-time and adopt a governancemodel where individuals are given responsibilities as per their core competencies, only then can we rise up to combat the menace of terror on social media in a systematic manner and exploit it to our advantage.

Major Takeaways

Doctrinal Issues. The conclave witnessed discussion on a number of doctrinal issues and some of the major ones are listed below:-

- An understanding and acceptance of the technological potential of the time and its application in warfare including its impact on doctrines is the cornestone to achieve a consequential transformation in the armed forces. Changes in organisation and operational concepts will facilitate this transformation.

- The very character of warfare is changing, especially with the non-kinetic forms coming of age and being effectively used to achieve political aims of a country. However, while warfare has evolved over time, the mindset of the Armed Forces and the States has remained the same and needs to change.

- The concept of 'total security' needs to be adopted in response to the contemporary security challenges.

- The current environment requires full spectrum integration across all domains of warfighting.

- Victory requires the defeat of not just the opponent's military capabilities, but also the successful resolution of the deeper problems which lie at the root of the conflict.

- Given the blurring of lines between war and peace, there could be no single, universally-accepted concept of victory and thus in the current day and age, there was no decisive and enduring victory; and each form of warfare may have a different concept of 'success'.

- The focus on human capital must not be diluted.

- The set of natural resources critical to strategic industries would change in the Fourth Industrial Revolution, while their use as a geo-economic tool would continue.

- Employment of a Tactical Nuclear Weapon (TNW) cannot be restricted to a 'limited' nuclear war. A limited nuclear war would escalate very quickly into a strategic nuclear exchange.

- Grey zone operations are not a purely military affair, rather a national and institutional challenge. The tendency of the military to keep all types of warfare under its purview has led to grey zone operations being given a military hue and being seen as 'warfare'.

- The principal difference between hybrid warfare and grey zone warfare is that conventional operations necessarily constitute a part of hybrid warfare.

- The strategy against grey zone operations should be based on transparency, deterrence, political and bureaucratic adaptation and building the resilience of the civil society. The Armed Forces should shift major focus to the sub-threshold space, regain and seize the initiative in that domain.

- In an era where grey zone environment is going to be the norm, especially in the context of India, it is imperative that it starts talking about sub-conventional deterrence and not limit its options to nuclear and conventional deterrence.

- While technology is driving the change in the character of warfare, the lure of technology should not push doctrine into the background.

Structural Issues. Some key structural issues deliberated during the conclave are as under:-

- India needs a well-articulated Military Space Programme to exploit space as an enabler for operations, with space-based communication and navigation being central to warfare in future. It should be proactive in developing an 'Indian Space Defence Force'. A model with three agencies – an agency with a civilian space-agenda, Space Command/Defence Space Agency (DSA) and Space Force could be the way forward.

- The security challenges presented by the Information Age in multi-domain operations, weaponised social media and cultural engagements have become an important component of cyber operations. Information manoeuvre will require specialists, manpower and tailor-made organisations.

- A nation using hardware, software and even networks which are not indigenous is susceptible to cyber attacks and thus building in-house capabilities is absolutely essential.

- While India understands the importance of data and networks, all its capital is directed towards platform-upgrades. Collecting, collating, storage and security of data as a strategic weapon will need an integrated approach.

- AI & robotics including swarm technology will be a game changer in future conflicts. Development of systems, employment doctrines and counter measures for and against autonomous weapon platforms and directed energy weapons will enable the Armed Forces to equip, train and fight differently.

- In order to embrace the technological challenges and optimise the way of functioning, the Armed Forces must have specialist officers with experience across various platforms and the vertical and horizontal growth to be able to deliver optimally.

- The battlefield has become increasingly information-dense and technologically driven. To ensure that the SF retains its role as a force multiplier, organisational and doctrinal changes in the SF are necessitated.

- Given the economic cost of precision munitions, conventional fires would remain relevant and must be catered for.

- While the preparedness for hybrid warfare is a national effort, within the Armed Forces, the capital, concepts, organisations and training should serve the purpose of combating hybrid warfare.

Strategies. Some of the strategies necessitated due to the impact of the changing character of warfare are as under:-

- The ease of accessibility of dual-use technologies by non-state actors has raised their capacity of causing destruction. In addition to the military/kinetic response, an understanding of the factors driving such groups or individuals and radicalisation is essential to mitigate their influence. An engagement and shaping of the social environment will produce exponential results in countering such threats.

- The first strike in a high-intensity conflict, would probably not be opening up with conventional artillery on the front, but a hypersonics-threat which would come with virtually no warning and potentially knock out one's higher echelon capabilities.

- The primary task at the onset of hostilities would not necessarily be heavy contact between manoeuvre elements; rather with relatively small force-packages and recce forces, trying to map out the enemy's Centre screen for their 'reconnaissance-strike complex' and subsequently start attriting those centres.

- The role of non-state actors and proxies in intra-state conflicts is likely to see an upsurge with a lower probability of conventional conflicts. The indirect approach in dealing with these changes could be extremely effective, as propounded by ancient thinkers such as Sun Tzu and Kautilya.

- Hybrid players will exploit the urban battlegrounds, to inflict high casualties and prohibitive collateral damage; technology needs to be leveraged to effectively minimise these.

- One needs to keep pace with the speed of change occurring, especially in technology, impacting warfighting and unless we keep pace with the speed of change, we will lose the ability to compete.

- The gap in capability competence and imagination while tackling the menace of online radicalisation needs to be addressed. We need to understand the nature and characteristics of the terrorist discourse on social media and then devise the tools for intervention.

- The strategy against grey zone operations must be based on the understanding of the essentially opportunistic, gap-seeking character of grey zone operations and a

proportional, commensurate, timely and limited-natured responses must be crafted to the adversary's grey zone operations.

- AI could be used to generate advance-warning data based on social media activity of terrorists, thus using their digital footprint to harness data, collect intelligence on them, intervene, misdirect or contain responses.

- Deception is extremely important in Information Manoeuvre and warfighting and while focus is on denying the information environment to the adversaries, there is also advantage in leaving small channels open, for when they communicate, multiple dilemmas could be fed to them.

- Develop an entirely different and elevated set of attributes and skill sets to operate in the sub-conventional space.

Conclusion

The seminar clearly highlighted the fact that there is an urgent need for change of the strategic mindset, to adapt to the changing conceptual, structural and cultural military needs and sensibilities, as also adjust to the skill and speed at which the transition is being made. Given the increase in multi-domain operations, doctrines need to keep pace with technological changes. Evolutionary changes are now resetting the rules that Land Operations will be structured by, all driven by a 'military-technical revolution', bringing unprecedented firepower, depth and transparency to the battlefield.

DETAILED REPORT

DETAILED REPORT

The aspects enumerated as part of this report are based on the deliberations by the panellists. These do not necessarily conform to the views of the Centre for Land Warfare Studies (CLAWS) or that of the Indian Army or the Ministry of Defence, Government of India.

'Pragyan Conclave' – The international seminar of the Indian Army and CLAWS was conducted on March 04-05, 2020, on the topic '*Changing Characteristics of Land Warfare and its Impact on the Military*' at the Ashoka Hall, Manekshaw Centre, Delhi Cantonment.

Objectives

The objective of the seminar was to:-

- Scan and evaluate the current and emerging trends in warfare, developing conflict-spectrum and future battlefields.
- Provide an insight into the changing contours of warfare and its influence on land warfare.
- Explore and understand the technological advancements shaping the future battlefields.
- Assess the embryonic influence of the third dimension, hypersonic, precision long-range missiles and state-of-the-art unmanned aerial vehicles (UAVs) on land warfare.
- Construct conventional operations under the backdrop of nuclear weapons in future land battles.
- Evaluate the dynamics of hybrid warfare and challenges posed to future battlefields by non-state actors exploiting technology and social media.

Modalities of Conduct

The two-day seminar was conducted at the Ashoka Hall, Manekshaw Centre, Delhi Cantonment on 04 &05 Mar 2020. The participants, both Indian and foreign, were from the armed forces (including Defence Attachés), strategic community, observers from friendly foreign countries, veterans, academia and students. Nominated Indian Army officers from field formations also participated in the seminar.

Guest Speakers

Shri Shripad Yesso Naik	Hon'ble Raksha Rajya Mantri
Gen Manoj Mukund Naravane, PVSM, AVSM, SM, VSM, ADC	Chief of the Army Staff & Patron CLAWS
Lt Gen SK Saini, PVSM, AVSM, YSM,VSM, ADC	Vice Chief of the Army Staff & Chairman, Board of Governors, CLAWS

Chairpersons

Session I	Lt Gen (Dr.) VK Ahluwalia PVSM, AVSM**, YSM, VSM (Retd)	Director, Centre for Land Warfare Studies (CLAWS), New Delhi
Session II	Lt Gen (Dr.) Rajesh Pant, PVSM, AVSM, VSM (Retd)	National Cyber Security Coordinator, Government of India
Session III	Lt Gen AK Singh, PVSM, AVSM, SM, VSM (Retd)	Distinguished Fellow, Centre for Land Warfare Studies (CLAWS), New Delhi
Session IV	Lt Gen Subrata Saha, PVSM, UYSM, YSM, VSM** (Retd)	Member, National Security Advisory Board

Speakers

- Lt Gen Raj Shukla, YSM, SM, Director General, Perspective Planning, Indian Army.
- Mr Lazar Berman, Fellow, Jerusalem Institute for Strategy and Security, Israel.
- Maj Gen AKM Abdullahil Baquee, RCDS, ndu, PSC, Bangladesh Army.
- Brig Simon Goldstein, MBE, ADC, Deputy Commander Reserves, 6th United Kingdom Division.
- Col John Kendall, Deputy Commander,1 ISR Brigade, British Army.
- Ms Sharon Weinberger, Global Fellow, Woodrow Wilson International Centre for Scholars, United States.
- Gp Capt Ajey Bishwanath Lele (Retd), Senior Fellow, Manohar Parrikar Institute for Defence Studies and Analyses, India.
- Lt Col PJ Anand Kumar (Retd), Chief Technology Officer, Data Val Analytics Pvt. Ltd., India.
- Lt Gen D S Hooda, PVSM, UYSM, AVSM, VSM** (Retd), Board Member, Cyber Peace Foundation, India.
- Dr. Jack Watling, Research Fellow, Royal United Services Institute, United Kingdom.
- Brig H P Ranasinghe, RWP, RSP, ndc, Director of Operations, Sri Lanka Army HQ.
- Lt Gen Amit Sharma, PVSM, AVSM, VSM (Retd), Scientific Consultant (Strategic Issues), Office of the Principal Scientific Advisor to the Government of India.
- Lt Gen (Dr.) Rakesh Sharma, PVSM, UYSM, AVSM, VSM (Retd), Distinguished Fellow, Centre for Land Warfare Studies, India.
- Maj Gen Binoj Basnyat (Retd), Independent Political and Security Analyst, Nepal.
- Dr. C Christine Fair, Provost's Distinguished Associate Professor, Georgetown University, United States.
- Dr. Ajai Sahni, Executive Director, Institute for Conflict Management, India.

INAUGURAL SESSION

INAUGURAL SESSION

Keynote Address by the Hon'ble Raksha Rajya Mantri

Shri Shripad Yesso Naik
Hon'ble Raksha Rajya Mantri

Delivering the Keynote Address, the Hon'ble Raksha Rajya Mantri (RRM)-Shri Shripad Yesso Naik, underscored the need for taking a wide-angled view of the changed dynamics that necessitates a comprehensive transformation of the Indian Armed Forces and the wider defence eco-system in India, in order to be future battle ready.

Elaborating on how the appointment of the Chief of Defence Staff (CDS) and the setting up of the Department of Military Affairs (DMA) were seminal and transformative, the RRM mentioned that the CDS is mandated to structure the programme of change and transformation, to meet India's security needs. The CDS and the DMA will thus help forge future-ready forces by working on doctrinal collaboration, budgetary prioritisation, force-development, establishment of new operational structures like theatres & functional commands and so forth. The RRM further added that the DefExpo-2020 held at Lucknow was demonstrative of the resolve to establish a Defence Corridor to attract global talent related to defence.

Talking about novel disruptions in the battlespaces, the RRM mentioned how the changing nature of economics and evolution of technology impact the character of war and the type of conflict. The RRM said that as old rivalries playout in new theatres such as cyber, robotics and artificial intelligence (AI), one needs to reform one's beliefs, doctrines, objectives and strategies. It is imperative for India to define her aims and her instruments for the changing world and that impacts traditional organisations like the military. In this regard, the RRM raised a crucial query of how armies should re-tool and re-structure for modern combat, given that information is the new centre of gravity and data as a critical raw material and a new strategic resource.

Touching upon the 'sub-threshold space' or the 'grey zone', including political warfare, the RRM highlighted the significance of agile, mobile and technology-driven forces. He

questioned the rationale behind keeping massive funds locked up in large inventories and underscored the need for a ‘restructured, ready-to-wage military instrument’. Elaborating on how the digital battlespace was re-defining the traditional boundaries, the RRM brought out the need for incorporating the power of digital network and space assets into the armed forces and also the complete metamorphosis of the nation’s security horizon, outlook and responsibility. He stressed on the need to create networks that were seamless and integrated across agencies & forces and the need to protect them, for they will be the first target of the adversaries.

Drawing an analogy between cement in the Industrial Age and rare-earth elements in the Digital Age, the RRM brought out how the challenges of the digital world would extend to the industrial ecosystem and why it was important to develop capacities in that critical domain. We, thus, need to put all our creative energies together to make a roadmap for the future, which could be facilitated by this seminar.

The RRM concluded by stating that he looked forward to hearing the issues that confront armies across the domains of warfighting and ways of securing competitive advantage in the digital world.

Inaugural Address by the Chief of the Army Staff & Patron, CLAWS

Gen Manoj Mukund Naravane, PVSM, AVSM, SM, VSM, ADC
Chief of the Army Staff

The Chief of the Army Staff (COAS) - Gen Manoj Mukund Naravane, PVSM, AVSM, SM, VSM, ADC - giving ample examples, lucidly brought out how successive technological revolutions are occurring at smaller intervals. Underscoring the need for armies to be agile in thought and fleet-footed in action, he mentioned how modern technology had paved the way for multi-functional devices and how dual-use technologies are changing the character of warfare. Distinguishing the 'nature' of war from the 'character' of war, the COAS opined that while the nature, in terms of the 'victor imposing his will on the vanquished', the organised violence, the blood & gore, is constant and unchanging; the character keeps on evolving and changing with respect to how wars are fought in terms of weapons, technology and strategic context. Technologies such as AI-driven targeting, automation and intelligence, surveillance, reconnaissance (ISR) will impact the character of war, while the unchanging nature of force and violence will manifest in newer forms. The COAS emphatically stated that hard power will always remain relevant and will have to be leveraged in accordance with the changing strategic context. Underscoring the need for the Armed Forces to keep pace or stay ahead of change, the COAS mentioned that warfare evolves faster than war-fighters do, but the Armed Forces, being conservative by nature, prepare not only for the last war, but very often, for the wrong war.

Giving the example of how icons of the battlefield of the 20th century i.e. the main battle tank, the large surface combatant and the modern aircraft have become relatively less significant and are on their way out, the COAS elaborated on how war had evolved over time and we had to keep pace with the change. Wars are a social construct and an interaction between political communities. In the olden days, war had a clear end-state and they were tools to settle ideological disputes decisively and were won in clearly defined and demarcated military and political arenas. To prove this point, the COAS highlighted how the military victory of Babur in the First Battle of Panipat resulted in land gains for him and the establishment of the Mughal empire, the military victory of the Allied Powers in World War II established the supremacy of Anglo-American democracy over Nazism and that of the US in the Cold War marked the triumph of western-liberal democracy over Soviet-era

communism. These stand in stark contrast to recent conflicts, whereby compartmentalised military endeavours, which did not address the political questions, had resulted in the fatigue of endless wars. Big budgets, cutting-edge technology and spectacular military campaigns notwithstanding, the Taliban and Al-Qaeda, though 'vanquished', emerged in time and space in other avatars –the Islamic State (IS) and other motley groups. The COAS underlined that the notion of 'victory' and 'defeat' had become turbid, as wars no longer have a clear end-state.

Detailing the changing role of armoured formations, the COAS mentioned that, during the 1973 Arab-Israeli War, two armoured formations of the two armies manoeuvred against each other supported by artillery and air forces. This was in contrast to recent times, whether in Iraq, Lebanon, Georgia, Chechnya or Syria, where armoured formations had either followed or supported the application of airpower and artillery; if not, their units and sub-units had been committed in smaller tactical groupings as part of infantry armoured assaults in urban terrain. Questioning the notion of 'victory' in the context of urban warfare, the COAS made a mention of the Battle of Zelenopillya (2014), in which the Russian artillery destroyed two mechanised formations in a few minutes. In 1999-2000, in Chechnya, the Russians lost 122 of the 146 platforms, tanks or infantry combat vehicles to tank ambushes due to the sheer intensity of urban warfare. He further remarked that since 1994, 78 per cent of tank-casualties occurred in urban warfare or built-up areas. Elaborating further on the notion of victory, the COAS brought out how 'victory' is still defined using the logic of World War II. He emphasised the need for a clear distinction between the 'political aim' i.e. the end-state and the 'military aim' (the means to achieve that end-state). 'Victory' no longer rests on the ability to inflict massive destruction, but on the ability to wrest popular support from one's opponents. The COAS defined 'victory' as an outcome or descriptive statement of the post-war situation, or as an aspiration driven to accomplish specific objectives through the use of force. The rise of non-state actors and transnational criminal networks has not only necessitated a nuanced approach to achieving 'victory', but also fuelled the postulate of a narrowing space for all-out conflicts. The COAS remarked that while massive, World War II-type wars were a thing of the past, the world would continue to smolder in numerous conflicts of a smaller scale but greater intensity.

Elaborating on how geo-strategic realities and spaces are being altered without altering the state of peace, the COAS remarked that the Clauzewitzian way of war, dedicated to hardcore kinetic wars, had given way to Sun Tzu's way of war encompassing tenets of 'winning without fighting', victory without bloodshed, to name but a few. This Chinese way of war, as per the COAS, had given a new lease of life to the concepts of non-contact warfare or grey zone warfare, wherein one sheds the binary nature of war and ambiguity and careful risk escalation becomes the key. Giving the examples of China's dominance over South China Sea, the attacks by Houthi rebels on the Riyadh airport and the oil facilities in Saudi Arabia and the 2019 Balakot airstrikes carried out by India, he underscored the importance of ambiguity and careful risk-escalation in grey zone warfare. Talking about how these incidents witnessed short and intense escalatory-cycles in full media glare with the accompanying war of narratives, the COAS underscored how the Balakot airstrikes falsified the traditionally-held belief that crossing the International Border (IB) would lead to a full-fledged war. If the game was played with skill, military ascendancy could be established with cycles that do not necessarily lead to a full-scale war, he remarked.

Elaborating on Kautilya's *Arthashastra*, the COAS mentioned that ancient Indian strategic thought could be used to create contemporary templates for modern, geo-political competition. Predicated on the sheer majesty of power and guile, the Kautilyan view in strategic policy espouses an outward orientation, a calibrated power projection and influence as against a passive, defensive crouch. The COAS opined that the security challenges in the current, multi-polar world were no different from those which vexed the Mauryan Empire in 300 Before Common Era (BCE) and as such, *Arthashastra* could become a touchstone for the foreign and strategic policy-makers to devise a distinctively Indian view of international relations and statecraft. In fact, an analysis of most insurgencies in the world shows that Kautilya was accurate in his belief that the greatest cause of insurgencies was societal discontent. The COAS also made a mention of Kautilyansutra underlining the four forms of strategic means against the enemy diplomacy *(upayas) – sama* (conciliation), *dama* (gifts), *danda* (coercion) and *bheda* (influencing the mind). He further explained how Kautilya employed secret services to achieve a threefold purpose – keeping the ruler informed of the developments within and outside the empire, conducting covert operations aimed at undermining both internal & external enemies and maintaining internal discipline and loyalty of the bureaucracy and the military.

Examining how technology was impacting the battlespace, the COAS underscored how combat had become multi-domain and that doctrines needed to keep pace with technological changes. He further talked on the informational and cognitive aspect of combat and deterrence, bringing out how China, despite not being involved in hardcore combat for a few decades, had created an aura of being the undisputed military leader in key technological domains by regular showcasing of its military might. Citing the example of Gulf War II, where 85 per cent of the Iraqi mechanised forces were destroyed as a result of the precision in American air and artillery assaults before the former could even move. The COAS brought out how technology and technology-enabled attributes like ISR were severely challenging, if not eclipsing, the traditional metrics of firepower and manoeuvre. In fact, during the said war, only 50 out of the 10,000 Iraqi artillery pieces survived the preparatory air and artillery assault. Discussing how technological superiority is impacting the military balance, the COAS explained how low-technology adversaries were responding to it by weaponising the mundane. Commercial airliners, roadside bombs, suicide vests, cheap drones off the net, social media platforms and so forth are easy to obtain and difficult to defeat. Giving the examples of IS, an organisation steeped in 17thcentury fundamentalist outlook, which leveraged social media and digital technologies better than 21st century militaries like the US or the UK and the drone and cruise missile strikes on the Saudi oil facilities in Abqaiq and Khurais, he emphatically stated that the current era is an era of technological equivalence, wherein, while the strong embrace cutting-edge technologies, the weak have technological options of their own.

Shifting focus to how the Indian Army is dealing with the changing character of war, the COAS listed out the following:-

- ***Kinetic and Non-Kinetic Responses in the Grey Zone***. Even as the Indian Army strengthens its conventional prowess, plans and capacities are being built focusing on dynamic responses and actions below the threshold of an all-out war, both along the western and northern borders.

- ***'IBG-isation'***. To achieve operational objectives in diverse terrains, lean, agile and tailor-made structures called integrated battle groups (IBGs) have been created.

- ***Enhancement of Jointmanship and Integration***. The creation of DMA and the post of CDS will give a fillip to jointmanship and integration. Given the budgetary constraints, the right balance needs to be struck in the investments in continental, maritime, aerospace and other emerging domains.

- ***Focus on Technology***. There is great emphasis on innovation wherein low hanging technologies are being inducted into our units and formations. The military leveraging of emerging disruptive domains especially capacities in space, cyber and electronic warfare (EW) are being given a boost. Blockchain technologies, lasers and directed energy weapons are being looked at for possible military use.

The COAS concluded by stating that even as traditional capacities were being fortified, a long-term view of the changes in the character of war was being taken. The Indian Army was determined to stay abreast and ahead of the change and also lead and shape the future battlespaces.

Presentation of Awards by the COAS to the Winners of 'Field Marshal Manekshaw Essay Writing Competition on National Security'

Award Winners and Proud Parents with the COAS, VCOAS, DG PP and Director, CLAWS

With an aim to promote strategic culture amongst the youth of the country, CLAWS conducts an annual, essay writing competition in the memory of the first Indian Army officer to be promoted to the rank of Field Marshal and COAS during the 1971 Bangladesh Liberation War – Field Marshal Sam Hormusji Framji Jamshedji Manekshaw. This competition gives a platform to young minds to present their ideas on emerging security challenges and encourages students to write about their views on national security.

This year marked the second year of the competition and it saw 94 entries not only from the top universities of India, but also from abroad including the Oxford University, the London School of Economics and the University of Bonn. Entries were sought from University students in two categories – 'Manekshaw Paper' with a limit of 8,000-10,000 words and 'Issue Brief' with a limit of 4,000-5,000 words.

This year, the best essay entries will be published by CLAWS in the form of a book "National Security Challenges: Young Scholars Perspective' and the Indian Army will present a copy of the book to all the Universities in India. The following six are the winners

for the year 2019-2020 in the two categories and they were felicitated by the COAS:-

Category	I Prize		II Prize		III Prize	
	Name & University	**Topic**	**Name & University**	**Topic**	**Name & University**	**Topic**
Manekshaw Paper	Poornima B, Manipal University, Karnataka	Emerging Cyber Threats to India's Nuclear Facilities: Ramifications & Mitigation Strategies	Siddhant Tomar, ICFAI University, Dehradun	India's Cultural Identity Under Siege: Threat to National Security	Shishir Rao, Manipal University, Karnataka	Understanding India's Responses to its National Security Challenges through Four Realist Perspectives
Issue Brief	Priyanka Patel, Central University of Gujarat	India's National Security Strategy: An Idea Whose Time has come	Avishkar Pamnani, Manipal University, Karnataka	Neutralising Pakistan's Nuclear Capability by 1000 Mouse clicks	Rayan V Bhagwagar, OP Jindal Global University, Sonipat	Blitzkrieg: Relevance in the 21st Century

DAY - I

SESSION I: EVOLVING WARFARE – AN INSIGHT INTO THE CHANGING REALM

SESSION II: TECHNOLOGICAL REVOLUTION – A SEMINAL CHANGE

SESSION I: EVOLVING WARFARE – AN INSIGHT INTO THE CHANGING REALM

Opening Remarks by the Chairperson

Lt Gen (Dr.) VK Ahluwalia, PVSM, AVSM, YSM, VSM (Retd)**
Director, CLAWS

Highlighting the focus of the Session, the Chairperson –Lt Gen (Dr.) VK Ahluwalia, PVSM, AVSM**, YSM, VSM, (Retd), mentioned three aspects that needed to be brought out with regard to warfare – ongoing trends, plausible future conflicts and the rationale for evolution.

Sean McFate in his book, *The New Rules of War: Victory in the Age of Durable Disorder*, lucidly puts forth that despite having the best of troops, resources and technology, the West, especially the US, lost wars because of the way it thought – a '1945 mindset of fighting conventional wars'. Thus, there is a need to change the mindset, especially given the emergence of grey zone, hybrid and urban warfare – since the warfare, as expected, has been evolving, however the mindset has remained the same.

If we examine two sets of wars, one hundred and fifty years apart i.e. the Franco-Prussian War of 1870 and the major wars of the 20th and the 21st centuries, some interesting facts emerge. Three reasons behind the victory of the German States led by the Kingdom of Prussia in 1870 were as under:–

- ***Mobilisation**:* They mobilised their forces by all available means, in the quickest time frame.

- ***Artillery fire**:* The accurate and quick artillery fire caused devastation.

- ***Will**:* They decided to carry out several offensive actions to bring a decisive end to the war.

In context of the above, we must reflect on the probability of a total war, a total mobilisation and the will to bring the war to a decisive end, in today's environment.

On examining the conflicts of the past three decades, right from the First Gulf War to the most recent battles of Aleppo, Mosul and Raqqa, in context of their objectives, the methods adopted (in terms of military, economic, political, technological, informational, etc.), the multiple stakeholders and the multi-dimensional consequences of the wars, certain lessons have been learnt and changes brought in. We should thus try to ascertain what are the changes experienced in terms of doctrine, strategy, warfighting concepts and organisational structures, in these conflicts. An example of organisational changes is what the US and China have undertaken. In the wake of the Vietnam War and the Iran hostage crisis (1979-80), the US took the decision to organise their forces into theatrised commands and it took them six years to bring in this concept. China, after evaluating the Gulf Wars and the Kosovo Conflict, brought in the integrated theatrised commands in early 2016.

There are rapid geo-political, economic and social changes taking place in the world with technology playing a major role in warfare in the wake of the Fourth Industrial Revolution and the fusion of technologies. While Clausewitz attributed the change in the character of conflict to three factors, namely–capabilities, circumstances (geo-politics) and motives, the competition and confrontation between Nation States vis-à-vis the fast-diminishing natural resources, is the crucial, fourth factor. This is leading to world disorder with the world today being more volatile, uncertain, complex and ambiguous, due to the rise of China, resurgence of Russia, the instability in the Middle East and North Africa, the situation in Sub-Saharan Africa, an unstable Asia/Indo-Pacific, vulnerable sea lanes of communications, the global war on terrorism, insurgencies, civil wars, militarisation of space, militarisation of the Indian Ocean and so forth.

Post World War II, there has been a progressive increase in intra-state conflicts. In fact, post1980, the world witnessed the golden period of insurgencies, as also, terrorism. These were purely because of religious, sectarian, ethnic and identity-driven alienation, as also, socio-economic exclusion, huge youth-population, unemployment and non-responsive governments. All these have a relation with the ongoing conflicts the world over.

India has, in fact, been living in a grey zone environment for the past thirty one years, owing to proxy war cum state-sponsored terrorism from Pakistan – a situation termed by the Indian Army as 'No War, No Peace (NWNP),' at the Indo-Pak border. The 2019 Abqaiq-Khurais attacks in Saudi Arabia and the killing of Lt Gen Qasem Soleimani reflect a shift in the security paradigm and India should be prepared for non-contact warfare (NCW), as also, urban warfare.

The world has moved from foot soldiers to elevated platforms, network-centric platforms, further to knowledge-based warfare and eventually now to NCW. In the book, – *Unrestricted Warfare*, written by two senior colonels of China's People's Liberation Army, it says that "in the present time, the battlefield is everywhere" and thus we need to be always prepared.

Sub-Theme 1: Military Futures - Prospects and Possibilities

Lt Gen Raj Shukla, YSM, SM
Director General, Perspective Planning, Indian Army

Putting forth his views on the topic, the speaker-Lt Gen Raj Shukla, YSM, SM –emphatically stated that military future is entirely imaginable, if not completely predictable. In this regard, he gave the example of the US Army officer-Maj Gen William Lendrum Mitchell (Billy Mitchell)–for his prescient words espousing the cause of airpower at sea. He was charged with insubordination, suspended from the army without pay for five years for suggesting that an airplane could sink a battleship, that aircraft carriers should replace battleships, highlighting the vulnerability of the US' Pacific fleet at O'ahu, predicting that the next war for the US would be with Japan and that it would be initiated by a surprise Japanese air-attack. Thus in 1924-25, more than a decade before the 1941 Pearl Harbour Attack, Maj Gen Mitchell outlined with telling precision, the entire anatomy of one of the most seminal battles of World War II.

Militaries, the world over, are perhaps faced with a 'Billy Mitchell moment', especially the traditional, western-style militaries as their mindset is crucibled in distinct thresholds of war and peace. The adversaries, both state and non-state, have exploited this oversimplified conceptual and legal framework of war and peace by waging a battle in the virgin terrain – that of the sub-threshold space. The strategic stakes are high in this terrain and this space was also witnessing great power or state-on-state competition. Maj Gen Soleimani was a great practitioner in the sub-threshold space, giving him an iconic status and Iran, Russia, Israel, Syria, Turkey and China are some of the countries optimally utilising this space. Some of the tools available in this space are weaponised information, fakery, destabilisation, diplomacy, use of proxies, mercenaries and infra-aggression. Infact, a section of US' Defense Advanced Research Projects Agency (DARPA) is working on differentiating fakery from reality and there is a grim possibility of deep fakes being on YouTube by 2022.There is thus, an urgent need for change of the strategic mindset, to adapt to the changing conceptual, structural and cultural military needs and sensibilities, as also adjusting to the skill and speed at which the transition is being made.

In today's 'Information Age conquests', military vile & guile and not brute force, can be used to secure competitive advantage. China has effectively used this and acquired more territory in South China Sea than perhaps what the East India Company held at the peak of its power. Change in Russia's messaging strategy in Europe is another example of its effective use. In 1981, to keep the Western powers at bay, Leonid Brezhnev resorted to a huge show of force by conducting the largest ever military exercise to be carried out by the Soviet Union – Exercise Zapad-81. This is in stark contrast to 2016, when Putin did not message through munitions and firepower, instead chose to weaponise refugees to keep North Atlantic Treaty Organisation (NATO) off its periphery. By bombing Syria, Russia created a migrant crisis for Europe which led to anti-establishment protests and entry of IS terrorists into Europe. There was a general sense of a weakened and destabilised Europe, marked by the undermining of the position of somebody as politically well-ensconced as Chancellor Angela Merkel of Germany. In fact, this indirect approach characterised by strategic subversion and tactical deniability reaped richer dividends for Russia.

Employment of contractors or high-end mercenaries in 'contract warfare' saw the Wagner group (a mercenary force loyal to Moscow) carrying out attacks against the US military outpost at the Conoco gas plant in Deir ez-Zor province, Syria, demonstrating sophisticated military prowess against the elite forces of the US – the Delta Force, the Army Rangers and so forth. The use of contract warfare, thus is increasing, as is evident in Yemen, Nigeria, Ukraine, Syria, Iraq and the Kurd territory. The salience of contractors, who have no national loyalties and are highly trained, thus outclassing the local military, is rapidly increasing in grey zone conflicts.

In light of the above, traditional militaries needed to take the following, three steps –

- ***Doctrinally Need to Shift Major Focus to the Sub-Threshold Space, Regain and Seize the Initiative in that Domain***. There is a need to be more Kautilyan and Sun Tzu-ish as opposed to Clausewitzian in today's time with a need to embrace 'total security' in response to the total war that is being waged in the sub-threshold space. There has to be an aggregation of the entire gamut of military capacities across domains, cleverly fused with other levers of the State - intelligence, diplomacy, information, social media, covert capacities and so forth.

- ***Shed Over Structuring and Processing and Focus On Outcomes***. We need to demonstrate agility, focus less on structures and more on final outcomes. We need to be much more innovative and unconventional.

- ***Develop an Entirely Different and Elevated Set of Attributes and Skill sets to Operate in the Sub-Conventional Space***. While jointness was good enough to meet the needs of the Industrial Age, the Digital Age requires full spectrum integration of the three traditional domains- land, sea and air as well as space and cyber capabilities. India has just begun the journey to build joint capacities in the three traditional domains with the CDS and the prospective theatre commands. It is pertinent to note that, it is full spectrum integration and not jointness, that will help in undertaking seamless planning and effects across all

domains at a pace and tempo that will outstrip the adversaries. Regular forces, Cyber, Space and Special Forces will need to operate and, if necessary, fight together, while skilfully integrating disruptive technologies. The UK is showing the way in this issue, with raising of the Strategic Command which is mandated with ensuring the transitioning of the British Armed Forces from an Industrial Age 'joint force' to the Information Age 'integrated force'.

As we know that the conflict has expanded into new domains, we must develop expertise in the new domains if we need to outstrip our adversaries. This expertise needs to be developed at the speed of 'Cyber' and not at the Industrial Age speed, if we need to remain relevant. We need to organise and equip ourselves to fight in these new domains and, while, some small steps have been taken, we have a long way to travel. A few exceptions like China, USA and Israel aside, most countries are not equipped to fight in the cyber and space domains. While information is recognized as the new centre of gravity and data as a vital strategic resource, investments are still being made in platform-upgrades and brick-and-mortar capacities. It is required that one values networks and data as much as ammunition. Digitalisation of all of India's platforms, while imperative, is a challenge given the fact that the US took six years just to capture and cleanse data.

Hardly any of the great military innovations of the past century were direct outcomes of a military requirement, but were infact spinoffs of commercial opportunities and successes. Thus, acquiring and inducting the capabilities and technologies that the digital forces of tomorrow will need, requires deepening the engagement with the private sector as the latter is the natural hub of innovation and technology. In this context, there is a need for the following:-

- Models that encourage and share risks.
- Recruitment from a more diversified skill set while placing a huge premium on talent.
- Change in procurement norms, especially excessive reliance on specifications/General Staff Qualitative Requirements.
- Flexible, integrated career structures blending civil and military talents.

Additionally, in many domains, such as IT, space, etc. the armed forces are fishing in the same talent-pool as their civilian counterparts and as such, need to be agile and competitive in recruiting. There will be a need to create integrated career structures, blending the civil and the military. Given the example of China's near monopoly over rare-earth elements required in the manufacture of electronic devices and advanced weapon systems, there is a need for re-visiting and re-evaluating the wider eco-system needed in the Digital Era.

While there are growing demands in maritime, aerospace and other emerging domains, due to India's budgetary constraints and the issue of live and active unsettled borders, 'continentality' will continue to prevail over India's national security outlook. In addition, in order to embrace sunrise technologies, one must simultaneously identify and retire legacy

sunset capacities. The Fourth Industrial Revolution (4IR) demands comprehensive transformation - in concept and outlook, structure and culture and from mere jointness to full spectrum integration.

Sub-Theme 2: Changing Character of Conflict – Imperatives of Transformation

Mr Lazar Berman
Fellow, Jerusalem Institute for Strategy and Security, Israel

Stating right at the outset that there is no real transformation sans change in organisational and operational concepts, the speaker, Mr Lazar Berman, highlighted the importance of transformation in not just technology, but organisation and operational concepts as well. Military transformation can be defined as a major innovation or series of innovations in which new organisational frameworks and operating concepts, usually based on new weapons, drastically change the way war is fought. Not all transformation is positive or necessary and if one is relevant to the threats one is facing, transformation may not be required since it is risky and expensive. Large organisations, such as the military, dealing with much smaller, armed actors can learn a lesson from how small electric mills replaced established, bulky, integrated steel mills in the US, thus bringing out the need for transformation when there is a competition and the risk of becoming less relevant.

Knowing when to transform, is one of the biggest challenges in the transformation process. Initially, concept and reality are nearly the same and there is no need to transform. However, the relevance-gap i.e. the gap between concept and reality, increases as time and environment change, exacerbated by a denial to acknowledge this gap, till there is a major surprise/loss/incident that brings out the need for transformation. In addition, when the adversary catches up with the military revolutions, it also necessitates a new revolution.

A historical perspective of military revolutions, lists out the following:-

- ***Revolution 1: Strategic Mobility***. This era lasted till World War I, characterised by steel, early electricity, mass armies and the creation of massive headquarters to manage all this. All the major actors becoming excellent industrial armies warranted a change.

- ***Revolution 2: Tactical Mobility***. This era was characterised by exploitation of the internal combustion engine, transistor radio and electricity. Ideas such as strategic bombing and blitzkrieg were based on platforms – tanks, planes, etc. that focused on the operational level of war. The human casualty that this type of war inflicted on the militaries made the US and the NATO look at neutralising platforms, thereby bringing in the next change.

- ***Revolution 3: Information Technology (IT)***. This is the present era characterised by the use of microprocessors, personal computers and internet which has made platforms much more vulnerable. Not only have state-actors, such as Russia and China, taken advantage of the IT revolution, non-state actors have also exploited the same in terms of developing precision fires and drones to direct those fires. This has necessitated another revolution with militaries focusing on emerging, civilian technologies such as AI, robotics, big data and so forth. This revolution has come at a cost to land warfare with most of the bigger budgets and cutting-edge technology going to the air force and intelligence.

The Israel Defense Forces (IDF) was part of a first-rate Revolution 2 (tactical mobility) relevant in 1956 and 1967 operations. While that sufficed when the IDF faced the Egyptian tanks and planes in 1973, the non-platform threats in terms of Sagger and surface-to-air missiles, restricted Israeli manoeuvre and Israel paid the price for not transforming while its adversaries did. This led to Israel developing its own Revolution in Military Affairs resulting in decisive Israeli victory during 'Operation Mole Cricket 19'. However, this led to bulk of the budget and technology going to the Air Force and the ISR capabilities and not to ground forces, which ultimately affected IDF's ground manoeuvre. Operation Grapes of Wrath, saw no manoeuvres at all, 'Operation Defensive Shield' being an exception while the Lebanon War of 2006 witnessed halting manoeuvres at the end that didn't accomplish much. As far as the Gaza campaigns were concerned, there were some manoeuvres, but only after a long campaign of air bombing. During 'Operation Change of Direction'in 2011, the adversary, despite not being able to destroy a lot of tanks and planes, was able to stop tanks and the biggest air assault in Israeli history at the very end of the war. Thus, the present military concept based on expensive platforms without ground manoeuvre requires a change.

The present day relevance-gap is a strategic challenge since Israel's enemies have been able to take advantage of the proliferation of new technologies and have transformed from terrorist organisations to basically near-peer adversaries with the ability to carry out their own anti-access/area denial (A2/AD). In this regard, the adversaries are talking about limited offensives into Israel while denying access to IDF into their territory, giving the adversaries enough time to strike the Israeli home front. These adversaries are the ones which disappear

on the battlefield, see the enemy before being seen and do not stop, but wear down manoeuvre and inflict a high price. Thus, the transformation in the IDF, based on Revolution 3 is stuck with the relevance gap having increased. As far as transformation in the IDF is concerned, bringing tactical mobility back to the land battlefield is pivotal; and better access to technology and greater ability to develop weapon-systems based on it, works in IDF's favourvis-à-visnon state actors.

While the services in the IDF were generally good at innovating against challenges that were service-specific, it was usually much harder when the problem fell between the services. Israel has learnt that at the joint level, the General Staff is not effective enough in leading transformation. Consequently, Israel's present Chief of General Staff was trying to strengthen the joint level with new organisations that will be able to manage innovation and transformation that fall between the services. In the IDF, ex-Air Force personnel were leading a lot of these organisations, in light of which, one needed to introspect if the military was still relevant against the threats and whether old concepts were just being stretched to solve new problems without new concepts actually being generated. Real change can come only when change in organisation occurs. The ability of a military to meaningfully change is intimately connected to its ability to understand the broad technological potentials of the time and through their application, understand warfare in a new way.

Sub-Theme 3: Trends in Warfare - Concept of Victoryand Strategic Conquest

Maj Gen AKM Abdullahil Baquee, RCDS, ndu, PSC (Retd)
Bangladesh Army

Defining war as a social construct to unleash violence, the speaker– Maj Gen AKM Abdullahil Baquee, RCDS, ndu, PSC–characterised such violence as direct, intentional, organised, sanctioned, regulated and sometimes, ritualised. Why one fights is a matter of debate with theories ranging from the genetically driven to the socially created ones. Patterns, purposes and end-states of conflicts have varied throughout the ages.

To recap the trends in warfare, one could talk of them since the 'Hundred Years War' which is often called the dawn of modern warfare. This was the pre-Industrial Age era and it

witnessed the manifestation of national identity and loyalty to the Nation State. The trends in warfare from the Industrial Age to the current time are as listed below:-

- ***The Industrial Age****:* The advent of refined weaponry and technology gave rise to new tactics in warfare, such as infantry groupings and mixed order formation employed by Napoleon. With naval shells being introduced and more emphasis being placed on heavy artillery offence from behind the troop line formations, this period witnessed the rapid decline of the cavalry as seen in the Crimean War (1853). The Russo-Turkish War (1877-78) witnessed the introduction of loaded rifles equipped with repeating fire-rounds, taking another step forward in weapon modernisation.

- ***World War I****:* While this war saw the tedious trench warfare, German biplanes brought in the third dimension as well.

- ***World War II****:* This war witnessed not only a full-blown armoured sweep with synergistic air-support, but also the use of nuclear bombs.

- ***Cold War****:* This period was spent under the 'Damocles sword' of a nuclear war between the two super powers. With the invention of rockets and developments such as the launching of satellites into the outer space and landing on moon, the US and the then Soviet Union started vying for supremacy in the new domain –the outer space.

- ***Network-Centric Warfare****:* Post the invention of computers and internet, the cyber domain has become the latest domain for future battles. During the Gulf War in 1991 and the wars against the former Yugoslavia, the Taliban regime in Afghanistan and Iraq, the US demonstrated its unchallenged ability to conduct devastating, large-scale, precision-guided missile and bomb strikes. Network-centric operations were a result of improvements in miniaturisation and data handling capacity of digital information systems throughout the 1990s.

Current developments impacting warfare consist of robots, drones, directed energy weapons, genetically engineered clones, nanotechnology. The future of warfare looks increasingly autonomous with aircrafts, warships and armoured vehicles that operate without human crews and robots taking over from fallible human beings with networks that link surveillance, acquisition and target engagement. In such an environment, computer scientists might become soldiers.

This notwithstanding, in Somalia, Rwanda, Zaire, Congo, Liberia and Sierra Leone, a high-intensity, low-technology warfare, is still the dominant kind of warfare. The weapon-of-choice for insurgents tends to be the standard trio of AK-47s, RPG-7s and mortars, in addition to roadside improvised explosive devices (IEDs) as seen in Iraq, where 70 per cent of US casualties have been due to IEDs. While high-tech sensors, communication systems, as well as precision bombing can play a useful role in conventional warfare, it cannot substitute for the large numbers of relatively low-tech light infantry soldiers.

Today, irregular fighters are exploiting the technologies of the Information Age. The Al-Qaeda has created its own form of sophisticated network warfare, maintaining affiliate cells

in over forty countries in addition to exploiting the internet for facilitating financial transfers, recruiting & training fighters as also passing encrypted instructions and intelligence.

The collapse of central governments and the splintering of states along ethnic, religious or tribal lines has stimulated the trend of ethnic and/or religious communities being targeted in campaigns of terror. Most contemporary war zones are populated by disparate groups of irregular fighters with different objectives and motivations. The insurgency in Iraq, for example, includes Sunni and Shiite militias, Al-Qaeda jihadists and criminal gangs. In Sub-Saharan Africa, the conflicts resemble large-scale turf-wars between rival criminal gangs and bear little resemblance to the popular image of warfare, while in Colombia, Marxist-Leninist insurgents have joined forces with major narcotics-trafficking gangs. Urban terrorism rather than rural-based insurgency is now the dominant form of irregular warfare and it is reflective of not just the accelerating global urbanisation, but the contemporary terrorists' desire to cause the maximum number of civilian casualties.

The Fourth Industrial Revolution will have a major impact on international security with the new modes of artifacts of industrial production changing demand patterns, empowering countries controlling supply and transit and disempowering others. While the set of natural resources critical to strategic industries would change, their use as a geo-economic tool would be repeated. The haves and have-nots of the nuclear weapons club became a major determinant of the post-war global order in the 20th century and it continues to be relevant even today. The importance of technology can be borne out by the fact that the gap in military capability which separated the US from others in the world helped it in sustaining its leadership of a unipolar world.

Though emerging technologies may grab headlines, the greatest impact of AI on conflict may be socially mediated. Algorithmically driven, social media connections funnel individuals into transnational, but culturally enclosed echo-chambers, radicalising their world-view.

Victory should be considered within the context of the political aim and war & victory are about statecraft, rather than only hostilities. Clausewitzian understanding of military victory looks at it as a condition where the enemy's ability to enter battle and resist or resume hostilities is destroyed. Some may consider the notion of 'victory' as laying down of arms or replacement of the political system of the other side with that of the victor's choosing. However, while it is believed that the Allies won in World War I, accompanied with the signing of the Treaty of Versailles and the other side lay down its arms, twenty years on, the same enemy re-emerged with similar ambitions, leading the world into a costlier war. In that context, it becomes hard to justify World War I as a victory for the Allies. During the Cold War, the realisation emerged that the concept of victory no longer had any practical significance in the context of nuclear weapons. No victory would be worth the price. This, despite World War II being seen as the epitome of a clear, grand and strategic victory that restructured the world order.

The complexities of defining victory in counter-insurgency warfare get compounded due to the non-state composition of the adversary and the difficulty in using metrics to indicate progress towards a stated goal in such an environment. As has clearly been seen by the American experience in Iraq and Afghanistan, strategic success cannot be achieved by military force alone and victory requires the defeat of not just the opponent's military

capabilities, but also the successful resolution of the deeper problems at the root of the conflict. In the end like most thinkers have philosophised “there are no victors in war”.

Session I : Chair and Panellists

SESSION II: TECHNOLOGICAL REVOLUTION – A SEMINAL CHANGE

Opening Remarks by the Chairperson

Lt Gen (Dr.) Rajesh Pant, PVSM, AVSM, VSM (Retd)
National Cyber Security Coordinator, Government of India

The Chairperson– Lt Gen (Dr.) Rajesh Pant, PVSM, AVSM, VSM (Retd)- gave a global perspective of the challenges associated with the cyber world. The world is witnessing a high intensity of information and cyber warfare due to the following four faultlines:–

- ***Applicability of International Laws***. The talks at the 6th United Nations Group of Governmental Experts have collapsed due to differing ideas regarding the governance of cyberspace. There are two clear lobbies– one consisting of Russia, China, Mexico, and Cuba and the other consisting of Western Europe and the US. Hitherto, there was an understanding that international laws, such as the International Humanitarian Law (IHL), applied to cyberspace, but Russia recently disapproved of it stating that IHL applied to conflict situations, while cyber war was prosecuted during peace time. In addition,11 norms of responsible state behaviour in cyberspace are idealistic and non-binding.

- ***Governance of Cyberspace***. Control over root servers translates into control over information and intelligence, and out of the total 13 root servers, 11 were in US, one in Europe and another in Japan. While the US, understandably, is comfortable with the status quo, the other side is not, raising the demand for UN-led, multi-stakeholder, multi-lateral internet governance.

- ***Non-Attributability***. Cyber attacks are carried out using hired servers, virtual private networks, dark net, etc. thus traceability of the attacks is a major challenge and what is seen on the global cyber attack maps in any of the national-level Security Operations Centres or Network Operations Centres is misleading. For example, while the National

Informatics Centre displays information that shows that 40 per cent of the attacks come from the US, the reality is not so.

- ***Definition of Cyber War***. Frameworks such as the Budapest Convention, the Tallinn Manual, the Paris Call for Trust and Security in Cyberspace, the Prague Proposals, etc. notwithstanding, there is no understanding on the minimum threshold of when an act will qualify as cyber war. Besides, there is no clarity or consensus on the definitions of cybercrime, cyber weapons, etc.

What makes 'cyber deterrence' very difficult is the fact that it requires 'persistent presence' in the cyber domain of the adversary, where one may have to go through six of the eight stages of an attack, just to show what one can do. This is unlike 'nuclear deterrence' that involves power projection by demonstrating one's capability within one's own national boundary. With a million attacks per month, India is the second most-attacked country in the world, as far as cyber attacks are concerned.

Sub-Theme 4: Salience of Information Warfare inMulti-Domain Operations

Brig Simon Goldstein, MBE, ADC
Deputy Commander Reserves, 6th UK Division

Col John Kendall
Deputy Commander
1 ISR Brigade, British Army

The speaker– Brig Simon Goldstein, MBE, ADC –gave a historical perspective of the 6th (United Kingdom) Division, which prepares the army's Information Manoeuvre and Unconventional Warfare forces and explained its structure and concepts of functioning. Col John Kendall, his co-speaker in the second half, covered how these concepts were operationalised.

The Division has five subordinate brigades and is persistently engaged worldwide and also retains the contingent capability to integrate with UK's high readiness force for any eventuality, from disaster relief to warfighting. Increasing number of domains, the ability to conduct cross-domain operations and the proliferation of technology and communications has brought in radical changes that provided both threats and opportunities. High-powered lasers, attack satellites, debris clouds and weaponisation of social media and cultural engagement, has brought out the criticality of space, cyber and human domains. However, the lack of

coordination and interaction between the services has been a major inhibitor to progress and such 'single-service stove-pipes' have been open invitations to the adversaries.

An adversary will seek to halt the opponents' manoeuvre by fracturing their synchronisation, to break apart inter-domain cohesion, as also, the cohesion within the opponents' country to undermine support for any war or operation they are in. Multi-domain operations address this by seamlessly and concurrently integrating effects across multiple domains and creating multiple dilemmas for the adversary. Through multi-domain operations, the adversary could be overwhelmed by acting faster, deceiving, disrupting and dominating the narrative. In such a competitive environment there is a need to break out of stovepipes and properly network, *inter alia*, sensors, since the windows of advantage will be short. It also requires maintaining an information advantage over the adversary.

While hard power remains relevant, the ability to use the information domain to disrupt, attack the homeland and undermine social cohesion has made information warfare a vital facet of constant competition and warfare. This was evident not only in UK and US' doctrines, but also in Russia's Primakov and Gerasimov doctrines.

The key aspects of Information Warfare in the UK are as under :–

- ***Joint Action***. A Ministry of Defence joint doctrinal concept that orchestrates military capabilities and activities, both kinetic and non-kinetic, to affect an actor's understanding, capability and cohesion between them, to achieve influence and output.

- ***Information Superiority***. This seeks to gain competitive advantage through continuous, directed and adaptive employment of relevant information, principles, capabilities and behaviours.

- ***Information Advantage***. Information superiority results in information advantage – a credible benefit gained through the continuous, adaptive, decisive and resilient employment of information and information systems.

Information Warfare is not only offensive and there is also a need to defend one's narrative, both within the armed forces and amongst the citizens, as also, collect, analyse and exploit both the information environment and one's data whilst protecting it from the adversary. In this regard, the 6th Division has a concept of 'Information Manoeuvre', which, at its heart, is about fusing and synchronising multiple information-centric capabilities in one Division under one command. These capabilities are drawn principally from the ISR brigade, influence specialists in 77th brigade and the two Signal brigades which protect and exploit own data. Information Manoeuvre delivers improved understanding, enhanced methods of communication, more nuanced and innovative ways to influence target audiences and protects UK's people, equipment, infrastructure and data. Information Manoeuvre allowed the UK to generate options to mitigate risk and seize opportunities in the era of constant competition.

While hard power remains relevant and is an instrument of military power that sits with the rest of the national instruments, Information Warfare (IW) has been embedded in everything we do. IW is critical for retaining the legitimacy and narrative dominance in warfighting.

The conduct of unconventional operations against state adversaries and violent, extremist organisations employs 12 effects in Information Manoeuvre – Find, Fix, Understand, Communicate, Persuade, Protect, Partner, Deceive, Disorientate, Frustrate, Undermine and Discredit. The adversary is found and fixed, both physically and cognitively, based on thorough understanding of the human terrain. This ensures that when they communicate, they conduct outreach which is effective not just in working with neutral groups and the host nations, but also in undermining and discrediting the adversaries. The activity may be virtual (through IT systems and communication networks) or directly cognitive or could be also physical, involving killing. It is also simultaneously needed, to protect oneself, one's information networks and those of one's allies. All this will frustrate the enemy and disorientate his/her command and control systems. The situation will then present multiple dilemmas to the adversary's commanders which may force them to take decisions favourable to the opponent. Operations and support provided differ based on whether the situation is below or above the threshold of conflict.

Below the Threshold of Conflict

The aim of preventing the adversary from dominating the perceptual landscape and gaining operational surprise in the grey zone is achieved by persistent, worldwide engagement, both physical and cyber, through collecting intelligence and challenging the adversary's incremental gains in the physical, virtual and cognitive spaces. To achieve this, the 6th Division seeks to understand :–

- The enemy commander's intentions at the strategic, operational and tactical levels.
- The threats the adversary can present.
- The opportunities available, based on the knowledge of the adversary's strengths and weaknesses.

Enemy propaganda and covert operations are exposed and technical intelligence is gained to build the battle picture further. This is then followed by shaping the environment for offensive information operations.

Offensive information operations involve not just getting one's narrative across, but also pursuing key, high-value targets in the enemy's command, shattering their principles and the coherence of their conversations. While this could be enhanced through the means of cyber and electronic warfare, UK also works with host nations by advising, assisting and accompanying them on operations. This helps in extending UK's reach, builds the sophistication of UK's sense &warn systems and contributes to UK's understanding of the world. Such partnerships not only frustrate the enemy's propaganda narrative, but also deny them the opportunity to seize ground. Winning the physical battle aside, it is important to win the battle of narratives too.

Since every task is different, the team deployed for unconventional operations is different too, ranging from as few as 12 to as large as 200. The intelligence picture is created pre-deployment by harnessing all government intelligence, surveillance and collection assets, ranging from space to cultural awareness.

The physical and/or virtual access into the adversary's home base or contested area and technical information pertaining to weapons, explosives, etc. are exploited by the force. However, the importance of reconnaissance troops in terms of identifying key human, economic and physical terrains and conducting military capacity building remains undiminished.

There is a need to preserve the freedom of operations and offset multiple dilemmas and it is imperative to have the right people in the team, ranging from cultural property protection teams to critical national infrastructure advisors looking at power, water, fuel supply, cyber protection, etc.

Above the Threshold of Conflict

The Divisional Information Manoeuvre Group (DIMG) is expected to be deployed in such a scenario and it delivers stand-off decision-advantage to the commander. It counters threat by looking at how the adversary is gathering intelligence and uses cyber and electromagnetic activity, influence operations, networks and multi-domain ISR. This is enhanced by a reach-back deep into the UK, to the specialist Reserve Officers.

The battle-winning advantage of the DIMG is gained by leveraging all multi-domain assets. In this regard, the Information Manoeuvre personnel ranges from academics to specialists on cultures. The DIMG operates as a part of the fighting Division Headquarters with staff integrated throughout the division. The staff of the DIMG is quitt strong, with upto 2000 people deployed on ground. The concept of Information Manoeuvre has been tested in US exercises against a free thinking enemy and has been found to give the corps commander a disruptive edge. Some of the major learning points which have emerged are as under :–

- The preparation for battle needs to start years in advance.
- Information Manoeuvre not only supports troops on ground but is sometimes supported by the troops classically in deception.
- Electronic warfare is still a battle-winner since cyber cannot be used against everything and there has to be a mix of capabilities.
- It is required to be competitive and ensure everything is done at the speed of relevance.

While Information Manoeuvre and warfighting tend to focus on denying the information environment to the adversaries, there is also advantage in leaving small channels open, for when they communicate, multiple dilemmas could be fed to them. Deception is extremely important in these operations and if one breaks into the adversary's system, it is better to plant false intelligence reports or deepfake videos of the enemy commander pronouncing surrender, rather than shutting it down. UK believes that IW is an absolutely critical factor of multi-domain operations and its doctrine of Information Manoeuvre implemented through the 6^{th} Division provides it with great advantage.

Sub-Theme 5: Cyber as a Tool of Warfare - Paradigm Shift

Ms Sharon Weinberger
Global Fellow, Woodrow Wilson International Centre for Scholars, United States

The speaker– Ms Sharon Weinberger– began by giving a historical US perspective of computer networks, beginning with its origin under the visionary guidance of JCR Licklider, in the early 1960s. In this regard, she made a mention of the Advanced Research Projects Agency's (ARPA's) use of the Semi-Automatic Ground Environment computer system, that was designed to link 23 air defence sites to coordinate tracking of Soviet bombers in case of an attack on the US and of the Pentagon's 'command and control' programme. While cyber warfare is a commonly used term, 'computer networks' instead of 'cyber' may be a more apt word when referring to their role in warfare and the experiences discussed in the following paragraphs, bring out the various ways in which computer networks have got incorporated into warfare.

- ***The Vietnam Experience***. Vietnam War has been the first demonstration of 'network-centric warfare' and a computer network combined with air and land operations. The US adapted the nascent science of computer networking to fight the Viet Cong insurgents. The US Air Force dropped strings of acoustic sensors along the weapons-smuggling route from North Vietnam to South Vietnam – the Ho Chi Minh Trail and these sensors detected passing convoys and relayed the data to a pair of IBM mainframe computers in Thailand, which in turn directed helicopter gunships and aircraft to the predicted coordinates. Rather than dropping bombs on something they had seen, pilots were, for the first time, attacking based on computer-derived targets, ushering in the era of Push-Button Warfare. Post the war the US realised that while they were fighting insurgents in Vietnam for ten years, the Soviet Union had invested in modernisation. Consequently, the Pentagon decided to take the sensors and networking capabilities developed for counter-insurgency and apply them to land warfare and specifically against, the Soviet conventional advantage in Europe. One of the concepts that came out of this was that of the 'Assault Breaker', which further gave rise to the concept of Joint Surveillance and Target Attack Radar System (JSTARS).

- ***The Kosovo Experience***. During the 1999 Kosovo Air War, the US Army approached the DARPA to find a way to deploy forces/assets faster and lighter. DARPA came up with an idea of distributing combat capabilities across the network. The Future Combat Systems, as it was called, relied on a mobile adhoc network, where the

devices would act as 'self-configuring nodes' in a network. The aim was to get the lethality and mobility of a battleship with four or five smaller platforms that could be networked together. This idea of substituting electron for armour worked fine from 1999 to 2003. Post the invasion of Iraq in 2003, where home-made bombs proved deadly to the US forces, they realised that they could never have enough information to make up for armour.

- ***The Iraq Experience***. The US battled insurgency in Iraq, using the Real-Time Regional Gateway – the National Security Agency's (NSA's) computer programme designed to pull together many feeds of information, ranging from intercepted phone call to information on bomb attacks and analyse that data to identify insurgent-networks and predict attacks in real time. During 'Operation Desert Storm,' the first JSTARS aircraft spotted a massive convoy of Iraqi vehicles fleeing Kuwait and passed the data directly to the strike aircraft. The resulting destruction of some 2000 Iraqi vehicles earned escape route the name 'highway of death'.

- ***The Afghanistan Experience***. With regard to the Afghanistan experience, the 'Nexus 7',which grew out of the Red Balloon Challenge in the US, was used. Nexus 7 was based on pooling information from social data feed, social media, cell phones that were distributed to the Afghans, price of commodities, markets, etc. and integrating them with feeds that the NSA was getting, to predict where the next IED attack would take place.

- ***The Islamic State Experience***. As far as the IS was concerned, it was an entirely different problem compared to the insurgencies in Iraq and Afghanistan. 'Operation Glowing Symphony' was the biggest cyber operation carried out by the US Cyber Command, that involved attacking the IS' information networks with malware and other tools which prevented IS members from communicating and posting propaganda. In this instance, the focus of cyber operations was not collecting information as much as countering propaganda.

An interesting analogy can be found between the period the US was engaged in Vietnam, investing in technologies for counter-insurgency and the current period where the US has spent the last 20 years building capability for network-centric operations. However, those efforts aren't what you need for what has been outlined in the most recent National Defense Strategy, which focuses on China and Russia. In fact, in a 2019 report for the Government Accountability Office, the oversight arm of Congress says, "The Army activated a cyber battalion in December 2018 and as of March 2019, this unit was understaffed by more than 80 percent."

China, Russia and Iran meanwhile have been building cyber capabilities and experimenting with different ways of operating in the cyber realm. What seems to be lacking, compared to the post-Vietnam situation, are visionaries who can think about how to take the last 20 years of cyber research that was applied to counter-insurgency and adapt it to the national security challenges the United States and its allies face today, whether in land warfare or any other area of national defence. There is thus a need to have a different viewpoint on how we use the computer network and what we are defending against, to optimise the cyber warfare capabilities.

Sub-Theme 6: Drivers Space Command to Space Force

Gp Capt Ajey Bishwanath Lele (Retd)
Senior Fellow, Manohar Parrikar Institute for Defence Studies and Analyses, India

Stating right at the outset that India lacked a Space Command, much less a Space Force, the speaker - Gp Capt Ajey Bishwanath Lele (Retd) - brought out the difference between the militarisation and weaponisation of space. Militarisation of space, is the use of satellite technology for navigation, reconnaissance, communication and various other aspects of intelligence-gathering. It is legal and not against any treaty or rule. Weaponisation, on the other hand, is using militaristic means to prevent the adversary from using his/her satellite-network, for e.g. by jamming/blasting the adversary's satellite, which is not permitted.

In terms of capabilities in space, India has no separate military architecture for space and her investments in the field are moderate. Since India does not have all the technologies relevant to space and can lift only 4 tonnes into space, the belief that India is a 'space power' may be misplaced. India at present could be considered a second-rung space power along with Israel and Japan, while the major space powers are Russia, US, China and the EU. However, India can become a 'smart (space) power' by incorporating both hard power and soft power elements into its space capabilities.

A historical perspective of India's space programme shows that its focus has been socio-economic development – something which continues till date. As far as launch vehicle systems and activities pertaining to deep space, Moon, Mars, etc. are concerned, India is doing well in those fields. The focus of the Indian space programme has never been military and the policy remains the same even today, however some mid-course correction is ensuring that India's space policy now has commercial and strategic aspects too. In this regard, while India does not have a well-articulated, military space programme, she does have assets in space with direct, military or dual-use relevance. Investments have been made from a military perspective in remote sensing, communication and navigation satellites.

With regard to where India stands in the strategic domain of space, the following points give a clearer picture:-

- There are a few systems which are for military utility and the Indian Armed Forces do receive assistance from space.

- India started with a space cell and had the ambition for a space command (three star). It now has a Defence Space Agency (two star).

- India has made major inroads into the space arena with the successful conduct of the anti-satellite (A-SAT) test.

India's military inventory, in the context of space, can be summarised as under :-

- ***Reconnaissance***

    - Remote sensing, dual-purpose satellites with sub-metre resolution.

    - Cartographic satellites. Technology Experimental satellite (TES, 2000), which are no more operational.

    - India also launched Synthetic Aperture Radar (SAR) satellites initially with Israeli help in the wake of the Mumbai attacks, but now has mastered the technology.

- ***Satellites with Military Utility***

    - GSAT-7 (Rukmini) provides real-time inputs to the Indian Navy.

    - GSAT-7 A interlinks ground radar, airbases and Airborne Warning and Control System.

    - RISAT-2A, RISAT-2B, RISAT-2 and RISAT-1.

    - Hyper-Spectral Imaging Satellite.

    - The GSAT-6 is mainly for strategic use. Geostationary satellite with S-Band antenna. Information over Indian mainland. It frees the soldier from carrying bulky communication equipment as very small handheld devices would be put in use.

- ***Navigation***
    - Indian Regional Navigation Satellite System (IRNSS/NavIC) to provide accurate position information services to civilian and military users.
    - This seven-satellite system is in place. Ground equipment is not fully operational. It is believed that the entire system will become fully operational for the armed forces and even the common man.A position accuracy of better than ten metres is expected to be provided to military users.

From a militaristic perspective, India's space capabilities could be termed as 'rudimentary plus', highlighting the need for more to be done, especially in light of significant Chinese investments in space. As far as space is concerned, India requires the following:-

- 24 satellites in low earth orbit (LEO) + 12 SAR/Earth Observation satellites in LEO for ISR.
- Constellation of 40 satellites in LEO to provide Internet to defence.
- Robust Space Situational Awareness.
- Number of communications, electronic intelligence and weather satellites.

The significance of space to militaries, due to its strategic and tactical relevance is undisputed and the first military use of satellites was for reconnaissance, however now Space-based communication and navigation technologies are central to warfare. This has led to a 'vulnerability factor' given the ever-increasing dependence of armed forces on this technology.

In India's case it faces the strategic reality of China and Pakistan being nuclear-weapon states, the nuclear triad thus assumes importance and India needs to be prepared for a 2 or 2.5 front battle. Thus, the space architecture should be structured with two separate space agencies - the Space Command and the Space Force. The rationale for having two, separate agencies–the Space Command and the Space Force– is to cater for the need to have a distinction, while looking at space from the perspective of deterrence and that of a force multiplier.

India's, close to USD 30 billion worth of space assets, needs to be protected especially since China's hypersonic missiles and anti-missiles tests are a reality and need to be catered for. Thus, space is important to the military from the perspective of conventional warfare, nuclear warfare (triad) and hybrid warfare, as also from the perspective of aid to civil authorities, disaster management and UN peacekeeping operations. But, there is a requirement to look at the investments in space from those being made to use it as a force multiplier vis-à-vis those done for deterrence value. Thus, the Space Command could look at the use of satellites as a force multiplier while the Space Force could look at the deterrence value.

The Naresh Chandra Committee's recommendation for a Space Command was given at a time when space was not being seen from the perspective of deterrence and only as a force multiplier for the three services. While, as a temporary measure the Defense Space Agency, which is a downgraded version of a Space Command, can be made responsible for space warfare, however, a separate agency is required in the long run. In this regard, a model with three agencies – an agency with a civilian space agenda, Space Command/DSA and Space Force could be a way forward.

The role of the Indian Space Research Organisation (ISRO) should remain intact and it should continue to do its job, while investing further in technology development, especially in the area of launch vehicles. The other agencies being recommended should plug-in as per the requirements. Space Command would have the major job of ensuring that the three

services get the benefit of space capabilities and the Space Force would deal with issues of strategic deterrence, Space Situational Awareness (SSA) and technologies with direct and indirect correlation to weaponisation of space. At some time in future, the Space Force might look at establishing 'extra-terrestrial supremacy' as also resolving conflicts that could arise as a result of excavation on the surface of the moon and Mars for minerals.

The safety of space assets is the job of the military as a net security guarantor aiming for a full spectrum dominance. Thus, there is a paramount need for India to be proactive in developing an 'Indian Space Defence Force' which is in line with its future requirements and stated policies.

Sub-Theme 7: AI and Robotics - From Concept to Delivery

Lt Col PJ Anand Kumar (Retd)
Chief Technology Officer, DataVal Analytics Pvt. Ltd., India

The speaker– Lt Col PJ Anand Kumar (Retd) began by elaborating on the philosophical, evolutionary and biological underpinnings of intelligence, bringing out the pivotal role of the prefrontal cortex (PFC) in inductive reasoning and drawing inferences. As we are aware, modern logic or inferencing are better means of disrupting the loop in battles compared to computational power.

AI is rapidly replacing human beings and some of the key reasons for the same are as mentioned below –

- ***Sight and Processing-Related Limitations***. The human neural network is habituated to seeing and processing data in a particular way. Besides, there are certain areas, such as the infra-red part of the spectrum, where human beings lack sensory and processing abilities.

- ***Lack of Pure Logic in Decision-Making***. In addition to the PFC, the human brain consists of the emotional part and the reptilian part, all of which responds to any input, which leads to stress. Hence, the human brain needs training so that the PFC (i.e. logic) is not undermined by other parts.

- ***Information Overload***. Given the volume of data available, it is not humanly possible to process information in an efficient, time-bound manner.

- ***Security Issues***. In the context of network-centric warfare, real-time situational awareness gets undermined because of the cyber constraints, as in the case of the Stuxnet worm-attack on Iranian nuclear facilities. AI provides a superior anti-penetration strategy. A knowledge base today is created by inductive processes involving machine learning, artificial neural network, deep learning, long short-term memory, natural language learning, etc. With big data having replaced data, computing can be done at different levels, i.e. at the edge, in-between and at the backend with the internet of things (IoT) and there is platform of agnosticism. Thus, since there were many changes and RMAs taking place, non-monotonic reasoning is required.

The need of the hour is to make autonomous systems which cannot be penetrated, since even having a link could lead to hacking, as with the case of the Iran-US RQ-170 incident. It is also becoming rather simple to weaponise existing, autonomous drones and as such, one has to be prepared for Lethal Autonomous Weapons System (LAWS). There are myriad ways in which drones could be used today and swarm bots are becoming increasingly popular since it is more difficult to respond to them. In addition, without the need to hard-code, they can directly be given missions. So, while it is operating within a secure zone where one has spectrum dominance, it could be flown into hostile ground where it can operate autonomously. They are also self organising and do not have a centralised command. So, loss of a couple of drones does not impact the mission. Thus, defensive measures against swarm attacks cannot be carried out manually and one needs to install autonomous systems.

The transformation in the way cyber attacks are being carried out can in a way be compared to what is happening in apiculture. Just as we have moved from looking for honey to farming honey, so also, cyber attacks have moved from hacking to farming. If a nation is using hardware, software and even networks which are not indigenous, it is susceptible to this technique and is in a very precarious situation. Anyone could be a conduit for a malware to reach a critical place like a nuclear facility and the example of Kaspersky's alleged involvement in stealing data highlights the same.

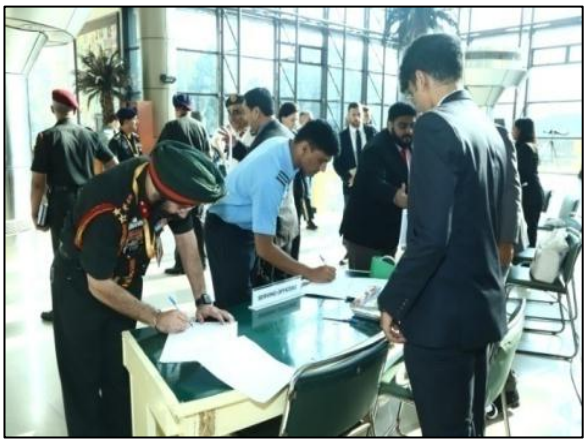
There is a need to have specialist officers, with experience across various platforms and the vertical and horizontal growth to be able to deliver optimally in this field. However, given the resource constraints, the role of integrated technologies and the art of abstraction has become important. Constraint propagation offsets the need for specialists, hence the need for being an integrator and being strong in modern logic emerges.

Warfighting is not limited to the battlefield, it involves guarding your supply chain and going into every process of nation-building. This is where having data scientists and becoming an integrator would help, as only AI can undertake such large-scale processing of data. While people may be averse to using robots, they could assist in the tactical, strategic, as well as the civilian space by eliminating the need for avionics, crew safety, logistics, etc. Not only can robots be replenished, they are economical and the law regarding them is at present vague too. While adequate caution needs to be exercised with regard to the use of robots and

LAWS, they have become a necessity. There is an emergence of a new AI-enabled species and apure PFC, unlike the human brain which has the emotional part in addition, which would help find the best solutions to most of the problems, including military ones.

Session - II : Chair and Panellists with Director, CLAWS

PRAGYAN KALEIDOSCOPE: DAY ONE



Signing In - Pragyan Conclave

Jam-Packed Manekshaw Auditorium

RRM with COAS

Chiefs Trio

Military Diplomacy at it's Best

Taking a Break

Dialogue Continues – COAS Dinner

Students – The Keen Participants

Dinner with the COAS

Deep in Discussion

DAY - II

SPECIAL ADDRESS

Special Address by Lt Gen Sk Saini, PVSM, AVSM, YSM, VSM, ADC

Vice Chief of the Army Staff &

Chairman, Board of Governors, CLAWS

Lt Gen SK Saini, PVSM, AVSM, YSM, VSM, ADC

Vice Chief of the Army Staff

Director, CLAWS, DG PP, eminent panellists, participants from home and abroad, ladies and gentlemen, members of the media.

It is my pleasure and privilege to be here this morning, amongst the domain experts in various fields, who are here to share their perspective on this very contemporary theme. I would also like to compliment DGPP and Director, CLAWS for selecting this topical issue which will give us fresh insight into the questions which we are grappling with-especially those who are in the profession of arms. I am confident that the deliberations today would be equally engaging and valuable, as yesterday.

As we commence today's session, I intend sharing my thoughts on what is changing and our coping strategy. Complexity and ambiguity have crept into present-day conflicts as compared to wars fought three decades back. There is widespread consensus that the character of conflict is changing, but little agreement as to how. New terms have proliferated, just to mention a few - hyper war, fourth and fifth generation war, hybrid war, non contact war, unrestricted warfare and grey zone warfare, which to my mind, is a misnomer. This approach of classifying conflict into such categories is overall compartmentalised and does not give one a sense of what is changing. In fact, we have a propensity to pick up new terms after an article appears in a journal and start changing them. I think, in our 'Glossary of Military

Terms' or otherwise, we have adequate terms with which we could describe the changes that are taking place. With these terms, there are different issues that come to the fore. We always say that the nature of conflict is enduring and the character is changing. These terms also indicate that, perhaps, we may have to look at the nature of conflict itself- all the adjectives that we use to define the enduring nature of conflict like 'victor and the vanquished', 'violence' etc. These indeed are changing and therefore, we may need to have a look at that as well.

By its very chaotic nature, conflict is impossible to anticipate precisely. Therefore, the challenge lies for the professionals to make a reasonable assessment, which should not be very much off the mark so that we can align the policy and the resources in the planning process. To do that, the first question we need to answer is - Is conventional war dead? I don't think so. Assessment or rumours of demise of conventional warfare have been exaggerated. Anticipated trends show that, while large scale traditional land wars may be less probable, conflict on the land below the threshold of all out war may be more frequent. However, as far as Indian Army is concerned, with the peculiar conditions that we have on our borders coupled with internal security situation, we need to be prepared to conduct operations across the entire spectrum of conflict.

In the last two decades, new medium or domains of space and cyber have joined the traditional war fighting domains that are - land, air and maritime. While our understanding and doctrine for traditional war fighting domains is mature and clear, the two new medium are continually evolving in an unstructured manner and are therefore impacting on war fighting in the other domains as well. In fact, it may so happen that in a given operation, the war fighting in these two domains may be preeminent, with the traditional domains in secondary role. We also see that the line between what equates to regular and irregular military activity has blurred and the conflict paradigm has shifted. Similarly, the differentiation between conventional and non-conventional activities has reduced. Therefore, the land forces need to be prepared for conduct of overt, covert and outsourced operations - either separately or as conjoint. We also see that the qualitative technological advantage that the states have amongst themselves, or with non state actors, is eroding and will erode further. The takeaway from this scan is that the range of threats that we now face is actually expanding.

Therefore what do we need to do? First and foremost, to my mind, is institutional and operational agility. To hedge against an uncertain future, land forces need to be more agile and this needs to be institutionalised both at organisation and individual level. It calls for a change of mindset as well as investing more in military education and training and here lies the primacy of the cognitive domain. Our agile organisations should also have the ability to decentralise resources, decision-making and have some uncommitted resources or reserves which can then help us deal with the unexpected.

A word about doctrine; by their very nature, military doctrine and operations are works in progress. To produce a firm doctrine takes anything from three to five years and thereafter for the doctrine to mature and implement takes another decade or so. Thus, there is a reason or cause for us to telescope this implementation time. Moreover, our acquisition and sustainment processes need to be more responsive so that we can cut down this time and be

more relevant to the change. Doctrine must also focus on cross domain synergy doctrine for land warfare cannot be totally separated from war fighting in other domains.

With a magnified grey zone (here, I am not using the grey zone term where political dimension is more paramount) unprecedented situations will arise defying solutions or clear-cut courses of action. As of now, as you are aware, we are grappling with anti-drone operations as to how to conduct them; all technology that is available these days is for point defence, but that is not what we are looking for, that is in the domain of the agencies like the NSG, etc.

How do we adapt to this paradigm to seize and retain initiative? What changes in our doctrine, organisational structures and training will this entail and what will constitute victory? These are some of the questions that we are looking for answers from this seminar.

Now a word about technological dependence paradox. While we have to embrace new technology, it alone won't help us win wars. We need to guard against creeping dependence on technology. Often these dependencies grow to an extent that it appears impossible to operate without technology and this generates vulnerabilities. We tend to lose basic skills of a soldier. Just to illustrate the point, GPS has dimmed the navigation skills over a period of time and similarly it has blurred the sharp eye for looking at terrain; but in case the technology is denied to us, or we cannot access technology at that point in time, a soldier should be able to perform the basic task for which his skills have been honed through the training period. Therefore, are we going to shun technology? Certainly, no. But we must recognise its limitations and vulnerabilities and have fallback options for the battlespace which has become both physical as well as virtual.

In the end, I would like to thank all our panellists for yesterday, as well as those who are going to give us the inputs today, for their effort and hard work and I am sure we are going to find answers to these very vexing issues.

Jai Hind.

VCOAS, DG PP and Director, CLAWS – Special Address

DAY - II

SESSION III: TRANSFORMATION IN THE BATTLESPACES

SESSION IV: HYBRID/ SUB-CONVENTIONAL WARFARE

SESSION III: TRANSFORMATION IN THE BATTLESPACES

Opening Remarks by the Chairperson

Lt Gen AK Singh, PVSM, AVSM, SM, VSM (Retd)
Distinguished Fellow, Centre for Land Warfare Studies, New Delhi

The Chairperson-Lt Gen AK Singh, PVSM, AVSM, SM, VSM (Retd)- began by stating that while war and conflict were and would remain intrinsic to human beings, its form and instruments would change rapidly. Warfare before the 21st century was intimately linked to statecraft, with an identified adversary and quantified threat, while the 21st century battle-field is multi-domain, with shades of grey.

There has been a paradigm shift in the character of conflict and modern-day conflicts have expanded to include sub-nationalities, terrorists, insurgents, religious fanatics and ethnic interests. The battlespace has encompassed sabotage, subversion, non-kinetic confrontation and traditional armed-conflict in all its forms, but with no traditional frontlines as witnessed during the two World Wars, as also, the Second- and Third-Generation warfare. Hybrid warfare strategy, driven by high-end technology that facilitates remote warfare, is moving to a new generation of warfare. As an unrestricted, collective methodology, the hybrid threat concept has bypassed the cognitive boundaries of traditional threat-characterisation and the application of organised, collective violence.

When we look at what impact technology will in future have on warfare, it is not very easy to predict how technology will develop further and how it will adapt to dominate the multi-domain battlespace. The future is unlikely to be a linear extension of the present trends, keeping in mind the disruptive technologies that are being pursued with great focus, such as directed-energy weapons, AI, cyber capability in both its offensive and defensive adaptations and autonomous weapons. Besides, robots and bot-swarms are set to revolutionise warfare as never before while the recent talks related to the regulation of LAWS in the UN have yielded no progress and led to a stalemate. The serious legal and ethical issues that arise consequent to the remotely-controlled drone strike on Maj Gen Soleimani have also contributed to the lowering of threshold of war. Remote warfare thus removed the need to address *jus ad bellum*, thereby minimising the risk for decision-makers, which may result in such decisions being taken for narrow gains and not being carefully thought through.

Precision fire at longer ranges and pinpoint targeting are replacing mass attacks and firepower respectively and the manifestation of kinetic war has and will undergo profound changes. The future battlespace for network-centric warfare would be defined by inter-connected physical, informational and cognitive battlespaces. There is a need for greater focus on the cognitive domain in India and the Indian Armed Forces and if the adversary is not confronted in the cognitive domain, it will hasten a kinetic confrontation, which, at best, would offer only a short-term outcome, as has been evident in the conflicts in West Asia. Sustained, long-term outcomes will remain largely dependent on the ability to influence or change the cognitive domain and prosecute ideological attacks.

In the aerospace dimension, the said battlespace will also undergo a drastic change. AI-based technology will dominate the battlespace, with a combination of optionally-manned aircraft operating along with autonomous drones and swarms. On the issue of the effectiveness of aero-deterrence in view of the new forms of hybrid warfare and non-state actors, a study by a US Air Force think tank which looked at 21 crisis deployments of the US, has surprisingly said that the main battle tank has been found to be the most effective deterrent, hence bringing out the criticality of the land battlespace. The means and methodology of controlling the land battlespace, however, will have to undergo a subtle change, both for deterrence as well as for warfighting. The Indian Army's decision of raising Integrated Battle Groups is in consonance with the same.

Keeping the centrality of the human dimension in modern conflicts, there is a need to develop military leaders with the skills, vision, steadfastness and comprehensive understanding of the challenges that modern warfare present, as also, the endurance, strength of character and mental resilience to meet the conditions that modern warfare impose. Thus, the Indian Armed Forces need to continue preparing leaders for the 21st century.

Sub-Theme 8: A New Strategy for a Changing Era

Lt Gen DS Hooda, PVSM, UYSM, AVSM, VSM (Retd)**
Board Member, Cyber Peace Foundation, India

The speaker-Lt Gen DS Hooda, PVSM, UYSM, AVSM, VSM** (Retd)- began by stating that while the contours of the change in the character of warfare were broadly understood, the

difficulty lay in the army's ability to adapt to that change in terms of organisational structures, thought processes and doctrines.

Keeping in mind that the future political ends and the means of warfighting are unclear there can only be broad guidelines, as opposed to specifics, for a strategy dealing with future warfare. Some aspects about the changing character of warfareare as given below:-

- **Man-Machine Interface**. The technologies of the Fourth Industrial Revolution will have a huge impact on the way future wars will be prosecuted, one key area being 'man-machine interfaces'. The important point that merits attention is the degree of autonomy that will be provided to autonomous systems and the position of the human with regard to the loop. It is still unclear whether this will be of assistance or turn out to be a complication during warfare.

- **Democratisation of War**. War is no more restricted to soldiers alone and the actions of the military have become very transparent. Videos pertaining to the military going viral on social media, puts caution and restriction on the way the armed forces operate and think. In addition, like Andrew Krepinevich in an article mentioned that there is 'democratization of destruction', it happens when dual-use technologies that mirror or outstrip military technologies are available in the civilian sector and accessible by locals and non-state actors. This has increased the capacity of the latter to wreak violence to a level, earlier limited just to the military.

- **Cyber and Networks**. India needs to view data, both military and personal, as a strategic weapon. Data as we know can be used for influencing political processes and decisions, as also, causing divisions in society and inciting violence without resorting to the use of force. There is thus, a need to protect one's systems and networks, since if these systems are targeted and degraded through various kinetic and non-kinetic means, it will amount to winning half the battle.

- **Hybrid Warfare**. One has to be prepared for wars prosecuted through a combination of economics, politics, diplomacy, military, State, non-state actors and so forth.

In preparing for the future conflicts, one needs to plan for the war one will be forced to fight and not which one wishes to fight; the latter being based on one's own capabilities, weapons systems and doctrines. Case in point being the Russian and American experience in Afghanistan.

In an India – Pakistan context, will Pakistan fight a conventional battle with India, as India would desire, given her conventional superiority over Pakistan? Pakistan could raise the nuclear issue from the very beginning, given that India tends to ignore the nuclear aspect almost totally whilst planning for a conventional conflict. In addition, it is critical to have an exit-strategy. In a scenario in which there is a conventional conflict between India and Pakistan and the former achieves some spectacular success occupying parts of Pakistani Punjab, would India be able to gracefully exit, or would she get embroiled in a hybrid conflict there? In a similar vein, the Chinese will exploit their superiority in the cyberspace, long-range missile systems and information warfare, rather than attacking Indian defences in the Himalayan watershed. Hence, it is important not to plan everything based on one's doctrine but look at various contingencies.

The salience of doctrine when planning for operations should not be pushed to the background due to the lure of technology. Merely relying on technology without

organisational structures, concepts and a doctrine never works as was proved by the Germans, when despite the Americans, the Russians, the British and the French having aircrafts, tanks and radio, it was the Germans who succeeded initially in manoeuvre warfare as they could put all three together into a strategy and a doctrine of 'blitzkrieg'. In India, there is a tendency to first procure the system and then try to integrate it into the existing structures and doctrine, not being the right way forward. Developing a doctrine, incorporating the future battlefield scenarios into it and looking ahead is exigent.

Another aspect that needs to be debated is the issue of 'integrated low-cost systems versus a monolithic, complex platform'. In this regard, if we compare the Rafale aircraft with Kratos Defense's Valkyrie drone, does it make sense to buy 50 of the latter for the same price as one Rafale? In the US, DARPA's 2019 call for proposals for research in 'Future Disruptive Technologies for Warfighting' was required to reduce reliance on stealth technology and to increase lethality through overwhelming performance, under the Air Force section Similarly, the need to reduce reliance on monolithic, complex platforms using small, highly networked vessels based on commercial designs is given under the maritime section.

There is also an urgent requirement for integrating numerous, small systems. While purchasing systems, integration must be kept in mind or else it will be like the F-22 and the F-35, which despite being the most modern aircrafts available with the Americans, are not able to talk to each other stealthily.

Information War has become a game changer and it is not only non-state actors, but States too who are engaging in propaganda and fake news, since it has become easier than ever to do so. Wars are fought on Facebook and Twitter and victory is defined by who gets more 'likes'. When engaged in a real war, it will become difficult to match the illusion that one has created in the virtual space with what is happening on the ground. There is also a lack of joint functioning in the cyberspace and in the Army different arms like Signals, Intelligence, etc. are looking at different aspects, thus maybe necessitating the requirement of a Cyber Corps.
Human capital will remain very important and we must plan for the kind of soldiers that are needed for the future. The training methodologies, standards and systems need to be in congruence with the requirements of the future battlefields. Thus, the need and methodology to invest in the military human capital should be dictated by the importance of understanding the wars one will get engaged in.

Sub-Theme 9: The Impact of Long - Range Vectors &Precisionary

Dr. Jack Watling
Research Fellow Royal United Services Institute, United Kingdom

Highlighting the importance of artillery, the speaker-Dr. Jack Watling- stated that the destructive nature of war had not changed and as such, if non-kinetic operations did not enable one to deliver kinetic effects, one will not remain competitive.

Trends in Technology : Some trends in technology that will re-shape how fires are delivered in the future are discussed below-

- **Range.** In the next decade, the range of artillery could double across most systems, which means that 155 mm howitzers would have a range of 70 km Multiple Launch Rocket Systems with range of 150 km and tactical battlefield missiles with range of about 500 km. However, beyond the range of 40 km, these systems would need precision munitions.

- **Automated Fusion.** This is the capacity of computers to take multiple sensor-streams and fuse the information. Various techniques, such as edge processing have significantly reduced the human burden of analysis, unlike the situation during the Gulf War and the War in Afghanistan where the US troops achieved precision by employing over 1,000 and 200 personnel, respectively. An example of this technology is the 'Fire Weaver' system developed by Rafael. Using this, the reconnaissance troops can select a pixel in the picture indicating the target, which will be then processed by the system and the only input required from the command post is the decision regarding whether or not the target needs to be engaged, whether it is worth the munition, as also, whether it is worth revealing the position of the munition. This has not only enabled precision effects, but also enabled conventional and legacy artilleries to become highly effective. Similarly, in the Zelenopillya rocket attack, the Russian 'Leer-3' system, consisting of three Orlan-3 UAVs and a mobile centre, revealed the concentration of Ukrainian forces by triangulating the position of every cell phone in the set grid squares. This, along with the live feeds given by the UAVs, enabled 40 salvos of BM-21 to be fired; rendering the two Ukrainian formations combat ineffective in about 20 minutes. While it is not a highly accurate system but it certainly is a very quick and an effective engagement system.

- **Multi-Sensor Active-Seeker Munitions.** The present generation sensor-fused munitions are highly capable, active seekers which remove the need for a live feed from the forward posts or for the target to be static, thus transforming the timeline on targeting. Based on the information of a target's presence in a specific grid square, the active seekers, having gone through the fusion system, will scan the area and strike the targets. The fidelity of the sensors on the munitions is very high given the fact that only a couple of munitions are fired. Targets can be engaged even in complex terrains and environments, including high density of cloud, by having multiple sensors, thus increasing their reliability as well.

- **Defensive Measures**. The defensive measures of the past, Counter Rocket Artillery and Mortar (C-RAM), ran out of ammunition very quickly. Some modern defensive measures are as enumerated below–

    - High-energy lasers. These are able to engage incoming munitions but their efficacy is terrain and environment-sensitive.

- Ballistic Missile Defence (BMD) systems. This technology is maturing and as BMD systems are rolled out in greater numbers, their cost is also coming down. An example is the Iron Dome.

- High-frequency Microwaves. These are limited in terms of their range but can engage multiple incoming munitions simultaneously and hence, don't suffer from the same issues of saturation as other types of defensive systems.

Re-shaping of the Modern Battlefield

If we look at the economic aspects of engaging the adversary with precision munitions, then an artillery shell costs at least USD 70,000 a shot, missiles around USD 3,00,000 per fire and tactical missiles around USD 8,00,000 per fire. As such, any force will have to be selective about how they are applied. This further means that conventional fires still matter and without a significant conventional-fire capability, one can simply be overwhelmed.

Since artillery systems with a range of 70 km will require precision munitions beyond 40 km, the target can be engaged with massed conventional artillery when it is manoeuvring upto 40 km. Thus, there will be a stretch of 30 km where one would have significant levels of precision to engage the target but only a limited stockpile of these. Hence, the challenge for the force is in crossing that 30 km gap and getting into the 40 km conventional space without being decisively engaged and losing the critical enablers. As we know, all warfare relies on logistics and while one's logistical footprint at the tactical level can be reduced but at the operational level, there are large depots and concentration of munitions and material. This will not only fix most of one's available defensive capabilities but will also create fixed points of defence or 'defensive nodes'. These nodes cannot be targeted by the adversary without risking the exhaustion of their limited stockpile of precision munitions. At the point of such exhaustion, one can move into the 30 km space and engage the adversary who will not be able to fire back reliably or with the same effect. These 'defensive nodes' could be in urban areas because of better camouflage, better logistics links and the areas being more defensible and about 70 km or more away from the enemy forces.

One can also envisage a 'contested zone' in the centre where both sides are equally vulnerable to each other's conventional artilleryfire. There is also a 30 km gap between the forces which they have to manoeuvre through. Hence, the primary task at the onset of hostilities will not necessarily be heavy contact between manoeuvre elements; rather, pushing into the 30km space with relatively small force-packages and recce forces, UAVs and potentially autonomous systems, essentially trying to map out the enemy' scentre screen for their 'reconnaissance-strike complex' and start causing attritionto those centres. If those centres are not attacked, the result could be the same as the devastation unleashed on the Syrian Army by the Turkish precision-fires enabled mainly by the Bayraktar UAV in Idlib.

Implications

A traditional armoured-assault involves breaking through the front line, however, if the logistics chain is 70 km away from the fighting edge or 35 km away from the meeting point, there is no 'front line'; rather, a 'front line-of-control' and a large no-man's land where the forces could potentially mutually penetrate, leading to engagement at an unexpected angle as witnessed in Ukraine. Speed of engagement becomes of paramount importance in such unexpected encounters. There is also a need for the force packages to be smaller, capable of sending back images for fusion so as to enable fire's-effect, have significant lethality and also have short range air defence capability to avoid attrition.

While the main battle tank could cut though the formation, given that it would have to traverse 70 km to get into the direct fire zone, the question is whether it would get there with its supporting infantry?

When factoring in Hypersonic Weapons one must remember that the said capability is expensive and one would not have much of it. Hypersonics make all of one's critical nodes vulnerable and the speed at which it comes gives the target no reaction-time. The real threat from Hypersonics is in the sub-threshold context and not in a warfighting context where one had been fighting for a while and expended a lot of the capabilities. If the adversary decided to escalate to a high-intensity conflict, the first strike would probably not be opening up with conventional artillery on the front, but a Hypersonics threat which would come with virtually no warning and potentially knock out one's higher echelon capabilities. Given that the entire battlefield is held at risk, the art in beating the threat of Hypersonic Weapons will lie in how tooperate in a way that does not present the adversary with opportunities that it cannot resist.

Sub-Theme 10: Special Forces - A Force Multiplier for Land Operations

Brig H P Ranasinghe
RWP, RSP, ndc, Director of Operations, Sri Lanka Army

The speaker, Brig H P Ranasinghe, RWP, RSP, NDC, began by mentioning that the Special Forces (SF) had made significant contribution during the two World Wars with their ability to operate behind enemy lines. As an outfit, the SF is sophisticated, highly trained, motivated

and capable of operating in all terrains and weather conditions using unconventional tactics, techniques and modes of employment. The battlefield is becoming increasingly information-dense and technologically-driven tending to non –contact battles, which has necessitated organisational and doctrinal changes in the SF. There are several categories of force multipliers including human, environmental and organisational and SF belongs to the organisational category. What makes it an operational force multiplier is its ability to engage in significant deep operations in the operational framework, engage in decisive engagements in adverse conditions to change the tide of war and the fearsome reputation gained from the past successful operations.

In the Sri Lankan context, the necessity for the Sri Lankan Army to re-organise and re-structure in response to the then principal terrorist threat-the Liberation Tigers of Tamil Eelam (LTTE)- led to the raising of Sri Lanka's SF consisting of two of the finest fighting regiments - the Commandos and the Special Forces.

In response to the increased threat by LTTE, Sri Lankan military experts decided to maximise the use of small-team operations leading to the formation of Long-Range Patrol (LRP) teams in the mid 1990s to neutralise targets of strategic nature. Two major missions conducted by the LRP teams were the neutralisation of Shankar, LTTE's second most important leader and in-charge of LTTE's air wing and neutralisation of the LTTE air threat. During the neutralisation of Shankar the most advanced equipment available with the LRP teams was only the Garmin 72 GPS and one of the of the four-man team was required to penetrate 60 km inside the jungles of LTTE controlled areas without effective communication facilities with higher headquarters. All this notwithstanding, the LTTE could not cope with the tempo of the small group operations and declared a ceasefire in 2002 and in fact one of the clauses in the ceasefire agreement was the cessation of LRP operations in the LTTE held territory.

The second mission, which was against the air threat presented by the LTTE, as in 2006, the LTTE had acquired the capability to enter Sri Lankan word airspace with their single-engine aircraft – the Zlin Z 143. While the Z 143 had limited offensive capability in comparison to the Sri Lankan air superiority, the LTTE could create potent deterrence by utilising the low flying aircraft for deceiving the radar system and carrying out suicide missions. In response to this threat, LRP missions were launched into LTTE's high-security zones. These missions were successful in locating and neutralising the runway used by the LTTE, 70 km away from their forward defence lines and by the later part of 2006, the Sri Lankan SF had access to the latest communication facilities which enabled the small groups to have direct and secure communication with the higher headquarters.

The Sri Lankan SF during that time operated from the sharp-end of the strategy through the operational and tactical level executing a multitude of tasks including striking the terrorist leadership deep inside LTTE controlled areas, destroying and disrupting LTTE's indirect weapon-system, logistic lifeline and, at times, also their reserves.

The physical use of SF even in the contemporary, digitised battlefield can have strategic impact like in the missions to neutralise Osama bin Laden and Abu Bakr al-Baghdadi. Operating in a technologically-driven battlespace, has put tremendous pressure on maintaining operational secrecy, which is the core value of SF operations. Besides, the technological advancement of the adversary hinders the effective employment of SF. In the information domain, the adversary is capable of winning a major portion of the battle even in the preparatory stages, using cyber-tools. Additionally, the SF faces the following challenges:-

- Finding the hostile parties and locating their activities without being detected or exposed.

- Dislocating the enemy or hostile groups without physically deploying troops on ground.
- Launching into mission areas undetected and overcoming restriction on insertion-options.

- Difficulties in long-term survivability inside the hostile territories.

- High dependence of the SF on the electro-magnetic (EM) spectrum.

- Difficulty of acquiring latest technology for SF in developing countries as compared to SF in developed countries.

These vulnerabilities have to be addressed with doctrinal changes and increased utilisation of technology. The doctrine of LRP behind the enemy line requires to be changed into a more clandestine manner. Maintaining operational secrecy has also become increasingly important as all SF members are also human beings, widely connected with social networks. In the light of the pace of technological advancement and IW adding complexity to SF operations, the following are recommended –

Organisational Changes

- SF should keep abreast with the latest developments in their fields and situational awareness, integration with horizontal and vertical stakeholders will be a key to success.

- Ensure friendly access to the Electro-Magnetic Spectrum while denying it to the adversary.

- The capability-development of small groups should focus on technology and alternatives for the same in case of its failures.

- Since future dimensions of warfare are subject to sudden changes, the SFs should be equipped to face such challenges.

Doctrinal Changes

- There is a need to maintain a database of actors and adversaries and analysis of their capabilities to ensure optimum preparedness.

- There is a need to revise the size of the SF to suit sustainability of small groups.

- Revise communication and other technical equipment to be above the standards of the adversary and modernise the weapons and ammunition used by the SF. All these should be incorporated when modifying the operational philosophy.

The SF will be equally relevant in technologically advanced, digitised battlefield conditions and would be a force multiplier for any theatre commander in the present and future battlefields.

Sub-Theme 11: The Nuclear Environment to Include the Impact of Hypersonics

Lt Gen Amit Sharma, PVSM, AVSM, VSM (Retd)
Scientific Consultant (Strategic Issues), Office of the Principal Scientific Advisor to the Government of India

Addressing the topic, the speaker-Lt Gen Amit Sharma, PVSM, AVSM, VSM (Retd), mentioned that Asia was the most nuclearised zone in the world, with seven nuclear powers in the vicinity, namely, India, China, Pakistan, Russia, Israel, North Korea and also the US owing to its extended responsibilities. Only France and the UK are left out. The doctrines regarding the employment of nuclear weapons by the nuclear-weapon states (NWS), the modernisation taking place in this field and the implications of the said modernisation are discussed below.

Nuclear Weapon States

United States

The US became a nuclear power with the Trinity test in July 1945. A majority of its present infrastructure is over 40 years old, with 25 per cent of the infrastructure dating back to the time of the Manhattan Project and weapons & launch systems dating back to the early 1980s. This has necessitated modernisation in the US and as per the Stockholm International Peace Research Institute (SIPRI), around a trillion dollars have been allotted to achieve the same by 2040. This includes changing the Ohio-class Ship Submersible Ballistic Nuclear (SSBN) to Columbia-class by early 2040.

Modernisation has already taken place in the field of command and control systems, infrastructure, launch systems and warheads and the weapons have grown from the First generation to the Fourth generation, making them more accurate and at least three to five times more potent. Moreover, the entire arsenal is capable of destroying the adversary's status of a nuclear-weapons power in the first strike, with the addition of 'super-fuse' to warheads. Hence, while the modernisation has been carried out under 'Stockpile Stewardship Program' which aims to keep the stockpiles safe and secure, it has led to insecurity and strategic imbalance, leading to an arms race.

As per the US's Nuclear Posture Review (NPR) 2018, the role of nuclear weapons is to prevent others from using nuclear weapons against the US and deter a large-scale conventional war with any NWS. The clause regarding the necessity of having a flexible response capability i.e. low-yield nuclear weapons, is a new addition to the NPR. It has been put into effect as per open sources, with one of the SSBNs on operational patrol equipped with a five-kiloton nuclear weapon. However, there is a contradiction in this clause as there is no 'limited' nuclear war; a 'limited' nuclear war escalates very quickly into a strategic nuclear exchange, unless the adversary is a non-nuclear country. The 2018 NPR further mentions that in the event of Russia and China using limited nuclear weapons against the US, they would be subjected to incalculable damage. If that is the US's posture, using a five-kiloton weapon against someone else is also likely to evoke the same response. India's posture of 'massive retaliation to inflict unacceptable damage' in response to the use of tactical nuclear weapons (TNWs) is also quite similar.

Russia

Russia became a nuclear power in 1949 and developed a triad by the 1960s. Modernisation had been going on in Russia since the 1970s at a very fast pace. On the weapons system, while the Hypersonic Glide Vehicle (HGV) has been inducted into the Russian nuclear forces in very small numbers, nuclear powered underwater drones and nuclear-powered cruise missiles are under development. While the Americans have also been working on Hypersonic Weapons for a while, they have not been inducted, as the priority for the US is to work on Hypersonic Weapons for conventional operations as opposed to nuclear. HGVs are an expensive, niche capability, which China also claims to possess and some analysts believe that the HGV capability has resulted in a strategic imbalance. The US believes that as the HGV is capable of beating any BMD, it gives Russians a first strike capability while the Russian point-of-view was that it gives them a credible second strike capability. However, since Multiple Independent Targetable Re-entry Vehicles (MIRVs) are capable of beating BMDs, inducting HGVs into the defence inventory does not make much difference. A situation of mutual vulnerability has been created, with the Russians and Chinese feeling that the US has a better BMD capability and the US feeling that these countries have a system which could penetrate it. This mutual vulnerability has infact led to strategic balance.

The Soviet Union followed a policy of 'No First Use'. Gradually, it changed to 'First Use' after the formation of Russia. In 1999, the then chief of the Russian nuclear forces had spoken about escalating to de-escalate. While this was mentioned only once and there was no official doctrine regarding it, the NPR quotes 'escalate to de-escalate' as the doctrine of the Russians. This has been challenged by a number of Americans themselves. Officially, from the Russian side, President Putin had spoken twice in 2018 about Russia's nuclear status and mentioned that there was no provision for a preventive strike and that Russia's concept was based on retaliatory, reciprocal counter-strike. Such a counter-strike, President Putin added, should also be avoided as it could only result in catastrophe.

China

Military power is an important aspect of China's ambition of becoming a global power by 2049. As such, China has concentrated both on conventional as well as nuclear strengths, developing missiles with the longest range in the world – the Dongfeng-41. China possibly has the HGV-capability too, which was showcased in the National Day Parade in 2019. China's White Paper clearly states that they have a policy of 'No First Use', leading to strategic stability. However, the problem is that China's ballistic missiles are fordual-use. As it is not clear whether the missile would have a conventional or a nuclear warhead, there is a threat of miscalculation in countries like the US which have a launch-on-warning system.

France, UK, Israel and North Korea

Modernisation is ongoing in all of them. What makes France different from the other countries is that it has the concept of firing a warning missile before resorting to the use of the nuclear option in the form of a massive retaliation.

Modernisation

Nuclear Command and Control

The nuclear command-and-control of any country has the potential to be targeted, especially in view of increasing cyber threats. Command-and-control consists of two portions – people in the command authority and the system through which orders are passed. Regardless of whether one's doctrine is of 'No First Use' or otherwise, adequate back-ups need to be in place to cater to eventualities of people in the command authority being killed or communications being targeted. It is imperative for the command and control system to be kept functional. While AI is impacting decision-making process in a major way, however, regardless of the improvements in technology, the final decision to launch the weapon must be with the head of the state or the political head and not a machine. Technology in this case can only help in the process of decision-making.

Tactical Nuclear Weapons (TNWs)

TNWs, are those weapons which are used in the tactical battle area and affect the conduct of the actual battle. There is nothing specified in the yield, or the number of casualties that a TNW can cause.

Implications

The India-Pakistan Equation

The two, essential differences between the nuclear weapons of India and Pakistanis that first, while India's nuclear weapons are meant to deter any country from using nuclear weapons against her, Pakistan's are purely anti-India. Second, while India's nuclear programme is more-or-less indigenous, the Pakistani nuclear arsenal has been developed as a result of a 'beg-borrow-steal programme'.

While conventional operations are based on the political aim that is translated into military objectives, deterring Pakistan or any other country from using nuclear weapons against India is the job of the Strategic Forces Command of India.

Deterrence can be in two parts – the military capability and the political will. India's reactions to Pakistani provocation earlier have not evoked strong actions and this had emboldened Pakistan. But all this has changed in light of bold actions taken by India, which includes cross-border operations in Myanmar, Surgical Strikes and use of the Air Force to target the enemy's terrorist camps. Today, India has the military capability and the political will, which has added to credible deterrence against any country. Conventional operations should be planned the way they used to be done, keeping the nuclear aspect out and if any adjustments needed to be made to plans, it can be done in real-time as the operations room of the three services, the integrated defence staff headquarters and the nuclear operations room are all connected in real-time.

As long as mutual vulnerability stays, no one will use nuclear weapons as everyone realises its dire consequences which is borne out by the fact that there has been no nuclear exchange since 1945. As such, nuclear deterrence has proved to be effective and India is safe as a nuclear power.

Session III : Chair and Panellists of with Director, CLAWS

SESSION IV: HYBRID/ SUB-CONVENTIONAL WARFARE

Opening Remarks by the Chairperson

Lt Gen Subrata Saha, PVSM, UYSM, YSM, VSM (Retd)**
Member, National Security Advisory Board

The Chairperson - Lt Gen Subrata Saha, PVSM, UYSM, YSM, VSM** (Retd) - began by stating that there was consensus on the points that the character of war was changing and that hybrid war had emerged as the cardinal challenge for the immediate future. Four major issues pertinent to hybrid warfare are as discussed below-

- ***Concept.*** Hybrid war is premised on avoiding the strength of the adversary and striking the weakness. In fact, since Article 5 of NATO states that an 'armed attack' on its member-states would be deemed as an attack on all NATO members, Russia has skillfully kept all its actions restricted to the grey zone, so as to avoid a NATO consensus on the act warranting action under Article 5. Similarly, China has exploited India's faultlines in the North-East through the 1960s and 1970s. Pakistan also had done so, till they possessed East Pakistan. Post the liberation of Bangladesh, Pakistan has resorted to fermenting trouble in Punjab and Jammu and Kashmir (J&K). Deterioration of the social fabric of a country provides a fertile ground for the prosecution of hybrid war as is evident from the statement issued by Ansar Ghazwa' tul Hind, the J&K Al-Qaeda wing, saying that the riots in Delhi and the Taliban Peace Agreement have "energised jihad".

- ***Collaboration.*** Collaboration between agencies in a hybrid warfare environment is of utmost importance as was evident post the 2014 floods in J&K. The Indian army was on an all time high as an institution for its humanitarian and disaster relief operations, exemplified by the public in Srinagar wanting the Indian Army to handle the Public Distribution System. Post that high, every conceivable stakeholder was engaged during that time to provide a conducive environment for the elections, resulting in the

highest voter turnout across party lines in 25 years and with no interference from any agency.

- ***Communication.*** Like technology, social media is also neutral and even traditional media thrives on social media with tweets becoming the fodder for prime-time news. The general impression is that Hizbul Mujahideen militant-Burhan Wani, is a creation of the social media. His famous photograph with ten other militants in an apple orchard in Pulwama, was first picked up by a Srinagar-based newspaper with an annotation about the group and where it was hiding. This was then picked up by a Delhi-based, national daily and turned into a centre-page story during the weekend. Subsequently, it was even published by a leading periodical as the cover story and the rest is history. To be able to use social media one needs a narrative with substance, speed and scale to spread it. There is a need to have multiple agencies looking after social media, because authorising a few agencies to put out tweets for a 1.3 million-strong army, deployed in challenging areas, will not work. In fact, junior officers should be given the task of handling social media as their tweets are taken with greater credibility than official releases.

- ***Preparedness.*** The preparedness for hybrid warfare is a national effort which cannot be left to Army Commander's Special Financial Powers Fund alone and statistics reveal that in the last three financial years, India had signed 58 contracts worth 1.38 lakh crore rupees and sanctioned Acceptance of Necessity (AoN) for 4.04 lakh crore rupees worth of items in the last five years. Not many of those AONs and contracts are meant to prepare for hybrid threats. By the same principle we in the Armed Forces need to look at our investments in capital, concepts, organisation and training to serve the purpose of combating hybrid warfare.

In the Information Age, the emphasis has shifted from conquest to influence and it is futile to invest capital, both human and monetary, if political preferences can be influenced. The Information Age, which has given a set of advantages and disadvantages, has peaked in a decade or so and the world is set to witness a new age. This age would be driven by AI, nano-technology, quantum sciences and genetic engineering and characterised by individuals with augmented capabilities – or the 'Cyborg' era. This would have an impact on the competition for influence and power i.e. politics. If war is politics by other means, does it mean that we are returning to the primitive era of individuals and small groups, albeit with much more advanced technology?

Sub-Theme 12: Operations in a Grey zone Environment

Lt Gen (Dr.) Rakesh Sharma, PVSM, UYSM, AVSM, VSM (Retd)
Distinguished Fellow, Centre for Land Warfare Studies, India

The Speaker - Lt Gen (Dr.) Rakesh Sharma, PVSM, UYSM, AVSM, VSM (Retd) - began by stating that he believed that the nature of war was also changing and that the discussions on the nature and character of war in the present era could not be based on a 19th century understanding.

War has many definitions, though it is often defined as "an organised and often prolonged conflict that is carried out by states (countries) or non-state actors, characterised by extreme violence, social disruption and economic destruction." The UN and some other organisations define it differently. However, one school of thought feels that all these definitions of warfare are rigid and old, characterised by involvement of State and non-state actors, protraction, violence, social disruption, use of weapons and so forth. Military doctrines all around the world are designed to respond to these definitions but modern combat goes beyond the sensationalism of hi-tech weaponry which shadowed the broader concepts of social, political and cultural issues. Maybe it is time one moved beyond Clausewitz and revised the way 'war' is interpreted. The flawed conceptualisation of contemporary war results from the simplistic and jingoistic views of adversaries, the context under which the wars get triggered as also the unreasonable expectations of the larger public for quick wins at low costs. In addition, the excessively basic understanding of the politicians and the bureaucrats regarding the application of military power and what it will achieve, as also, the measures of victory or success further compounds the problem.

The emergence of grey zone warfare, which seeks to bridge the chasm between war and peace or between routine statecraft and an all-out war, can be attributed to the following two reasons –

- ***Breakdown of National Institutions***. Social media has overturned the importance of newspapers and hierarchical dissemination of information in numerous countries. This horizontal availability of information has resulted in the breakdown of national institutions and the way they function.

- ***Resurgence of Revisionist States***. The methods employed by revisionist states and non-state actors are beyond the realm of conventional war.

In order to develop response options, there is a need to distinguish between wars that use force and those which do not. In this regard, hybrid war is not synonymous with grey zone war. The tendency of the military to keep all types of warfare under its purview has led to grey zone operations being given a military hue and being seen as 'warfare'.

The US Department of State has laid down what it considers comes under the ambit of grey zone warfare, however there is no mention of a full, conventional war in that list. Grey Zone environment can be taken as 'a state between peace and war where adversaries aim to achieve geo-political and territorial ends without overt military aggression and crossing the threshold of open warfare.' The principal difference between hybrid warfare and grey zone warfare is that conventional operations necessarily constitute a part of the former and not of the latter; that grey zone conflicts could escalate to a conventional war is a separate issue.

Grey zone is a concept of gaining strategic advantage over an adversary with a breadth of operation that could be only limited by imagination. Seven basic characteristics of grey zone warfare are as mentioned below –

- ***Non-Military Nature***. Grey zone campaigns typically employ diplomatic and informational means, cyber militias, terrorists, etc. to avoid giving the impression of an outright military aggression. Such campaigns do not threaten the existential interests of the defender and are kept well below established military triggers. The aim is to retain ambiguity and avoid violations of international laws. The aggressor balances belligerent actions by placating the other parties, using deception. The non-military nature of grey zone campaigns ties down the recipient as the response becomes increasingly difficult. In this context, China occupying a large expanse of the South China Sea is a prime example.

- ***Protracted Emergence Using Proxies***. Grey zone operations unfold over a long period of time. The aggressor could plan an operation over 10-15 years. Such operations using proxies could involve provision of equipment and/or other enablers to terrorists or proxy forces active in the targeted country. In this regard, Russia's 'little green men' in Crimea, Hezbollah, Lashkar-e-Taiba and Hamas all bring out this characteristic. An important attribute of grey zone campaigns is that the recipient country faces a series of *faits accomplis* to which it is unable to react because it is not clear that the country is under a kind of aggression. While the belief is that it is routine but the country is being thrust with *faits accomplis* over a long duration.

- ***Non-Attributability***. Most grey zone conflicts and campaigns involve actions in which the aggressor aims to disguise the role, at least to some degree. It involves the use of cyber attacks or disinformation campaigns. These actions allow a grey zone aggressor to deflect the responsibility for offensive actions by simply denying involvement. Israel blaming Iran for the rockets fired at its settlements from Syria which was denied by Iranor Russia denying any interference in the US Presidential elections though Twitter notified that 1.4 million people interacted with Russian accounts during the 2016 US presidential electionare all examples of actions which are non-attributable.

- ***Use of Legal and Political Justifications (Sometimes Open and Attributable)***. Grey zone campaigns involve the use of extensive legal and political justifications often grounded in historical claims like the South China Sea Arbitration. The Sino-India border negotiations could also be placed on a plane of open and attributable grey zone warfare where things are deliberately delayed.

- ***Threat of Risk of Escalation as Leverage***. While remaining below the threshold of military response, the aggressor forcefully propagandises the risk of escalation as a source of coercive leverage. Pakistan often does this by raising the nuclear bogey and issue of TNWs as a deterrent against a conventional war with India.

- ***Creation of Economic Inter-Dependencies***. In the grey zone, aggressors plan to establish economic interdependencies that create implicit, long-time leverages. China's Belt and Road Initiative and its financial impact on nations could be seen as grey zone operations.

- ***Targeting of Specific Vulnerabilities***. Grey zone aggressors find societal divisions to undermine confidence in democracy and the leadership, including the military leadership. They attack in areas where the defenders cannot respond quickly and effectively. These could be social, religious, ethnic problems and grievances related to unemployment, economic stagnation, political polarisation, etc. All these issues which exist in a nation can be fanned as part of a grey zone campaign.

To effectively respond to grey zone operations, the following two things are essential –

- ***Identifying the Ambit of Grey Zone Operations***. The identification of initial actions by the adversarial State or non-state actors, with plausible deniability is crucial. It is not an easy task as such actions are purposely deceitful and the operations can constantly be scaled up, scaled down, stopped, re-started and new elements added.

- ***Crafting of Responses***. Proportional, commensurate, timely and limited nature responses must be crafted to the adversary's grey zone operations.

The strategy against grey zone operations must be based on the understanding of the essentially opportunistic, gap-seeking character of grey zone operations. In this regard, the following four aspects assume importance –

- ***Transparency***. Transparency is of paramount importance across the board. It has been significantly lacking in India, including the Armed Forces.

- ***Deterrence***. There has to be separate methodology of deterrence, not of the conventional or nuclear kind. Deterrence has to be evolved in the grey zone.

- ***Political and Bureaucratic Adaptation***. Scenarios need to be developed and exercised before a grey zone crisis occurs so that decision makers and analysts could lay down the groundwork for effective and timely reaction.

- ***Resilience of Civil Societies***. Grey zone operations are national campaigns and not military ones. Given the manner in which nations are developing, it is important that resilience is created in civil societies by a national effort. The nation and the hierarchies need to become more risk tolerant as well as tolerant to criticism.

While militaries keep upgrading their conventional preparedness these may be of only limited use in a Grey Zone conflict, thus it is time to prepare for the more probable and frequent conflicts – those in the grey zone.

Sub-Theme 13: Technology and Urban Warfare

Maj Gen Binoj Basnyat (Retd)
Independent Political and Security Analyst, Nepal

The speaker-Maj Gen Binoj Basnyat (Retd)- began by talking about the strong bond that Nepalese and the Indians share. By 2030, two-third of the world population is expected to be living in cities. Consequently, conflicts are also becoming more urbanised with technology playing a major role in the same. The two main challenges to the conduct of military operations in urban areas is understanding the urban environment as also being aware of how to operate in the same.

South Asia as a region is multi-ethnic, multi-religious, multi-lingual and full of complexities. It is a fragile region due to political instability, corruption and poor governance, as also, being home to more than 22 UN designated terrorist entities and nearly half of all UN listed individual terrorists. Last year saw an increase in terrorism in the region and there is a need for a collective South Asian resolve to fight terrorism.

Geo-political realities of South Asia

The old order of the region has been shifting with the formidable presence of China, the European Union (EU), Russia, US and the Middle Powers in South Asia. Geo-political realities attempt to challenge South Asia's civilisation and relationship and the way people have thought and behaved as South Asians. Aiding the shift in the old order of the region is the changing geography, new regional structures and power rivalry.

Changing Geography. Geography in the region is changing, with mountains which have been barriers flattening, so as to speak, with strategic communication networks being constructed and thus there is connectivity not just in the physical sense but also in terms of ideas, values, culture and technology.

Regional, Old Structure. The old, regional structure is changing, with growing Chinese interest in South Asia as seen in its White Paper of 2017 and marked by recent visits of President Xi Jinping to Nepal and Myanmar, Chinese support to Pakistan in the UN and her increasing engagement in Bangladesh. India's decision with respect to Jammu and Kashmir on August 5, the Citizenship Amendment Act (CAA), the National Register of Citizens and the Sino-Indian confrontation in Doklam are all part of the change process. There are also decisive Chinese actions with regard to accessing the Indian Ocean as exemplified by the so-called 'China-Pakistan Economic Corridor', the China-Myanmar Economic Corridor, the Bangladesh-China-India-Myanmar Economic Corridor and the BRI.

Power Rivalry. World powers are competing for influence and power in South Asia with the US and China making use of the economic tool. The rise in competition with China and Russia has been a challenge to the American power, influence and interests. Big-power politics is undermining globalisation, with the US disregarding global institutions, assaulting multilateralism, cutting financial aid to UN relief actions and engaging in trade policy predominantly based on bilateral approach. However, the Indo-Pacific region remains of vital, strategic significance for US's 'America First' policy. The Sino-Indian competition and cooperation also impacts the region. Essentially factors influencing geo-politics in the region are the growing international power and influence of China over all the South Asian capitals, the US prioritising the Indo-Pacific as a core geo-political interest and India's 'Neighbourhood First' policy.

Trends in Technology & Terrorism

Finding the technological safeguards to potential threat of terrorists using technology in the urban environment in India and the rest of South Asia will be a real strategic challenge and vulnerability in the years to come. Technology has proved to be instrumental in the rapid takeover of territory by the Islamic State(IS) in Syria and Iraq and its propaganda strategy included dissemination of violent videos, audios and narratives through social media. The IS's idea of 'Khorasan', as shown in a map released by them included territories of South Asia, such as, Bangladesh, Myanmar and India and it seems to be planning to expand into South-East Asia through South Asia.

While terrorism is not new to the region, South Asian countries have been witnessing increasing terrorist acts. Jaish-e-Mohammed, the terrorist organisation which claimed responsibility for the Pulwama attacks, operates freely in Pakistan which means that the intelligence and other security agencies of various South Asian countries are not united against the common threat. Terrorism in South Asia is fuelled by diverse factors ranging from global dynamics to local communal grievances. However, the significant factors are Information Technology (IT), finance, logistics, communication, organisation, leadership and recruitment.

Use of technology by terrorists is not new and Ramzi Yousef exploiting the technique of encryption in the 1993 World Trade Centre bombing amply brings out the same. Terrorists in fact use the internet for a variety of purposes including fundraising, operational planning and propaganda and the techniques used by terrorists are becoming more and more sophisticated. This includes the use of more advanced communications systems, drones and smart gadgets.

New, technology-enabled capacities include facial recognition, cloning, use of smart dust and so forth.

Recommendations

The region offers unprecedented opportunities for security-related cooperation however there is a need for a core, strategic, geo-political mechanism to formulate reliable, intelligence-based assessments and forecasts for South Asia. One model could be with Pakistan leading the effort in tackling the terrorist organisations in South Asia such as the Islamic State-Khorasan, based on the model of late Maj Gen Qassem Soleimani.

The important, geo-strategic situations unfolding in South Asia are the US troop withdrawal from Afghanistan, which will most likely lead to instability in the region and impact India, China and Russia, the supposed, unprecedented challenge to the social order in India, post the amendment to Article 370 and the passing of CAA and China's growing influence in South Asia.

In light of the above, the following is recommended –

- Continue to broaden and strengthen partnership with the US, especially in the field of technology, to combat the threat of terrorism in South Asia.

- Enhance information exchange at the regional level by initiating engagements between the Defence Ministers, Home Ministers, chiefs of law-enforcement agencies and the intelligence community.

- Include conferences of the Chiefs as part of military-to-military diplomacy.

- Enhance the cyber and other technological capacities of the military and other security forces.

- Identify common strategies and laws for South Asian States for counter-terrorism.

- Network with think tanks for exchange of data and expertise. It is important to note how and who think tanks influence.

The next probable visit of the Indian COAS to Nepal is an opportunity to develop a cooperative and collaborative approach to South Asian security and technology connectivity, imperative for the new South Asian order.

Sub-Theme 14: Rise of Non-State Actors

Dr. C Christine Fair
Provost's Distinguished Associate Professor Georgetown University, United States

Addressing the topic, the speaker - Dr. C Christine Fair - focused primarily on the LeT and a few other Pakistan supported terrorist organisations. She said that the terrorist groups she worked on, did not operate through the cyberspace and that the way they communicated and grew their membership was through face-to-face meetings and publications.

The LeT is the most favoured terrorist group of the Pakistani State and the group forms a part of the Order of Battle for the Pakistan Army as it is different from every other militant or terrorist organisation on Pakistan's payroll. The LeT is at odds with *Deobandi* organisations, which comprises virtually all militant organisations except the Hizb-ul-Mujahideen, over which, the Jamaat-e-Islami exerts control. The *Deobandis* rely upon the network of *Deobandi madrassas* and mosques for raising of human and financial capital. While the *madrassas* might or might not act as primary factories for recruitment of terrorists, the *Deobandis* do rely upon their *Ulema* to make pronouncements that justify their actions. The *Deobandis* are the largest cluster of terrorists in Pakistan and the difference between LeT and the *Deobandis* is as given below -

- ***Organisational Structure***. The LeT has hierarchical structures that reflect the State's relationship with them, while the *Deobandi* groups have a very flat organisational structure. Though a hierarchical organisation is ordinarily susceptible to leadership decapitation, the LeT does not even have to undertake leadership changes to make itself immune to it, given the impunity with which it operates, making such a decapitation highly unlikely. The *Deobandis* operate like a network-of-networks, with the result that even if one cell is neutralised, the rest of the organisation still functions. The *Deobandis* have such a structure because, at times, the State turns against some of these groups even if it is working closely with other *Deobandi* groups.

- ***Perpetration of Violence***. The *Deobandis* are inherently sectarian and these groups have joined the IS to kill Shias and Alawites even before the caliphate had been declared. The LeT is anti-sectarian and anti-communal while operating inside Pakistan, firmly opposing the *Deobandis*' practice of declaring Muslims *takfir* (excommunicating a Muslim) and thereafter, *Wajib-ul-qatl* (deserving to be murdered). While the LeT espouses violence outside Pakistan, it does not permit the same inside Pakistan, being the lackey of the State's security agencies. This has made the LeT useful both internally and externally. To date, no attacks inside Pakistan have been attributed to LeT and that is why Pakistan is so unrelenting on retaining LeT and promoting it through Jama'at-ud-Da'wah and Falah-e-Insaniat Foundation (FIF). To further this aim, the Pakistani State has deprived Sindh, which had a significant Hindu population, of public services and then allowed FIF to function, with the explicit goal of converting Hindus.

The LeT and the Pakistan Army recruit very similar human capital and data analysis shows that the LeT selects the best of the lot, since their recruits have been consistently better educated than the population they were drawn from. The recruitment process is not merely about training and then tapping the recruits for missions. In fact, there is a constant back-and-forth and vetting at every level of additional training and only the best are selected.

The LeT is very particular about who gets selected as it is about converting to the Ahl-e-Hadith interpretive tradition of Islam. These recruits are bureaucratic entrepreneurs who want to be deployed and attain *shahaadat* (martyrdom) and seek ways to improve and become eligible for the same. The LeT has two missions – *da'wah* (proselytism) and *jihad*, former being crucial to the domestic politics of this organisation. In India, while *jihad* may be priority, in Pakistan it is *da'wah* and the selected recruits are used to tap into the rest of the family for support.

Individuals join LeT and other terrorist organisations, despite not being religious zealots, in fact, many are ordinary boys who are bored and want to serve a bigger mission. They have a taste for violence and are disgusted by the decadence in their families. These people influenced by the LeT often get offended by the relatively luxurious life led by their families and the same becomes evident, in the advice they give to their family members regarding how to dress, how to behave with women and so forth. Many come from families which had members both in the Pakistani Army and the LeT, which is not surprising given the overlap of the districts in the Army and the LeT recruitment. Akin to the US Army's 'Buddy Team Enlistment Option', in many cases, the individual joins with at least one other associate and in such cases, they are likely to perform better. The motivation to join the LeT, hence, could be visualised as a three-dimensional space where one dimension is geography because the angle of Partition is brought in, the other is personal aspiration and finally there is devotion.

Mothers have a very important role and there is a different kind of motherhood that is being promoted. A woman takes pride in being the mother of a *Shaheed* (martyr) and does not want her son to come back as a *ghazi* (veteran) and this "macabre social capital' is being exploited by the LeT. Additionally, the mothers want their sons to intercede for them in heaven because there was a belief that if one dies in combat as a *shaheed*, he is allowed to bring 70 family members to heaven with him. Thus, persuading the mother is pivotal to the recruitment

process and the LeT puts in a lot of effort into cultivating mothers, since if the mother is not won over, she would spoil the recruitment-pool of the entire neighbourhood.

The LeT propagates that it is defending Muslims from occupiers and while it might sound like a religious argument, it is a political argument being made to reclaim a political status that Muslims used to have. The LeT believes that Islam fell into political decline when Muslims stopped waging *jihad*. Hence, Muslims in general and Pakistan in particular, can reclaim their political status and worthiness in the international system by waging *jihad*.

The LeT today, is ripe for leadership decapitation and perhaps that is the reason why Hafiz Saeed is always going into protective custody or jail. There is also a possibility that the JeM would replace the LeT in the operations for the time being, given Pakistan's own efforts to defeat the Pakistani Taliban, as also, the peace deal in Afghanistan where the Deobandi groups are going to be critical of Pakistan in securing its final victory in Afghanistan.

Finally, sub-conventional deterrence is very important to Pakistan despite its Army and the nuclear deterrence since the Army cannot win wars against India and nuclear weapons cannot be used. Proxy warfare is, hence, the only tool remaining. Thus, India also needs to start talking about sub conventional deterrence and not limit its options to conventional deterrence.

Sub-Theme 15: The Salience of Technology and Social Media in Hybrid Operations

Dr. Ajai Sahni,
Executive Director, Institute for Conflict Management, India

Beginning by briefly addressing the challenges in the grey zone, the speaker- Dr. Ajai Sahni- mentioned that he preferred the term 'unrestricted warfare' and said operations are not purely a military affair. These are national and institutional challenge which the system and government are not capable of responding to, as they not only lack the institutional framework but also because the institutions are being eroded by patterns of authority which are tribal and individualistic in orientation, the world over. Those who conceptualised the

idea of ‘unrestricted warfare’ were thinking of a civilisational war which would endure till the time the adversarial civilisation was destroyed. While grey zone and hybrid warfare seem to suggest a beginning and end, unrestricted warfare has the following characteristics –

- No limits of morality, scruple or value.
- No limits on the instrumentalities that may be employed.
- Indeterminate time-frames.
- Blurring of distinction between the civilian and the war-fighter.
- Omnipresence of the battlefield.
- Ambiguity - Such was the level that many target States often celebrated the very factors that were destroying them.

Technology has become a very important and integral component of the way we function and live. We are looking at an accelerating technological treadmill and unless we keep pace with the technological advancements, we would be thrown off the system and be left behind.

When we talk of terrorism and social media, the assessments are largely hysterical, lacking sobriety, information and understanding. There is a need to distinguish between the message and the medium, which are two different components in social media. The message is the most powerful component, alongside the social and the political contexts which also play key roles. This is amply brought out by the spread of Christianity. The Roman Empire banned Christianity for 300 years, however, within 50 years of being legalized, it became the state religion of the empire. Thus, an idea in a particular environment will find its medium and social and political context dictates that to control the population something was required, hence, Christianity became that force. Thus, it is not the medium which is important but the message and many of us exaggerate the importance of social media. The importance of social media is exaggerated because it is not understood properly, which is evident in responses such as cutting off access to it. Social media presents as much an opportunity for the adversary as for the defender but many times because we do not comprehend it and cannot manage it, thus, we think of shutting it down or banning it.

Cyber radicalisation in today’s world of social media connectivity has become a standard whipping boy. However, radicalised individuals engage in a direct, seeking behaviour online; engage with terrorist websites/ propaganda material; and thus it is not cyber-radicalisation but cyber-mobilisation or cyber-recruitment which is actually taking place. The base-problem is that, mindsets are being created in the conventional social circumstances and environments, which lead them to engage through the internet.

Terrorists use the social media to propagate their cause by twisting stories leading to the inability of the young to distinguish between real and fake news. However, fake news is not a crisis of social media, it is just being carried by social media and there is a comprehensive, enveloping ecosystem of political falsification that is adding fuel to fire. Lies are not just being spread by terrorists but also by those who hold State authority, thus leading to a loss of faith on institutions and people.

We underestimate the 'social' in social media with emphasis largely being on the technical nature of the media since it is easier to talk about them. There is a need to focus on the 'social' in social media. The fact that there are relatively a miniscule number of Indian Muslims joining IS when compared to many of the European countries, requires us to study the social and local dynamics leading to this situation and not so much the impact of social media since it exists at all these places.

Given the scale of social media, controlling it might look daunting at first sight especially if our response mechanisms remain primitive. However, control is already being exerted by the social media platforms themselves wherein between August 2015 and December 2018, Twitter suspended 1.4 million terror linked accounts and as per the UK government on an average the platforms remove about two thirds of the terrorist content within two hours of it being identified as such. Thus, there is much that is being done by the social media platforms despite governments always wanting to get more and more powers to control social media, which usually is due to their lack of understanding of the capabilities of social media and measures to harness them.

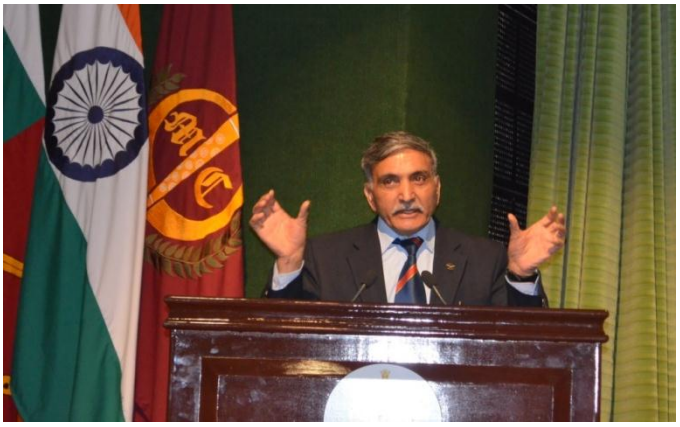
Monitoring of the digital presence of terrorist groups can actually prove to be a force multiplier for the states and research organisations. AI could be used to generate advance warning data based on social media activity and the said data can be used to intervene, misdirect or contain responses. In J&K, where social media is being used to generate flash mobs wherever operations are being conducted by the Security Forces, monitoring using AI based tools could generate data about these in real time and the same could be used to calibrate our response. The State thus, is better suited to exploit the medium than the non-state actors. However, it is the State's lack of capability, competence and imagination in understanding the nature of subversive discourse ongoing in social media, that restricts it from devising tools to intervene in the same and exploiting social media to its advantage.

There is a need to understand the nature of the content and narrow the gap between the pace of technological transformation and one's reactions. This has to begin at the level of policy, which is most difficult, since adaptations by professional organisations can occur overnight. There is a need to change the reaction-time and adopt a governance model where individuals are given responsibilities as per their core competencies, only then can we rise up to combat the menace of terror on social media in a systematic manner and exploit it to our advantage.

Session IV : Chair and Panellists of with Director, CLAWS

CLOSING REMARKS

CLOSING REMARKS



Lt Gen (Dr.) VK Ahluwalia, PVSM, AVSM, YSM, VSM (Retd)**
Director, CLAWS

Delivering the Concluding Remarks - the Director, CLAWS-Lt Gen (Dr.) VK Ahluwalia, PVSM, AVSM**, YSM, VSM (Retd) - mentioned that every age has had its own wars and its own forms of warfare. Warfare is a prolonged and protracted process which gives the guidelines for a war to be executed; whereas war is a part of the warfare. Pointing to non-kinetic forms of warfare, such as economic sanctions, energy resources being withheld, etc. the Director brought out the incongruity in the nature of warfare being defined as interactive, destructive, violent and political, given that the political objectives of the country were being achieved. However, today, the wars have also acquired non-kinetic, non–contact character, which do not necessarily result in physical destruction and violence. Therefore, there have been varied opinions among the panellists and participants on whether nature of warfare is also changing.

Giving his views on various topics that were deliberated upon during the course of the Conclave, the Director stated that he agreed with the view that it was easier to talk about the trends in the ongoing conflicts and perhaps, the immediate future, but very difficult to crystal gaze into the distant future. On the issue of insurgency, he mentioned that in addition to the revolutionary form of insurgency, there were separatist, secessionists, reformist, proxy-based and commercial forms; each one of which has a different centre of gravity and different method of managing and resolving it. Quoting from Rear Admiral JC Wylie's book, *Military Strategy: A General Theory of Power Control*, regarding the inevitability of war, the Director emphatically stated that given India's myriad internal and external security challenges, it needed to be prepared for the full spectrum of conflict – right from conventional to information, hybrid and grey zone, with special emphasis on the latter. On the point regarding the need to have 'Information Age, integrated force structures,' he mentioned that it must meet the conventional and other requirements of the future conflicts, which are unique and different in each region.

Focusing next on what was said about the 'indirect approach', the Director elaborated on Kautilya's *Arthashastra*. He remarked that what was deliberated upon during the Conclave was already said 2,300 years ago by Kautilya – a military strategist, scholar and advisor to the Mauryan Empire. In this regard, he mentioned the four forms of warfare expounded by Kautilya –

- ***Mantrayuddha***. This refers to war by counsel where diplomatic acumen plays a key role in winning wars.

- ***Prakasayuddha***. This is open warfare i.e. a set-piece battle at a specified time and place.

- ***Kutayuddha***. This refers to concealed warfare, primarily using psychological warfare, including instigation of treachery in the enemy camp.

- ***Gudayuddha***. This is clandestine warfare aiming to win the war without waging it, using covert means such as assassination and use of double agents.

The Director defined hybrid warfare as a blend and cumulative effect of political, economic, military (conventional and sub-conventional), informational, criminal and psychological means. There has been a progressive increase in the intra state conflicts since the late 1950s, when the after decolonisation was in its final phases. Conventional way of warfighting is not the way to combat unconventional, asymmetric and irregular forms of warfare. Therefore, there is a need to develop expertise in the new domains. On the point that only organisational change reflected transformation, he opined that transformation, first and foremost, was reflected by a change in the mindset, further leading to changes in the doctrines, strategy, warfighting concepts, organisational structures, as also, training and human resource. He agreed with the thought of a speaker that 'we seem to stretch old concepts to meet new challenges.'

With regard to what was spoken on the concept of victory, the Director mentioned that given the blurring of lines between war and peace, there could be no single, universally accepted concept of victory. He further opined that in the current day and age, there was no decisive and enduring victory; and each form of warfare had a different concept of 'success. Additionally, he also highlighted the salience of influence operations. With regard to the point made on 'Nexus7', he expressed the need for more clarity on whether the said intelligence programme was more quantitative, not taking into account social and behavioural sciences, as also, the success of the programme. Reflecting on the talk vis-à-vis space warfare, he remarked that the distinction between militarisation and weaponisation of space, as brought out by the speaker, was much required, as also, the kind of structures that would be required in future. Regarding the use of data as a strategic weapon, the Director stated that India and the entire sub-continent, lacked the kind of empirical data required to carry out analysis and thus use data as a strategic weapon. On technology and doctrine, the Director recounted a joint seminar of CLAWS with US Air War College, held in 2018, where a Chinese Professor mentioned that while the doctrine is formulated first in the US and the technology follows, the Chinese first look at the technology and then formulate the doctrine. The Director remarked that he was unsure of the sequence in India, but it could be the case of formulation of doctrine as per available technology, which was not state-of-the-art either. While calling the discussion on 'integrated low-cost swarms versus monolithic complex systems' thought-provoking, he emphatically stated that India lacked a focus on human capital.

The Director addressed the point made by the speaker that artillery beyond the range of 40 km would require precision-guided munitions. He mentioned that that the artillery should continue to make efforts to remain accurate even at much lesser ranges, especially in the mountainous terrain where accuracy gets affected due to frequent changes in the weather conditions between each valley. Giving examples of mountainous regions in India, the Director mentioned that artillery might require precision-guided munitions beyond even 15-20 km. Mentioning how urbanisation is going to pose a big challenge to India, South Asia and Africa, he said that the urban population in India had increased by 74 per cent in the period from 1991 to 2011. Further, a 54 per cent growth was expected in urban population

from 377 million in 2011 to more than 516 million in 2031. In the context of the point that was made about the mothers and the families in Pakistan being the motivation for terrorists, the Director referred to a national seminar held at CLAWS on the topic 'Mapping of Perception in Jammu and Kashmir', in which a professor from the Tata Institute of Social Sciences revealed the result of a survey she had carried out on students from the Kashmir Valley. It revealed that mothers had maximum influence on them, followed by teachers, friends and religious leaders.

Modifying a quote by Gen Joseph Dunford, the 19th Chairman of the Joint Chiefs of Staff of the US, where he stresses on the need to 'keep pace with the speed of war', the Director highlighted 'the need to keep pace with the speed of change' lest we 'lose the ability to compete'.

On behalf of the Indian Army and CLAWS, the Director thanked all the distinguished panellists for their presentations and the participants for their thought provoking questions. He also thanked and appreciated the overwhelming support from the friendly foreign countries for the Seminar. The Director stated that given India's peculiar set of security challenges, both internal and external, technology alone might not provide all the solutions. While there is a need for an Information Age manoeuvre force, the focus on territorial integrity and to fight the proxy war in J&K must not be lost sight of.

PRAGYAN KALEIDOSCOPE: DAY TWO

VCOAS arriving to deliver the Special Address

Director's tete-a-tete with Students

Captivated Audience

Continuing the Discussion

Chai pe Charcha

Intrigued and Fully Immersed Gathering

Compere at Work

Q & A Session

Ladies, Pragyan Gallery

Interactions Galore

CONCEPT NOTE

CENTRE FOR LAND WARFARE STUDIES, NEW DELHI

INDIAN ARMY INTERNATIONAL SEMINAR ON
CHANGING CHARACTERSTICS OF LAND WARFARE AND ITS IMPACT
ON THE MILITARY

04-05 March 2020

Manekshaw Centre, Delhi Cantt, New Delhi

CONCEPT NOTE

The strategic significance of land warfare in the history of conflict is rooted in a nation's resolve to achieve a decisive political outcome, the unique capacity to capture, occupy, hold terrain, to maintain a continuous presence where required and in the physical domain to control geographical areas and population. Whilst the character of land warfare remains embedded in the entire conflict spectrum, changes in methods and means are occurring at a very rapid pace. Changes in military warfare, which many military experts predict, will be a "military-technical revolution", bring unprecedented firepower, depth and transparency to the battlefield. The most significant developments for land warfare are simultaneity &non linearity, lethality & dispersion, volume & precision of fire, advanced technology, mass & effects, invisibility and detectability. These developments are driving adjustments in tactics, organisation, doctrine, equipment, force mix and methods of command & control. Modern conflicts display stark asymmetries between contending actors and are unforgiving to the unprepared.

The nature and character of wars is also being influenced by new concepts and technologies available to the protagonists. The global hotspots are throwing up trends and changes in the contours of future warfare. New forms of warfare like limited wars, proxy wars, asymmetric warfare, hybrid warfare, unconventional warfare, cyber warfare, space warfare and information warfare use all types of means including irregular forces and social media. There is a blending or blurring of distinction between the traditional state and non-state actors with capabilities which signify the domination of hybrid warfare in future battle. While the probability of full fledged conventional conflict between states or groups of states has been declining, the possibility of sub-conventional conflicts, ranging from intra-state conflicts to global terrorism is gaining prominence.

In the 21st century, the familiar form of warfare in which physical damage is meted out against the opponent's military forces and infrastructure has become only one form of attack. Instead, states are increasingly launching non-lethal attacks against an enemy's information systems - this is the rise of information warfare. Information warfare combines electronic warfare, cyber warfare and psychological operations into a single fighting domain and this will be central to all warfare in the future.

Cyber and Space Warfare have added new dimensions to war by making it real time and distantly controlled while eliminating collateral physical damage. Paradoxically, the more sophisticated the fighting force, the higher the likelihood of suffering from cyber attacks. Space based assets have also become pivotal to strategic security and play a critical role in

conduct of future land operations. Multifaceted information operations will become pivotal operational and strategic imperatives for land forces securing operational battlespace.

Important developments which have impacted land warfare in a significant manner are transparency due to all weather Intelligence, Surveillance and Reconnaissance (ISR) capability, the advent of long range accurate and precise fire systems, the mobility of forces in all terrain and the creation of non-state actors. ISR capabilities have transformed the situational awareness capability of land forces. With both sides able to obtain real time information, the battlefield transparency will pose its own challenges. The OODA loop will reduce; precision and lethality of weapons increase and a 24-hour battle become the norm.

The latest revolution to influence land warfare is in the field of Artificial Intelligence (AI) and Robotics. Innovations in weaponised AI have already taken many forms. AI has increasingly been integrated into the weapon systems of the world's leading militaries and some experts even argue that the greatest revolution in military affairs since the atom bomb is the advent of robotic warfare. AI could be repurposed to build lethal autonomous weapons - "Killer Robots", which can alter war forever.

Close support operations with standoff capability and helicopter operations in all terrain and time will improve manoeuvre capability. The advancement in the field of Combat UAVs has also revolutionalised land warfare. Time compression and speed will soon have battles that would be fought employing platforms such as hypersonic vehicles and missiles without having to actually go into the tactical battlespace.

All future wars in the Indian context will be fought in a nuclear environment where the tenets of nuclear warfare will form an integral part of planning and execution. The ability to use Tactical Nuclear Weapons will add to the complexity of operations and challenges to remain below the threshold.

Revolutionary changes are now resetting the rules the way land operations will be structured. War is now a national effort in all dimensions including the will of the people.

Objectives of the Seminar

The seminar aims to achieve the following objectives:-

- To scan and evaluate the current and emerging trends in warfare, developing conflict spectrum and future battlefields.

- To provide an insight into the changing contours of warfare and their influence on landwarfare.

- To explore and understand the technological advancement shaping the future battlefields.

- To assess the embryonic influence of third dimension, hypersonic precision long-range missiles and state of art unmanned aerial vehicles on landwarfare.

- To construct conventional operations under the backdrop of nuclear weapons in future land battles.

- To evaluate the dynamics of hybrid war and challenges posed to future battlefields by non- state actors exploiting technology and social media.

Themes

In order to address the subject '**Changing Characteristics of Land Warfare and its Impaction the Military**', the seminar will deliberate upon four themes with apposite sub-themes as mentioned below:-

- Evolving Warfare: An Insight into the Changing Realm.
- The Technological Revolution - A Seminal Challenge.
- Transformation in the Battle Spaces.
- Hybrid/Sub-ConventionalWarfare.

Methodology

Speakers representing a wide cross-section of domain expertise both from India and abroad have been invited to present papers and to share their perspective on the subject.

Conduct of Seminar

The seminar will be conducted at the Manekshaw Centre, New Delhi over two days under the aegis of the Centre for Land Warfare Studies(CLAWS), a well acclaimed Think Tank based at New Delhi.

Inaugural Session

The inaugural session is proposed to be addressed by the following dignitaries from India:-

- Hon'ble Raksha Rajya Mantri.
- Chief of the Army Staff.

Session One: Evolving Warfare - An Insight Into the Changing Realm

This session will analyse the emerging trends in warfare and crystal gaze into the future battlefields. It will also focus on changing contours of land warfare and strengths and vulnerabilities of the forces. The speakers will focus on the following issues:-

- Military Futures - Prospects and Possibilities.
- Changing Character of Conflict: Imperatives of Transformation.
- Trends in Warfare: Concept of Victory and Strategic Conquest.

Session Two: Technological Revolution - A Seminal Challenge

This session will examine the way technological revolution is influencing and warfare. The speakers will focus on the following issues:-

- Salience of Information Warfare in Multi-Domain Operations.

- Cyber as a Tool of Warfare : Paradigm Shift.
- Drivers : Space Command to Space Force.
- AI and Robotics: From Concept to Delivery.

Session Three: Transformation in the Battlespaces

The speakers will focus on the following issues:-

- A New Strategy for a Changing Era.
- Firepower: The Impact of Long-Range Vectors & Precisionary.
- Special Forces: A Force Multiplier for Land Operations.
- The Nuclear Environment to include the Impact of Hypersonics.

Session Four: Hybrid/Sub-Conventional Warfare

The speakers will focus on the following issues:-

- Ground Forces Operations in a Grey Zone Environment.
- Technology & Urban Warfare.
- Rise of Non-State Actors.
- The Salience of Technology and Social Media in Hybrid Operations.

PROGRAMME

PRAGYAN CONCLAVE 2020 INDIAN ARMY INTERNATIONAL SEMINAR

CHANGING CHARACTERISTICS OF LAND WARFARE AND ITS IMPACT ON THE MILITARY

04-05 MARCH 2020 AT MANEKSHAW CENTRE, DELHI CANTT

PROGRAMME

DAY ONE : 04 MARCH 2020

0900 - 0945hr	**Tea & Registration**	
INAUGURAL SESSION		
0945hr	Arrival of the Hon'ble RRM	Received by the COAS
0950 - 1010hr	Keynote Address	Hon'ble RRM
1010 - 1015hr	Presentation of CLAWS Publications to the Hon'ble RRM by the COAS & Patron, CLAWS	
1015hr	Departure of the Hon'ble RRM	
1015 - 1035hr	Inaugural Address	COAS
1035 - 1055hr	Award Presentation to Winners of Field Marshal Manekshaw Essay Competition on National Security by the COAS & Patron CLAWS	
1055 - 1130hr	Tea & Interaction	
SESSION I : EVOLVING WARFARE – AN INSIGHT INTO THE CHANGING REALM		
1130 - 1140hr	Opening Remarks by Chair	Lt Gen (Dr.) VK Ahluwalia, PVSM, AVSM**, YSM, VSM (Retd)
1140 - 1200hr	Military Futures - Prospects and Possibilities	Lt Gen Raj Shukla, YSM, SM
1200 - 1220hr	Changing Character of Conflict: Imperatives of Transformation	Mr Lazar Berman, Israel
1220 - 1240hr	Trends in Warfare: Concept of Victory and Strategic Conquest	Maj Gen AKM Abdullahil Baquee, RCDS, ndu, PSC, Bangladesh
1240 - 1310hr	Q & A	
1310 - 1400hr	Lunch & Interaction	
SESSION II : THE TECHNOLOGICAL REVOLUTION – A SEMINAL CHALLENGE		
1400 - 1410hr	Opening Remarks by Chair	Lt Gen (Dr.) Rajesh Pant, PVSM, AVSM, VSM (Retd)
1410 - 1430hr	Salience of Information Warfare in Multi-Domain Operations	Brig Simon Goldstein, MBE, ADC, UK; Col John Kendall, UK
1430 - 1450hr	Cyber as a Tool of Warfare : Paradigm Shift	Ms Sharon Weinberger, USA

1450 - 1510hr	Drivers : Space Command to Space Force	Gp Capt Ajey Bishwanath Lele (Retd)
1510 - 1530hr	AI and Robotics : From Concept to Delivery	Lt Col PJ Anand Kumar (Retd)
1530 - 1600hr	Q & A	
1600hr	**Tea & Dispersal**	

DAY TWO : 05 MARCH 2020

0900 - 0915hr	Special Address	VCOAS
SESSION III : TRANSFORMATION IN THE BATTLE SPACES		
0915 - 0925hr	Opening Remarks by Chair	Lt Gen AK Singh, PVSM, AVSM, SM, VSM (Retd)
0925 - 0945hr	A New Strategy for a Changing Era	Lt Gen D S Hooda, PVSM, UYSM, AVSM, VSM** (Retd)
0945 - 1005hr	Firepower : The Impact of Long Range Vectors & Precisionary	Dr. Jack Watling, UK
1005 - 1025hr	Special Forces : A Force Multiplier for Land Operations	Brigadier H P Ranasinghe, RWP, RSP, ndc, Sri Lanka
1025 - 1045hr	The Nuclear Environment to include the Impact of Hypersonics	Lt Gen Amit Sharma, PVSM, AVSM, VSM (Retd)
1045 - 1115hr	Q & A	
1115 - 1145hr	High Tea	
SESSION IV : HYBRID/ SUB CONVENTIONAL WARFARE		
1145 - 1155hr	Opening Remarks by Chair	Lt Gen Subrata Saha, PVSM, UYSM, YSM, VSM** (Retd)
1155 - 1215hr	Operations in a Grey Zone Environment	Lt Gen (Dr.) Rakesh Sharma, PVSM, UYSM, AVSM, VSM (Retd)
1215 - 1235hr	Technology and Urban Warfare	Maj Gen Binoj Basnyat (Retd), Nepal
1235 - 1255hr	Rise of Non-State Actors	Prof C. Christine Fair, USA
1255 - 1315hr	The Salience of Technology and Social Media in Hybrid Operations	Dr. Ajai Sahni, Delhi
1315 - 1345hr	Q & A	
1345 - 1355hr	Concluding Remarks	Director, CLAWS
1355hr	Lunch & Dispersal	

BIO DATA OF GUEST SPEAKERS, CHAIRPERSONS & PANELLISTS

BIO DATA OF GUEST SPEAKERS, CHAIRPERSONS & PANELLISTS

SHRI SHRIPAD YESSO NAIK
HON'BLE RAKSHA RAJYA MANTRI (MINISTER OF STATE FOR DEFENCE)

Shri Shripad Yesso Naik is the Hon'ble Union Minister of State for Defence, Union of India. Educated at University of Mumbai, he holds a Bachelor's of Arts degree. He has held a number of positions from 1984 onwards, and prior to his present appointment he was the Union Minister of State (Independent Charge), Ministry of Ayurveda, Yoga & Naturopathy, Unani, Siddha and Homoeopathy (AYUSH). He has also been the Union Minister of State for Health and Family Welfare and is an MP from North Goa. He is also involved in a number of social and cultural activities in Goa and Maharashtra and is in the committee of a number of educational institutions and is also a member of the Central Advisory Board of Archaeology and the National Shipping Board.

GEN M M NARAVANE, PVSM, AVSM, SM, VSM, ADC
CHIEF OF THE ARMY STAFF (COAS), INDIAN ARMY & PATRON, CLAWS

An alumnus of NDA and IMA, he was commissioned in The Sikh Light Infantry Regiment in June 1980. He has commanded a Rashtriya Rifles battalion, raised an Infantry Brigade, was Inspector General Assam Rifles (North) and has commanded the prestigious Strike Corps. His staff assignments include tenures as a Brigade Major of an Infantry Brigade, Defence Attaché at Yangon, Myanmar, an instructional appointment in the Higher Command Wing, besides two tenures at the Integrated Headquarters of MoD (Army), New Delhi. After successfully commanding the Army Training Command, Shimla and the Eastern Command in Kolkata, he held the appointment as Vice Chief of the Army Staff before assuming the appointment of the Chief of the Army Staff on 31 Dec 2019.

LT GEN S K SAINI, PVSM, AVSM, YSM, VSM, ADC
VICE CHIEF OF THE ARMY STAFF (VCOAS), CHAIRMAN, BoG, CLAWS

Lt Gen S K Saini was commissioned into 7 JAT in June 1981. He has also commanded his Battalion, a Mountain Brigade, a Counter Insurgency Force in J&K, Corps in the Western Theatre and the Southern Army Command.

The General Officer is a graduate of the Army Command and Staff Course at the Staff College, Camberley in UK and has studied at the Royal College of Military Science, Shrivenham, UK. He is also a graduate of the Higher Command Course and the National Defence College, Bangladesh. He has also served as the Deputy Chief Military Personnel Officer in the UN Mission in Iraq-Kuwait.

Previously, he has served as Brigadier General Staff (BGS) of a Corps deployed in J&K. In his last appointment as GOC-in-C, Southern Command, he steered transformation of the Operational Philosophy of the Southern Army to overwhelm the emerging threats and validation of many new concepts during training exercises.

LT GEN (DR.) VK AHLUWALIA, PVSM, AVSM, YSM, VSM, (RETD)**
DIRECTOR, CLAWS

After a career that spanned over 40 years in the Indian Army, he retired as the Army Commander, Central Command in 2012. Thereafter, he served as a Member, Armed Forces Tribunal, Jaipur-Jodhpur Benches. He commanded an Infantry Brigade in Uri Sector, Mountain Division in Kargil and Corps in Leh - Ladakh Sector. While commanding the Division in Kargil, his Division was awarded the BNHS National Green Governance Award 2005 by the Prime Minister of India, for conceiving and implementing the unique strategic concept, 'Operation Green Curtain'. He was also the first Indian Brigadier to attend the National Defence Course, at Dhaka.

A Doctorate in 'Internal Security and Conflict Resolution', he has also authored a book, 'Red Revolution 2020 and Beyond' and edited cum contributed in, 'Surprise, Strategy and Vijay: 20 Years of Kargil and Beyond'.

Currently, he is the Director, CLAWS.

LT GEN RAJ SHUKLA, YSM, SM
DIRECTOR GENERAL, PERSPECTIVE PLANNING, INDIAN ARMY

In his career spanning over three decades, the officer has commanded a Medium Regiment in the Eastern / Desert Theatres, an Infantry Brigade in Counter Insurgency Operations, an Infantry Division along the Line of Control and a Corps along the Western Borders.

He has also been the Commandant of Indian Army's premier training establishment and prestigious think tank - the Army War College.

He is currently the Director General, Perspective Planning in Army Headquarters.

LAZAR BERMAN
FELLOW, JISS, ISRAEL

Mr. Berman is currently a fellow at the Jerusalem Institute for Strategic Studies (JISS) and is the Head of Joint Learning in the IDF General Staff/J3, Dado Center for Interdisciplinary Studies. He was the foreign and defense policy research manager at the American Enterprise Institute in Washington DC and news editor of The Times of Israel. Mr. Berman commanded a Bedouin unit during his active IDF service. He taught at Salahuddin University in Erbil in Iraqi Kurdistan and studied the Kurdish language. He holds an MA in military operations from Georgetown University's Security Studies Program, where he wrote his thesis on IDF innovation. He has published in The Journal of Strategic Studies, Small Wars Journal, Weekly Standard, Mosaic and other journals.

MAJ GEN AKM ABDULLAHIL BAQUEE, RCDS, ndu, PSC
BANGLADESH ARMY

Maj Gen Baquee has held a variety of command, staffand instructional appointments. He has been an Instructor, Senior Directing Staff (Army) at National Defense College, Mirpur. He has commanded an Infantry Battalion, an Infantry Brigade and an Infantry Division. He has previously served as Chief of General Staff's Coordinator twice at Army Headquarters General Staff Branch and as Deputy Assistant Military Secretary in Military Secretary's Branch. He also served as Commandant, School of Infantry and Tactics and Defence Services Command and Staff College. He has served in UN peacekeeping missions from 1999-2000 as Operation Officer in UNIKOM, Kuwait and as Deputy Chief of Joint Military Assessment Cell in UNMIS, Sudan from 2007-2008.

LT GEN (DR.) RAJESH PANT, PVSM, AVSM, VSM (RETD)
NATIONAL CYBER SECURITY COORDINATOR, GOVERNMENT OF INDIA

Lt Gen (Dr.) Rajesh Pant (Retd), an internationally recognised cyber security expert, is tenanting the prestigious appointment of National Cyber Security Coordinator in the National Security Council Secretariat of India. He holds a PhD degree for his research in the field of Information Security metrics. He is also an MTech from IIT Kharagpur, MPhil from Madras University and Master of Management Studies from Osmania University. He served in the Army Signals Corps for 41 years and prior to this appointment, he was the head of the Army's Cyber Training establishment for three years. He brings to the table an interesting mix of military operations, academic excellence, corporate governance and cyber security wisdom.

BRIG SIMON GOLDSTEIN, MBE, ADC
DEPUTY COMMANDER RESERVES, 6TH (UNITED KINGDOM) DIVISION

Brig Simon Goldstein joined the Honourable Artillery in 1987 and joined 21 (Artists Rifles) in 1990, commissioning in 1992. He spent most of his time at regimental duty and commanded Exeter UOTC from 2005 - 2007 and London RTC in 2008. He served as Colonel Reserves in MOD, followed by AD Trg Ops (Reserves) at ARTD and most recently on the staff at RCDS where he attended the one-year course at the same time. He has operational experience in Bosnia, Kosovo, the Former Yugoslav Republic of Macedonia and Afghanistan and has worked for 6 months at SHAPE in Mons. He was awarded the MBE in 2005.

COL JOHN KENDALL
DEPUTY COMMANDER, 1 INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE BRIGADE, BRITISH ARMY

Col John Kendall was commissioned into the Royal Signals Territorial Army in 1995. Currently the Deputy Commander of a specialist Brigade, Col Kendall is responsible for innovation, technology and force development as well as overseeing the 2,500 Reservists. In civil life, he is a Strategic Analyst working with the UK and overseas governments on technology and military subjects.
Col Kendall has made extensive use of military history in both teaching tactics to junior officers and also using Historical and Scientific Analysis to inform operational-level problems.

SHARON WEINBERGER
GLOBAL FELLOW, WOODROW WILSON INTERNATIONAL CENTRE FOR SCHOLARS

Sharon Weinberger is the Washington DC bureau chief for Yahoo News and a Global Fellow at the Woodrow Wilson International Centre for Scholars. Previously, she was an executive editor at Foreign Policy magazine and before that, the national security editor at *The Intercept*. Her third book, published in 2017 by Knopf, is 'The Imagineers of War: The Untold Story of DARPA, the Pentagon Agency That Changed the World'. She has also held fellowships at the Radcliffe Institute for Advanced Study at Harvard University, MIT's Knight Science Journalism Program, the International Reporting Program at John Hopkins School of Advanced International Studiesand Northwestern University's Medill School of Journalism. She has written on military science and technology for the New York Times, the Washington Post, the Financial Times, Wired magazine, Nature, BBC, Discover and Slate, among other publications.

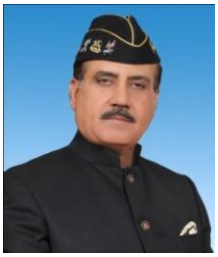
GROUP CAPTAIN AJEY LELE (RETD)
SENIOR FELLOW, MANOHAR PARIKAR - INSTITUTE FOR DEFENCE STUDIES AND ANALYSES

Gp Capt Ajey Lele (Retd), is a Senior Fellow at the Manohar Parikar - Institute for Defence Studies and Analyses, New Delhi. His areas of research include issues related to Weapons of Mass Destruction (WMD) and Strategic Technologies. He has obtained his masters in Physics and doctorate in International relations. He has contributed various research articles to national and international journals. He is the author of 'Asian Space Race: Rhetoric or Reality?' (Springer, 2013) and ' Mission Mars: India's Quest for the Red Planet' (Springer, 2014).

LT COL P J ANAND KUMAR, (RETD)
CHIEF TECHNOLOGY OFFICER, DATAVAL ANALYTICS PVT. LTD.

Lt Col PJ Anand Kumar (Retd) is an alumnus of National Defence Academy and was commissioned into the Corps of Engineers. He was specially selected to conceptualise and set up the AI & Robotics Lab at MCTE, which has evolved into a 'Center of Excellence' for the Indian Army. He was the station engineer at the Indian research station 'Maitri' in Antarctica from 2003 to 2005. He was also part of the project 'Battlefield Management System' at DGIS and was an instructor in AI, Robotics, GIS and Cyber Security in MCTE and CME. He is a Certified Ethical Hacker from EC Council and has completed his Cyber Law from Asian School of Cyber Law and Cyber Forensics from Gujarat Forensics Science University, Ahmedabad. Besides, he is certified in Remote Sensing and GIS applications from Indian Institute of Remote Sensing, ISRO. He is also certified in 'Deep Learning', 'Real-Time Cyber Threat Detection and Mitigation', 'Enterprise and Infrastructure Security' etc. Besides being the CTO of DataVal Analytics, he is also heading two cyber research centers in DSATM, Bengaluru and NGP Institute of Technology, Coimbatore.

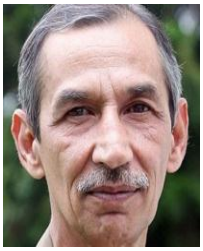
LT GEN AJAY KUMAR SINGH, PVSM, AVSM, SM, VSM (RETD)
DISTINGUISHED FELLOW, CLAWS



Lt Gen A K Singh (Retd) the erstwhile Lt Governor of the Andaman & Nicobar Islands and Puducherry, Ex GOC-in-C Southern Command has been an alumnus of NDA, Staff College Camberley, UK, Malinovsky Tank Academy, Moscow &the Higher Command & National Defence College courses.

The General has commanded the 7th Cavalry, a T-90 Tank Brigade, an Armoured Division and the most powerful Strike 1 (Corps) and has the distinction of conceiving and executing some of the largest ever manoeuvres in recent times. He was the Director General, Perspective Planning, where he drew up the long term perspective of the Indian Army. Presently, he is an Independent Director and Advisor with various firms/educational institutions including OP Jindal Global University. His edited book 'Military Strategy for India in the 21st Century' has been published recently.

LT GEN DS HOODA, PVSM, UYSM, AVSM, VSM (RETD)**
BOARD MEMBER, CYBER PEACE FOUNDATION



Lt Gen Hooda (Retd) is an alumnus of the prestigious Command and Staff College at Canada. He was selected as the first Chief Logistics Officer for the newly raised United Nations Mission to Ethiopia and Eritrea. During the massive earthquake of Jammu and Kashmir in 2005, he led the military's rescue and relief efforts in the Uri sector. As a Major General in Manipur, he led counterinsurgency operations in Manipur and South Assam. He was stationed in Jammu and Kashmir from 2012 to 2016, where he served first as a Corps Commander and then as the Army Commander of Northern Command. He is currently on the Advisory Board of Cyber Peace Foundation, an NGO dealing with cyber protection and training and on the Advisory Board of Cyber Security Research Centre at Punjab Engineering College.

DR. JACK WATLING
RESEARCH FELLOW, RUSI

Dr Jack Watling is a Research Fellow at RUSI, responsible for the study of Land Warfare. Jack has recently published detailed studies of the Future of Fires, Future Amphibious Operations, Allies in Multi-Domain Operations, the British Army & Strike Concept and Iran& Strategic Objectives and Capabilities. Jack's PhD examined the evolution of Britain's policy responses to civil war in the early twentieth century. Prior to joining RUSI, Jack worked in Iraq, Mali, Rwanda, Brunei and further afield, embedded with Iraq's Popular Mobilisation Forces and the Burkina Faso Army.

BRIG HP RANASINGHE, RWP, RSP, ndc
DIRECTOR OF OPERATIONS, SRI LANKA ARMY HQ

Brig Harendra Parakrama Ranasinghe was commissioned on 23 July 1987 and posted to the Gamunu Watch. Later, he voluntarily joined the Sri Lanka Army Special Forces Regiment in April 1990. He has commanded the01st and 2nd Regiments of Special Forces and has held the appointments as Commandant of Special Forces Training School, Center Commandant of Sri Lanka Army Special Forces Regiment and Commandant at Army Training School.

He has been the Commander of 571 Infantry Brigade and later, was the Brigade Commander of Sri Lanka Army Special Forces Brigade. He has served as the Defence Adviser to the Embassy of Sri Lanka in Washington DC, USA. He was the Brigadier General Staff of the Corps HQ North Central Province in 2019.

He has obtained Masters in Conflict and Peace Studies from University of Colombo and Master of Philosophy in Defence and Strategic Studies from University of Madras, India. He has graduated from National Defence College India. He has been decorated with gallantry awards of Rana Wickrama Padakkamaand Rana Sura Padakkama for three times in recognition of the bravery shown in the battlefield. He was awarded with the Purple Heart for physical injuries caused in the Battlefield. Currently, Brig Harendra Ranasinghe is the Director of Operations of the Sri Lanka Army Headquarters.

LT GEN AMIT SHARMA, PVSM, AVSM, VSM (RETD)
SCIENTIFIC CONSULTANT, OFFICE OF THE PRINCIPAL SCIENTIFIC ADVISOR TO GOI

Lt Gen Amit Sharma (Retd) served as the Commander-in-Chief, Strategic Forces Command. Born on Jul 04, 1956, in Mumbai, Lt Gen Sharma was commissioned in 45 Cavalry in December, 1976. Over the years he has held numerous command, staff and instructional appointments in all operational sectors including Counter Insurgency areas. During early years of service he has been General Staff Officer (Grade-1) of an Armoured Division and Directing Staff at the prestigious Army War College, Mhow. Later, he had the unique distinction of having served as Colonel Administration of an Infantry Division in Jammu & Kashmir, Colonel General Staff of a Mountain Division in the Eastern Sector and Brigadier General Staff of a Strike Corps. Lt Gen Amit Sharma has also served as Director Long Term Force Structuring, Headquarters Integrated Defence Staff and was the Defence Attaché at Embassy of India, Paris, where he was responsible for Army and Naval cooperation with France, Belgium, Netherlands and Luxembourg. He has commanded an Armoured Regiment, an Independent Armoured Brigade in the Western Deserts, an Infantry Division in a Strike Corps and the Strike Corps in the Southern Theatre.

LT GEN SUBRATA SAHA, PVSM, UYSM, YSM, VSM (RETD)**
MEMBER, NATIONAL SECURITY ADVISORY BOARD

Lt Gen Subrata Saha (Retd) from the Assam Regiment is currently a Member of the National Security Advisory Board. He retired as the Deputy Chief of Army Staff and post retirement he was the Founding DG of the Society of Indian Defence Manufactures. He is a distinguished fellow of the Centre for Joint Warfare Studies. His academic record includes the rare DISTINGUISHED grading on Junior Command Course. He is the only Officer who has the distinction of attending the Staff College Camberley (UK) and United States of America Army War College. He was adjudged Best Overseas Student at Staff College Camberley and awarded the Gold Medal at Higher Command Course. He has previously served as 15 Corps Commander in Kashmir, Additional Director General Military Operations, commanded a Division in Strike Corps and has operational experience in Kashmir, Assam, Punjab and the Siachen Glacier. He also served as Deputy Regional Commander United Nations Mission in Angola in 1996-97.

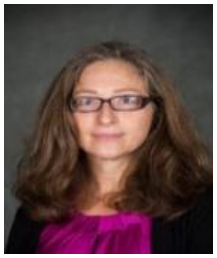
LT GEN (DR.) RAKESH SHARMA, PVSM, UYSM, AVSM, VSM (RETD)
DISTINGUISHED FELLOW, CLAWS

Lt Gen Rakesh Sharma (Retd) was commissioned into 5/11 Gorkha Rifles on Jun 11, 1977 and retired as Adjutant General of the Indian Army on Mar 31, 2017. The General Officer has had command experience spanning the entire mosaic, covering all theatres. Having commanded his battalion in the North East, he commanded an infantry Brigade in Western Theatre and an Infantry Division deployed on the Line of Control in the Northern Theatre. He has also commanded a Corps in Ladakh. He was part of Indian Army Training Team at IATT Botswana, Africa for three years and Director Strategic Studies (Global) at Army Headquarters. The General Officer has been a Research Scholar at Institute for Defence Studies and Analyses, New Delhi and did MPhil from the University of Madras and a Doctorate in Defence Studies from Meerut University.

MAJ GEN BINOJ BASNYAT (RETD)
INDEPENDENT POLITICAL & SECURITY ANALYST, NEPAL

An alumnus of National Defence College, New Delhi, Maj Gen Basnyat, Order of Suprabal Jana Seva Shree; Order of the Lion of Finland; Order of Cross of Germany, holds a Master of Philosophy degree in Defence and Strategic Studies with first class from University of Madras. He has attended the Command and General Staff Officer's Course in United States Army Command and General Staff College, Fort Leavenworth; Advanced Security Co-operation Course from the Asia-Pacific Centre for Security Studies , Hawaii, Executive Course in Defense Decision Making from the Centre of Civil Military Relations and Naval Post Graduate School, Monterey, USA. He is a graduate of the Royal Military Academy, Sandhurst, UK and the War College, Mhow, India. He represented the Army and the country in various International meets like the 6thXiangshan Forum in 2015 held in Beijing and Pacific Armies Management Seminar in PACC/PAMS-XXXVII 2013 in Auckland. He served in key leadership and management roles, notably as Brigade Commander, Division Commander and Deputy Chief of Staff. He has also headed prestigious Military Training Institutions like Nepalese Army Military Academy, Nepalese Army Command and Staff College and was Chief Instructor Higher Command and Management Course, Nepalese Army War College.

PROF C CHRISTINE FAIR
PROVOST'S DISTINGUISHED ASSOCIATE PROFESSOR, GEORGETOWN UNIVERSITY



Prof Christine Fair is a Provost's Distinguished Associate Professor in the Security Studies Program within Georgetown University's Edmund A Walsh School of Foreign Service. She holds a PhD in South Asian Languages and Civilisations from the University of Chicago. Prof Fair worked as a Senior Political Scientist with the RAND Corporation, a political officer with the United Nations Assistance Mission to Afghanistan and a senior research associate at the United States Institute of Peace. She is a member of Women in International Security, International Studies Association, American Political Science Association, the American Institute of Pakistan Studies, the American Institute of Bangladesh Studies, the American Association for Afghan Studies and the Association for Asian Studies, among others. She serves on the editorial board of numerous scholarly and policy-analytic journals. She has authored, co-edited and co-authored several books, including *'In their own words: Understanding Lashkar-e-Tayyaba;, Fighting to the End: The Pakistan Army's Way of War; Pakistan's Enduring Challenges and Policing Insurgencies: Cops as Counterinsurgents*. She is a well versed in Hindi, Urdu and Punjabi.

DR. AJAI SAHNI
EXECUTIVE DIRECTOR, INSTITUTE FOR CONFLICT MANAGEMENT

Dr. Ajai Sahni is the Executive Director of the Institute for Conflict Management, the South Asia Terrorism Portal & Khalistan Extremism Monitor. He is the publisher and editor of 'South Asia Intelligence Review', 'Faultlines: KPS Gill Journal of Conflict & Resolution' and 'Second Sight'. He is also the Project Director at Impact. He served as a Member of the Madhukar Gupta Committee on the 'Restructuring of the Ministry of Home Affairs' and is presently a Member of the Police Modernisation and Strengthening Committee, Uttar Pradesh. He has researched and written extensively on issues relating to conflict, politics and development in South Asia and has participated in advisory projects undertaken for various National or State Governments. He jointly edited (with KPS Gill) 'Terror & Containment: Perspectives on India's Internal Security'; 'The Global Threat of Terror: Ideological, Material and Political Linkages'; and separately, 'The Fragility of Order: Essays in Honour of KPS Gill'.