Contextual Evolution of Hybrid Warfare and the Complexities

Rakesh Sharma

> *The French historian Marc Bloch, post German blitzkrieg in 1940, remarked that "…our leaders . . . were incapable of thinking in terms of new war. . . [Their] minds were too inelastic."*

Prelude

On September 14, 2019, at 4.00 am, Saudi Arabia suffered a deadly attack on its Aramco owned oil facility at Abqaiq and Khurais oil field, with, as has been stated in a version, a swarm of 18 small drones and seven cruise missiles. Very highly protected and fortified facilities, in addition to armed guards, the area had six battalions of Patriot defence systems, Oerlikon GDF 35mm cannons equipped with the Skyguard radar and Surface-to-Air-Missiles (SAMs). The targets were designated with pin-point accuracy and, hence, the strikes were most effective. They destroyed nearly 50 per cent of the country's global supply of crude. The crude prices rose sharply in the international market that saw the US Secretary of State proclaiming it was an "act of war"– yet without a declaration of war. By exactitude, the perpetrators were unidentified, even the trajectory of the flights of the missiles and drones could not be ascertained; only remnants of the

Lieutenant General (Dr.) **Rakesh Sharma** (Retd) is currently Distinguished Fellow at CLAWS.

Yemeni Quds 1 missile were displayed. The conjectures are aplenty – from drone swarms, to cruise missiles, to stealth aircraft and even ground action! It is also a fallout of the usage of the modern war weaponry: plausible deniability! This is a manifestation of the 21st century's hybrid warfare.

War is a historic constant. In strategic history, 'war' has had many definitions and recurring generational divides. Nations invest billions of dollars in preparing their militaries for the next war. Futurologists, bright thinkers and strategists had, in history, forecast and laid down strategies and planned conduct of wars that did not succeed eventually. Warfare is an exceedingly complex venture, where information is scanty, unclear and outdated;[1] as the edifice of military planning is built on assumptions, these almost often go wrong. With dwindling defence budgets, and the veritable sprint in military technologies, the armed forces are placed in a dilemmatic situation on enunciating futuristic military doctrine strategy, and creating a future force. The easiest way out for militaries is to bask in the status quo, and, hence, it is often stated that Generals have a tendency to "fight the last war".[2]

Historically, the Clausewitzian relationship of politics and warfare has stood. Once a war was imminent or ensued, the political aims articulated were then translated into a military strategy for victory in war. Traditional percepts of warfare have remained inter-state, where victory implies capture of large tracts of territory (even in a desolate countryside), taking a large number of prisoners of war, or decimation of the adversary's war-waging potential, as these are the considered finality in the capitulation of the enemy and dictating the victor's political will.

This article aims to deal with the conceptual underpinnings of hybrid warfare, its complex character, and attempts to sift through the maze of its multi-faceted domains. It would highlight the emanating concoction in warfare, in which many forms of belligerence are usable, disaggregated or aggregated or in tandem, as per the political aims and military end state sought.

Transition in the Character of Warfare

The character of war has changed, and is steadily changing. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, these have exceeded the power of force of weapons and their effectiveness. This implies that wars in the future may remain unannounced, in non-kinetic format, and may even be successful in achieving political goals without transcending to force-on-force wars. Certainly, use of kinetic means in standoff forms such as precision guided munitions, missiles and rockets or space warfare, can supplement to achieve the political aims in a short timeframe. Indeed, "…the categories of warfare are blurring and no longer fit into neat, tidy boxes."[3]

Researchers and analysts worldwide are proclaiming that future warfare will be different. In the last 20 years, the pace of change has accelerated, due in no small part to the advent of new technologies that are transforming the way wars are fought, as well as the operating environment in which they take place. The pace of change in the information warfare domain and space, and technologies like drone swarms, directed energy weapons, artificial intelligence, high-powered microwave, autonomous systems and robotics, to name but a few, is so rapid that doctrinal and strategic changes are unable to keep pace. The ambit of information warfare and artificial intelligence is ever expanding, with digital storage, computation, and transmission of data bits combined with miniaturisation of land, air, surface, and sub-surface platforms of ever-increasing mobility and endurance.

Computers and the internet, in particular, have played a key role in shaping the transitory nature of warfare. Two emerging technologies relative to the fresh non-kinetic domains—cyber and autonomous systems—dictate contemplation. Non-kinetic means act as force multipliers to target the will of the adversary through shaping the environment, and lowering the enemy's will through coercion and hedging, leading to softening through exploitation of existing faultlines. There is movement towards future wars with extreme lethality. Loitering munitions, also known as Lethal Miniature Aerial Munitions (LMAMs), are a form of an unmanned aircraft system that incorporates a warhead and can be thought of functionally as an unmanned *kamikaze* plane. Given their plane-like attributes, LMAMs are able to stay aloft for extended periods, thus, "loitering" over a target area.[4]

Similarly, there would be concerns of fully autonomous systems having the authority to take a life or start a war as an agent of state policy. The possibility of life-or-death decisions some day being taken by machines not under the direct control of humans needs to be taken seriously.[5] The increased importance of precision guided munitions, space warfare, stealth fighters, strategic missiles and rockets are all indications of much increased lethality in warfare. China's new microwave weapon can disable missiles and paralyse tanks by shutting down electronic systems, even those with traditional shielding against Electromagnetic Pulse (EMP) by bombarding the target with energy pulses. This amount of directed energy interferes with, and overloads, electronic circuits, causing them to shut down. China has also tested a completely new weapon, a boost glide hypersonic weapon system, capable of blistering speeds. With the sprint of military technology and cybernetics, the offensiveness of the standoff attacks in the future is in the realm of threats rather than imagination.

The writing for transition in the character of warfare has been on the wall for some time. The narrative is that "[t]he roughly three-hundred-year period in which war was associated primarily with the type of political organisation known as the state… seems to be coming to an end. If the last fifty years or so provide any guide, future wars will be overwhelmingly of the type known, however inaccurately, as 'low intensity'".[6] The intense focus on counter-insurgency or low intensity warfare also tends to relegate the likelihood of conventional operations to clichés – short, limited, localised, intense, and the like. In this transition of warfare, a significant mention is of guerrilla warfare, terrorism and insurgency. Guerrilla warfare is not a recent innovation, though, in the 1960s, it was seen as a new form of war that could take place despite the nuclear stalemate. Later, terrorism became the new metaphor for warfare. Terrorism dealt with politics and particularly with the way politics is conducted. Illegitimate violence, akin to criminal activity, is undertaken against both political and civilian targets as a measure to manipulate political processes.

Evolving Hybridism and Complexities in Future Warfare

The term hybrid warfare refers to a non-linear conflict, where state actors, in addition to kinetic or military forces, employ non-kinetic means like cyber attacks, politico-economic subversion, psychological warfare, and diplomatic pressure to bring an adversary to heel. The hybrid nature of warfare has existed historically except may be in the cyber or information warfare realm. The breadth of hybrid warfare is limited only by the imagination of the employer. The concept, when postulated, referred to a "tailored mix of conventional weapons, irregular tactics, terrorism and criminal behaviour"[7] and soon got redefined to include the "full range of military intelligence capabilities, non-conventional weapons, armaments, support units, and combat equipment, available for instant employment… of regular forces or irregular insurgents, terrorists, or other non-state actors…"[8] Sometimes, the term 'fourth generation warfare', initially introduced by William S. Lind, is used interchangeably with hybrid warfare due to the erratic nature of the threats and their interplay in the attainment of strategic objectives. Fourth generation warfare, however, is distinguished from hybrid warfare by the involvement of non-state actors pitted against a traditional Army. They present a decentralised, non-hierarchical, and non-traditional structure of threat. Contrarily — in hybrid warfare — wars are fought between states using non-linear tactics involving all elements of national power.

It is apparent, hence, that kinetic or non-kinetic (the latter will include cyber, social media operations, disruption of critical network infrastructure, dissension, subversion, criminal activities, currency manipulation, environmental warfare, and the like), can be aggregated or disaggregated, as need be! In the study of warfare of the last decade, major shifts in war-fighting had been evident worldwide. Russia used only cyber attacks to compel Estonia in 2007, military force and cyber warfare in Georgia in 2008, and ‘Little Green Men’, ‘Night Wolves Motorcycle Club’ and cyber attacks in Crimea in 2014. Obviously, to achieve political aims, the protagonists utilised means other than conventional ones, and succeeded. The second Lebanon War in 2006 was a classic case of a military engagement between Israel and Hezbollah – the latter as a non-state actor used ‘hit and hide’ tactics. The Middle East imbroglio – Iraq, Syria and Yemen—comprises examples of the admixture of the conventional and unconventional. The most defining characteristics of the Syrian War are its complexities and intricacies, with multiple states and non-state actors pitted against each other – together or separated!

The 21st century warfare, hence, is metamorphosing without a distinct pattern, wherein the conventional, with increasing utilisation of Special Forces, irregular and terrorist forces, are not dissimilar, or with fundamentally different approaches. There is an increasing blurring of distinctions between war and peace, between the different domains of conflict (land, maritime, air, space, cyber) and between kinetic and non-kinetic effect. Cyber contributes to the blurring of the distinction between peace and war by creating uncertainty as to what constitutes conflict in cyber space. They are means employed in combination by the adversary and conducted by both state and non-state actors. Therefore, hybridity in warfare has evolved as a combination of more than two elements of power or components of the widely spread spectrum of conflict – both kinetic and non-kinetic. Kinetic in this consideration would imply a spectrum: space weapons, Chemical, Biological, Radiological and Nuclear (CBRN) defence, land, air, naval forces, as also insurgents and terrorists. Non-kinetic would encompass diplomacy, political activities, Information Warfare (IW) including social media, cyber disruption of critical infrastructure, subversion, criminal and economic activities and similar conflictual activities. This evolved hybrid warfare can, hence, be examined as a combination of both kinetic and non-kinetic tools, used disaggregated or aggregated, as and when need be!

Sifting Through the Maze of 'Hybridity'

The term 'hybrid warfare' has surely caused an immense amount of confusion, as it has encompassed activities that were non-military and hithertofore not classified as warfare. This has blurred the distinction between the state of war and peaceful competition – like the 'trade war' between China and the USA. Such generalisations and broad-brush will in future lead to pessimistic and gloomy inter-state relations, and enhance the dimensions of national security to unimaginable proportions. Many of the hybrid 'threats' may just be risks and, even if they germinate well, may not tantamount to 'war'. In a manner of speaking, the instruments of belligerence by an adversary in a nation like ours will be a multitude. Organisations tailored for space wars, cyber offensives, long range precision guided missiles, could well take the initiative and even terminate wars, without as much as involving the military in the gamut of conventional warfare. Indeed, disinformation campaigns under the overall ambit of information warfare, and, hence, under hybrid warfare are bound to cause grave understanding issues on the subject. It obviously implies that contextually, the response to the myriad threats will not be the military itself. The quagmire created by the hybrid nature of threats will place any political or national security decision-making establishment in a predicament to formally enunciate strategy. Therefore, the ambit of national security will encompass the bouquet of hybrid threats.

It must, however, be acknowledged that non-kinetic measures by themselves cannot provide assurance of victory or success in achieving political objectives. There are also comprehension issues, on whether non-kinetic attacks like cyber can be taken as declarations of war. It is well understood that non-kinetic means can be as devastating as kinetic ones and that they also have the advantage of plausible deniability by adversaries. A severe non-kinetic attack, though 'denied', will place the recipient nation in a quandary on what will constitute a proportionate response. Again, would a full-scale or limited conventional war be acceptable as a response to a major cyber attack?

As is apparent, the character, and, may be, even the nature, of warfare has changed, and the belligerents would use a new 'mix and match' of their capabilities to achieve a decisive victory. It actually implies that there would be no distinction between conventional and unconventional means to be used against the opponent, that is, in the hybrid context, attacks and responses can emanate from any military or even non-military sphere. For example, a cyber attack on civilian infrastructure like against the banking system, may be a kinetic full force response. This formulation of hybrid warfare would challenge the traditional concepts of conventional war. The standoff nature of the current day targeting by cyber means, utilising drones and cruise missiles, or even space-based assets, would blur the lines between the military and civilian domains. Such warfare is a game-changer. Any conventional superiority is of little value if the nation is woefully vulnerable to a catastrophic cyber attack. The threat of cruise missiles or drones is fine, but the fact is that a takedown of the energy grid or transportation network or health service is a far greater risk. This risk does not require any future development in cybernetics—the technology is available today, even in the open domain.

The broader ambit of hybrid warfare which includes the realms of information warfare – propaganda, psychological manipulation, media misdirection, subversion of the population—requires fresh thought. Most such typology of warfare – if it is so called – may not be practically attributable directly to an adversarial nation, or even a proxy. There would be obfuscation of state sponsorship –like the purported actions of

Cambridge Analytica in the build-up to the US elections in 2016, which included serious accusations about Russia.

Hybrid Warfare and Strategising for India

A question that begs an answer here is whether or not a hybrid war can be fought with our present national security structures? What is the inter-relationship between hybrid warfare and military strategy? In such context, how does a nation like India deter hybrid threats and formulate its national and military strategies?

Conventional Indian concepts of war are incompatible and fundamentally skewed from the realities of hybrid conflict in the 21st century. Indian adversaries have either mastered irregular warfare or have sufficiently advanced technologically to embrace hybrid warfare. A linear conventional conflict will be a near sequential progression of a planned strategy, whereas a hybrid non-linear conflict will comprise simultaneous deployment of multiple, complementary military and non-military warfare tactics. In a hybrid war, the adversarial conventional military force will be supported by irregular, cyber and informational warfare tactics, aggregated together or used in disaggregated form. It must, hence, be expected that in future, the conflicts that India will have to face will necessarily be hybrid non-linear wars that will be fought with the adversary employing conventional and irregular military forces in conjunction with psychological, economic, political, and cyber assaults. Confusion and disorder may ensue when weaponised information in India would worsen the perception of insecurity in the populace as political, social, and cultural identities will be attempted to be pitted against one another.

India must then develop a framework of strategic deterrence of weaponised information, finance, and other subversive forms of aggression against the adversaries. A 'one size fits all' national security policy would not be effective. The future nature of warfare leads us to the conclusion that multi-domain warfare (one that spans two or more military domains—land, maritime, air, cyber, space, etc) to create new and innovative ways against adversaries, is the one to be strategised for.

A joint multi-domain specialisation would indicate the right preparation for warfare – kinetic or non-kinetic. That is the responsibility on the shoulders of today's political and military leaders. Three key postulations are preferred:

- Hybrid warfare, as per definition and ambit, describes domains that can well be termed as non-military. Hence, the prosecution of non-military domain aggressive actions, that cause damage or destruction to national infrastructure, must be taken as war – even if the adversary is unidentifiable, unprovable or resorts to plausible deniability. Cases in point would be a cyber attack on the power grid, the banking system, and the like. As stated above, the September 2019 drone attacks on the Saudi Arabian oil fields have been called 'acts of war' by the US Secretary of State. War, hence, in a hybrid context may be a permanence state – blurring the distinction between war and peace. This might seem unduly alarmist, and may affect rationality in behaviour. However, the hybrid character of war has its dictates, and strategising for the same is imperative.
- Since hybrid warfare is not an isolated military domain, law enforcement capabilities – in India symbolised by the National Security Guard (NSG), National Technical Research Organisation (NTRO), National Cyber Coordinator and agencies and Central Armed Police Forces (CAPFs)—require parallel developments, which are skillfully fused with the military domain. The challenge is to plan development of offensive and defensive hybrid warfare technologies and expertise in an era of budgetary constraints. Hybrid warfare necessitates intensive consolidation of all resources and security assets available with various agencies, without resorting to any battle of the turf.
- It is obvious that in a scenario where non-state actors take credit, or where the initiator of an attack cannot be determined, deterring

hybrid threats may not be realistic. Military conventional deterrence remains fixated on all-out or limited high end conventional war that remains within the ambit of state versus state warfare. In the case of India, conventional military superiority, with the threat of deterrence by punishment, is insufficient to force the adversary to cease the proxy war. This credence requires a serious rethink. The likelihood of a strong conventional kinetic response to a hybrid, non-kinetic attack must not be negated. Even the converse can be construed as feasible. The *quid pro quo* response to any form of hybrid attack may emanate in a totally different realm. For example a conventional air strike at Balakot to a terrorist strike at Pulwama! This issue created by the hybridisation of threats opens new vistas in the deterrence debate and response options, and mandates further analysis. Suffice it to say that a strong conventional force will be an inadequate deterrent against hybrid threats. Hence, a proportional or disproportionate response cannot be predictable and will be contingent on the national will and political intent at that juncture. For this, India will require an effective bouquet of hybrid options, a quiver full of variable arrows that can be selectively employed as per the political decision.

- Psychological warfare, fake news campaigns, propaganda, subversion, intimidation, demoralisation and the like, are commonplace. State and non-state actors are weaponising information, to the detriment of adversaries. These will become permanent features among belligerent states. A case in point is Cambridge Analytica, and the influence pedalling in the last US Presidential elections. Naturally, these are also hybrid threats, ones that seem perfectly benign, but which have immense potential to address the collective psyche of the people of a nation. It is not that psychological warfare is a new realm, however the media (including social media) for reaching out have multiplied manifold, their techniques are being made sophisticated, and the effect they are having on the populace is credible. Also, a connotation of the hybrid threat, psychological warfare, is leading to increasing radicalisation and needs to be addressed pronto by parallel streams of well planned counter-radicalisation and information management.

- The definitional and terminological structure of hybrid warfare may have confused warfare itself. Each and every inimical act and risk is being branded as a hybrid threat or hybrid warfare. Any rational consideration of this plethora of hybrid threats, and planning for combating them is well nigh impossible. There is apparent generalisation of hybrid threats, with many of them being faceless, which will require a kind of toolbox that will be unimaginable in content. The cost-benefit analysis for catering for the hybridity will deter serious planning processes. Stepping back from this over-hyped debate that generalises hybrid warfare, and providing a deliberate and sifted out focus is essential.

Conclusion

In sum, in the last 20 years, the pace of change has accelerated, due, in no small part, to the advent of new technologies that are transforming the way conventional and unconventional conflicts are fought, as well as the operating environment in which they take place. The national security strategy in the context of the myriad threats, taken as hybrid, derives itself from a political formulation of national aim, vision and interests. Contextually, military strategy, as a sub-set,envisages employment of all of a nation's military capabilities at the highest of levels, including long-term planning, development and procurement to assure victory or success.

The domain of military strategy in the future needs to be taken as a systemic approach, without anchoring future war-fighting in a single thematic concept of force-on-force as the common and the only denominator. In effect, conventional operations of the force-on-force variety become part and parcel of the larger bouquet of options that amalgamate into multi-domain warfare. Domains may work in concert simultaneously to achieve goals, instead of only operating in, or between, two domains. Multi-domain means creating an effect in one domain that produces an effect in the other. Multi-domain-specific capabilities can be leveraged to defeat a capable foe in another domain, or the 'force-on-force' operations could supplement the creative ways. The armed forces are at a crossroads. Reliance on attrition, firepower and mechanised warfare had led to past successes, but this alone cannot win tomorrow's wars. The adversaries are analysing and testing capabilities in multi-domains, and would adopt and adapt their doctrines, strategies and capabilities to benefit from our vulnerabilities. Evolution of multi-domain warfare, from the concept to functional doctrines for each of the domains, and then an overarching grand strategy, requires understanding and creativity based upon emerging technologies. To arrive at the future, prepared and ready to dominate the fight, we need a concept to guide convergence and integration of capabilities across air, land, sea, space, cyber, and electro-magnetic spectrum.

India is a nation that has unsettled borders, and is also incessantly deployed in countering infiltration and terrorism. Our adversaries are continually upgrading to acquire hybrid capabilities that will offset any conventional war disadvantages that they may visualise. Hence, for combating the hybrid nature of warfare, India will need multi-domain strategies. The 'battlespace' will need decluttering by designating with rigour what inimical activities are 'war-like', in that they are tantamount to the use of force, and which ones amount to unregulated (and possibly unlawful) competition.

Notes

1. Chistopher Flaherty, *A Theory of War As Conflict Without Rules* (University of St. Andrews, 2016), unpublished thesis for Doctor of Philosophy, April 8, 2016. Available at https://pdfs.semanticscholar.org/53a2/84fde7c2347c06928e77dfdaf559c3f2e411.pdf. Accessed on September 24, 2019.

2. Fredric Smoler, “Fighting the Last War—and the Next”, *American Heritage*, Vol. 52, Issue 8, November-December 2001. Available at https://www.americanheritage.com/fighting-last-war-and-next. Accessed on September 24, 2019.
3. Robert M Gates, “A Balanced Strategy Reprogramming the Pentagon for a New Age”, *Foreign Affairs*, January-February 2009.
4. J Noel Williams, “Killing Sanctuary: The Coming Era of Small, Smart, Pervasive Lethality, War on the Rocks”, Centre for Security Studies, 2017. Available at https://www.css.ethz.ch/en/services/digital-library/articles/article.html/5097848a-d36d-4918-b62c-aab6c6dee9ea. Accessed on September 29, 2019.
5. Gjert Lage Dynda, *et al.*, “Autonomous Military Drones: No Longer Science Fiction,” July 28, 2017. Available at https://www.nato.int/docu/Review/2017/Also-in-2017/autonomous-military-drones-no-longer-science-fiction/EN/index.htm
6. Martin van Creveld, “Through a Glass, Darkly: Some Reflections on the Future of War,Naval War”, *College Review*, Vol. 53, No. 4, Autumn 2000.
7. Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007). Available at https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf. Accessed on September 29, 2019.
8. Max Boot, *Hybrid War: A New Paradigm for Stability Operations in Failing States* (Carlisle Barracks, Carlisle, PA: US Army War College, 2017).