Hybrid Warfare:
Battlegrounds of the Future

VK Ahluwalia

> *The most distinctive change in the character of modern war is the blurred or blended nature of combat. We do not face a widening number of distinct challenges but their convergence into hybrid wars.*[1]
>
> — Frank G Hoffman

In the 34-day Israel-Hezbollah War of 2006, Israel's Army, one of the most technologically advanced militaries of the world, was pitted against the fundamentalist Shia Muslim organisation Hezbollah in southern Lebanon. Hezbollah, a non-state armed group, was armed with high-tech weaponry and other disruptive technologies, such as Precision Guided Munitions (PGMs), anti-tank missiles and Unmanned Aerial Vehicles (UAVs) that are traditionally used by the regular forces of a country. Hezbollah forces shot down Israeli helicopters, severely damaged a patrol boat with a cruise missile and destroyed a large number of armoured tanks by firing guided missiles from hidden bunkers.The group's guerrillas stood their ground with their hi-tech weaponry and guerrilla tactics. They operated in a decentralised manner at the tactical levels, from both their urban and mountain bases, and shocked the Israeli Defence Forces (IDF) with their conventional-cum-unconventional forms of warfare. Israel accepted that it committed a mistake in not adequately preparing

Lieutenant General (Dr.) **VK Ahluwalia** is Director at the Centre for Land Warfare Studies (CLAWS), New Delhi.

for a 'hybrid' conflict with Hezbollah.[2] US Army Chief General George W. Casey said that a new type of war that would become increasingly common in the future would be "a hybrid of irregular warfare and conventional warfare."[3]

Similar to this, in the proceedings of the 2009 Hybrid Warfare Conference, Dr. Russell Glenn, Director, Plans and Policy, G-2, in the US Army Training and Doctrine Command, provided a comprehensive definition for a hybrid threat to apply to the tactical, operational, and strategic levels of war. He defined a hybrid threat as an:

> …adversary that simultaneously and adaptively employs some combination of political, military, economic, social, and information means, and conventional, irregular, catastrophic, terrorism, and disruptive/ criminal conflict methods. It may include a combination of state and non-state actors.[4]

Although there are ample examples of Generals and rulers of the ancient times who have used both regular and irregular tools of warfare against their adversaries at strategic and tactical levels, the term 'hybrid warfare' appeared at least as early as 2005. It was subsequently used to describe the strategy and tactics employed by Hezbollah in the Israel-Hezbollah War of 2006. Since then, the term 'hybrid' has dominated much of the discussion about modern and future warfare, to the point where it has been adopted by senior military leaders and promoted as a basis for modern military strategies.[5] Today, in the digital age, there is a wide range of hybrid tools available which enable nations to achieve their objectives at minimal cost, albeit without even fighting an actual war. Therefore, hybrid warfare/threats are the new battlegrounds of the future, as they pose a huge challenge to security and elements of national power. The aim of this paper is to briefly discuss the genesis of hybrid warfare, the various terminologies, the salient differences between

them and their objectives. While drawing the relationship between hybrid warfare and grey zone conflicts, their application at various levels and the recommended actions to minimise their impact would be highlighted.

Changing Nature and Character of Conflicts

There has been a progressive increase in internal armed conflicts (intra-state conflicts), the world over, primarily due to sectarian, ethnic and religious intolerance, socio-economic exclusion, feeling of inequality and injustice, unemployment, and non-responsive governments, unable fulfill the aspirations of the people. The level of violence peaked in the mid-1990s. Concurrently, rapid changes have been seen in the geo-political, economic, social, technological spheres, which has impacted the emerging geo-strategic environment. It is surmised that due to the mutually destructive power of nuclear weapons and the international legal conventions, the probability of all-out wars between the global powers is very low. However, the probability of sub-conventional conflicts or limited conflicts in different regions, with an active role by hybrid adversaries, and the potential to spill over into a major conflict is high. The key feature of the security environment in recent years has predominantly been a range of asymmetric threats, which provides a greater role to the hybrid form of warfare.

The terms 'nature of war' and 'character of war' have been used interchangeably. Besides the military factors, the character of war keeps evolving due to constant changes in technology, geo-politics and geo-economics. Carl von Clausewitz, a cavalry officer, suggests in his book, *On War*, that the capabilities, circumstances and motives of a nation-state too have an effect on the changing nature of conflicts. On the other hand, traditionally, war is interactive, and is an act of violence and destruction. The most common type is the attrition form of warfare. In simple terms, it refers to 'force on force', with a view to annihilate the opposing force. In traditional terms, war is also political in nature, which is generally prosecuted at the national level, with political aims and

objectives. Although conflicts may have political, economic or military objectives, wars may not necessarily always be interactive and violent. Moreover, warfare has continued to evolve from clear territorial wars with a well-defined enemy, to uncertain, ambiguous and irregular wars, in which information and cyber threats have gained prominence in the prosecution of the war. Hence, the nature of war is also changing. We need to also ascertain the difference between conventional and hybrid wars. The major difference between conventional and hybrid wars is that in the latter, all the available instruments of power, from the conventional to the non-conventional, pacification to coercion and subversion, are employed by both states and/or non-state actors.

Hybrid Warfare Over the Years

A peep into history suggests that in the ancient times, the rulers or their Generals in Mesopotamia, Persia, Greece, Central Asia, the Mauryan dynasty, including military leaders like 'Alexander, the Great' and Genghis Khan, who were masters of improvisation and manoeuvre warfare, were always ready to use unconventional war-fighting systems and tactics in their campaigns. A few tools of hybrid warfare were also employed during the Napoleonic Wars, Mao Zedong's protracted people's armed conflict in China, and Shivaji's campaigns against the Mughals in India. The essence is that most of them indulged in irregular warfare, in terms of both tactics and strategic aims.[6]

Kautilya's *Arthashastra* is an ancient Indian treatise on statecraft, economic policy and military strategy, written in Sanskrit, about 2,300 years ago. He has described four types of wars, which have relevance to the contemporary elements of national power. These wars were:

- one, *nantrayudha*, or 'war by counsel' in which diplomatic acumen plays a key role to win wars;
- two, *prakasayudhais* or open warfare, specifying the time and place – a set-piece battle;

- three, *kutayudhais,* concealed warfare, which refers primarily to *upajapa*, psychological warfare, including instigation of treachery in the enemy camp;
- four, *tusnimyudha* (*gudayudha),* in which 'clandestine war' uses covert methods to achieve the objective without actually waging a battle, usually by assassinating the enemy.[7]

The *Arthashastra* also discusses, in detail, the 'covert activities' of secret services, spies, secret agents, and clandestine activities. It specifically states, "Miraculous results can be achieved by practising the methods of subversion."[8] In the chapter on defence and war, psychological warfare covers the methods of propaganda by way of advertising, announcing the ill effects of bad omens in the enemy camp,[9] to play on the cognitive domains of the enemy's soldiers. Many such actions would facilitate easy victory, and are also similar to the modern hybrid warfare of today. Today's tools are far more sophisticated and do not require the physical presence of the adversary at the targeted domains.

Kautilya has also prescribed the four *upayas: sama*, *dana*, *bheda* and *danda*—the use of all available means to achieve one's objectives.[10] These were: *sama* (diplomacy, coercion or conciliation), *dana* (gifts, compensation, economic gratification), *bheda* (rupture, dissension, discontent, information or influence operations) and *danda* (use of force). It is evident from these practices that the Kautilyan concepts can be compared to terms such as hybrid, irregular, unrestricted, non-linear and grey zone warfare. These also have some relevance and similarity with terms like conventional and unconventional forms of warfare, covert operations, information operations, subversion, sabotage, deception, and propaganda.

Historically, it has been observed that nations, in order to achieve their politico-economic and strategic objectives, have continued to coin new terminologies based on the prevalent circumstances and situations, as they

affected them. They have applied various conventional or un-conventional techniques to achieve their national interests. Some of the terms like Low Intensity Conflict (LIC), low intensity operation, sub-conventional operation, asymmetric war, hybrid war, grey zone, unrestricted warfare, irregular warfare, fourth generation war, small war, non-linear, full spectrum, compound war, non-contact warfare, etc, have become part of the military vocabulary. It would be difficult to discuss all the terminologies, but they are similar to the roles, methods, and objectives for fighting in an asymmetric environment. A case in point is the term LIC, which was introduced by Frank Kitson in his book in 1971. It undoubtedly brought out that subversion and insurgency cover practically every form of disturbance, up to the threshold of conventional war.[11] However, a study of insurgencies the world over suggests that subversion is a sub-set of insurgency, which conforms to the tenets of hybrid warfare. Hybrid warfare itself has several terms like hybrid threats, hybrid war, hybrid influencing, hybrid adversary or fifth generation warfare, thus, making the understanding of the concept complex, and, therefore, there is no universally accepted definition of hybrid warfare so far.

Varied Definitions and Perceptions

A number of strategic analysts have given certain interesting definitions of the term hybrid warfare, based on their perceptions and application in their operational environments. In 1837, Rafael Carrera had led a revolt that resulted in the dissolution of the Central American Federation. Nevertheless, "While history portrays him as a guerrilla leader, analyses of the actions of his forces during the insurrection point towards a form of hybrid warfare, a type of combat that combines classical guerrilla recruiting tactics and rural insurgency logistics with mostly conventional combat tactics and operations."[12]

Frank G Hoffman, a Marine Corps officer, has written extensively on hybrid warfare. He explains hybrid warfare thus:

> … Hybrid wars are much more than just conflicts between states and other armed groups. It is the application of the various forms of conflict that best distinguishes hybrid threats or conflicts. This is especially true since hybrid wars can be conducted by both states and a variety of nonstate actors. Hybrid threats incorporate a full range of modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts that include indiscriminate violence and coercion, and criminal disorder.[13]

Russia had successfully invaded Ukraine and Crimea in 2014, following the tenets of hybrid warfare. While describing the case of Russia, Alexandru Apetroe states that the term 'hybrid warfare' has been used to refer to the combined usage of unconventional military tactics such as conventional warfare with irregular warfare and cyber warfare, as well as the employment of other instruments and tactics (subversive elements), to achieve a double goal: first, to avoid responsibility and retribution; and, second to weaken and destabilise the enemy without direct involvement.[14]

Sean Sullivan writes about the use of mass communication networks—based on the tenets of hybrid warfare—as these comprise one of the most powerful propaganda tools in the world:

> Examples of hybrid warfare include dissemination of disinformation or fake news via social media, cyber-attacks on the IT systems or as the case in the conflict in Ukraine, disinformation and the use of anonymous men, dubbed 'Little Green Men.[15]

Interestingly, Patrick Cullen *et al.,* have identified the vulnerabilities that may be exploited:

> Hybrid warfare is designed to exploit national vulnerabilities across the Political, Military, Economic, Social, Informational and Infrastructure

> (PMESII) spectrum. ... This process should direct comprehensive cross-government efforts to understand, detect and respond to hybrid threats.[16]

While discussing the definition, Matthew Symonds states, "Definitions vary, but, in essence, it is blurring of military, economic, diplomatic, intelligence and criminal means to achieve a political goal."[17]

Based on its wide experience of asymmetric warfare and employment of elements of hybrid tools in Afghanistan and Iraq, the US military describes hybrid war as being:

> …a combination of symmetrical and asymmetrical armed conflicts, where the intervention forces carry out traditional military operations against enemy military forces and targets, while acting simultaneously and decisively for gaining control of the indigenous population in the theatre of military operations, through stability operations.[18]

Thus, it may be fair to say that hybrid warfare is a strategy which employs a blend of conventional warfare, irregular warfare, disruptive technologies, cyber warfare, and communication networks with other influencing methods, such as fake news, diplomacy, and foreign electoral interventional methods, directly or indirectly, to achieve political, economic and strategic objectives. Efforts are made to synchronise the overall effort, but it becomes difficult due to the number of state and non-state actors involved. Another important feature of hybrid and grey zone warfare is to deny a country's involvement in unconventional or clandestine activities, to prevent any further escalation. Peter Pindjack of the Ministry of Foreign and European Affairs at the Slovak Republic, has identified the target places where hybrid war takes place and opines that "a *hybrid war takes place on three distinct battlefields:* the conventional battlefield, the indigenous population of the conflict zone, and the international community."[19]

To take preventive actions and to counter unconventional threats, the European Centre of Excellence for Countering Hybrid Threats has been established in Helsinki. Reid Standish, a special correspondent with *Foreign Policy*, gives the rationale for the establishment of the centre, which, in essence, also describes the elements of hybrid threats:

> …It was created to find new ways to defend against hybrid warfare: the blending of diplomacy, politics, media, cyberspace, and military force to destabilize and undermine an opponent's government.[20]

In the latest series of *Oriental Review*, an open dialogue research journal, Andrew Korybko, a specialist on hybrid warfare, has formulated the "Law of Hybrid War" which states that"[t]he grand objective behind every Hybrid War is to disrupt multi-polar transnational connective projects through externally provoked identity conflicts (ethnic, religious, regional, political, etc.) within a targeted transit state."[21] Similarly, while discussing the possibility of threats to both the North Atlantic Treaty Organisation (NATO) and European Union (EU), Ivo Pickner argues, ''It means that a hybrid threat is not exclusively a tool of asymmetric or non-state actors, but can be applied by state and non-state actors alike"[22] (Refer Fig 1). A few more elements can be added to the list like transnational forces abetting insurgencies, violence, organised crime and terrorism, support to political parties, religious extremism, etc.

Fig 1: Elements of Hybrid War

Source: Hybrid War as a Modern Instrument of Military Art[23]

Hybrid Warfare and Grey Zone Conflicts

In the recent years, two terms—hybrid warfare and grey zone conflicts—have been added to the glossary of terms of International Relations (IR) and conflicts, which are discussed briefly. Warfare has graduated to the fifth generation in the form of hybrid warfare. It has been used in the conflicts in West Asia, Afghanistan, Ukraine, China, South Asia, the USA and many other areas of conflict. Greg Grant is emphatic when he says that, as part of situational awareness, it is easier to know about own troops, but it does not solve the problem of finding the *"low signature" enemy.*[24] The most potent threats emanate from the information and cyber domains: espionage, attack and manipulation. These can affect a large portion of the population in a short time. Although, the Indian subcontinent continues to face sub-conventional war in the form of proxy war and cross-border terrorism,

it has not experienced the full dimension of hybrid war in the true sense of the term so far.

Grey zone conflicts, on the other hand, are conflicts which oscillate between war and peace and are generally waged by the great powers that do not want to cross the threshold of a total war due to the nuclear threat,[25] and yet aim to achieve their political and territorial objectives. It may perhaps be correct to say that it is also waged by a nation against a powerful adversary, to remain ambiguous, uncertain and below the threshold of an open conflict. In the grey zone, the moves are carefully calibrated to ensure that the situation remains ambiguous and uncertain.[26] Mark Galeotti has described the grey zone concept as "guerrilla geopolitics".[27]

While looking at the future, grey zone conflicts between the great powers will continue to be relevant for both the domination of strategic space and heightened competition for fast diminishing natural resources. While the hybrid warfare concept covers a much wider canvass, with a larger kitty of tools, the grey zone uses them selectively to oscillate between the grey zones of war and peace. Two distinctive examples of grey zone conflicts are Russia's intervention in Ukraine in 2014, and China's progressive, skillful increase in assertive actions in the South China Sea (SCS), by creating artificial islands to deploy Surface-to-Air Missiles (SAMs) and anti-ship missiles, and establishing security posts on the reclaimed islands.[28] Although, these activities are in the realm of the grey zone, they certainly point toward employment of hybrid threats. Subsequently, China has continued to conduct major naval and air exercises in the SCS, suggesting to America that any intervention would be "more risky and more costly."[29] The lines among military, economic, diplomatic, intelligence and criminal means of aggression are becoming increasingly blurred.

Increase in Hybrid Warfare

Hybrid threats have become predominant due to a number of reasons: one, the changing nature of the world order and the security matrix at the global and regional levels; two, the fourth industrial revolution—the fusion of technologies—in which technologies have developed at a very rapid pace and international norms and regulatory mechanisms have still not been established, e.g., for cyber, space and lethal autonomous weapon systems; three, technology has provided new tools and has empowered the state and non-state actors to achieve their objectives at much lower costs; four, information warfare, due to increased digitalisation, internet and social media influences that can change the perceptions of the target population in a much quicker timeframe; five, in counter-insurgency operations, asymmetry between the strength of a state and its enormous resources, against the will of the insurgents to fight for their cause has been facilitated by the availability of the latest technology. With the advent of new technology, digitalisation or the usage of the virtual sphere has not only provided a wide range of tools to easily and quickly propagate a fear psychosis among the masses but has also lowered the cost of achieving one's goals and objectives.

The fourth major industrial revolution has resulted in blurring the lines among the physical, digital and biological spheres.[30] The new technologies like: the Internet of Things (IoT), cyber security, simulation, lethal autonomous weapon systems, Artificial Intelligence (AI) and big data, augmented reality, cloud computing, addictive manufacturing and 3-D printing would play a key role in organising non-contact and non-kinetic forms of warfare to achieve objectives. These technologies are already providing the architectural support for hybrid threats and challenges to security, which should be exploited, both to counter them as also to employ them to our advantage in a proactive manner.

Moreover, hybrid warfare, also known as ambiguous warfare, generally pivots around political, economic and military objectives. It is

a blend of the realms of the economy, military, information, psychology and cyber, with a view to achieve political objectives.[31] The range of hybrid tools continues to increase with changes in the geo-political environment, new innovations in technologies and new ideas to serve one's national interests. A few of these elements and tools put together are: conventional warfare, irregular warfare, economic leverage, cyber warfare, cyber tools (espionage, attack, manipulation),information warfare, special operations, strategic leaks, subversion, propaganda, fake news, psychological operations, public information campaign, influence operations, funding various organisations, organised protests movements, transnational abetment of violence based on sectarian, ethnic and religious intolerance, operations by proxies, and radicalisation based on religious extremism. Information and cyber warfare are central to hybrid warfare.

Cases of Hybrid Warfare and Impact

Several countries have been affected by hybrid threats over the years, by both state and non-state actors, or a combination of the two. Only a few cases have been discussed. Some of the recent examples, published and spoken about at various forums, are the Russian ' little green men' in Ukraine; Russian hacks into the e-mail server of the US Democratic National Committee (DNC); the protest and counter-protest over the mosque in Houston, with both sides fake and organised by Russian trolls. Gregory Treverton *et al.* have described these as the "hybrid threats in the 21st century."[32] Considering the financial vulnerabilities of Ukraine, the Russian military actions were closely linked with political, economic and information campaigns.[33]

Similar to this, although its claims on a number of islands and territorial waters in the South China Sea (SCS) are disputed by several neighbours, China has built progressively militarised artificial islands in the SCS during the past decade. This remains part of the grey zone conflict with hybrid threats. To quote Gregory F. Treverton, "China has

concentrated on cyber tools, pursuing some combination of espionage, signalling capabilities or preparing to add cyber friction in the event of conflict."[34] Even the Islamic State of Iraq and Syria (ISIS), Hezbollah and Syrian Democratic Forces (SDF) have used the elements and mix of conventional and unconventional methods, symmetrical and asymmetrical tactics and capabilities for their violent actions and terror. Conflict in Yemen is another example of multifaceted hybrid warfare, where the Houthis, who were fighting primarily for a greater share of power, have "employed both kinetic and non-kinetic force to control the state and its socio-economic policies."[35] The Houthis have withstood the campaigns by the Yemeni armed forces since 2004, and the Saudi-led coalition that carried out ground and air attacks, and naval blockades, periodically since March 2015. Recently, the Houthis claimed to have attacked the two major oil fields of Saudi Arabia by a swarm of armed drones and missiles on September 14, 2019—a new form of unmanned armed attacks though not the first of the kind in the world.

Closer home, the actions of Pakistan are examples of what is now being termed as grey zone conflict and/or hybrid threats. These have been discussed very briefly. Since its independence in August 1947, Pakistan has remained obsessed with the idea of annexation of Jammu and Kashmir (J&K) with it. On October 22, 1947, as part of detailed planning, Pakistan launched 20 *lashkars* of Pathan tribal warriors from the Northwest Frontier Province (NWFP) into J&K, with a few retired officers from the Pakistan Army to guide the *lashkars* to achieve the ultimate aim of annexing J&K. The tribesmen were more adept at guerrilla war than infantry-style battles.[36] It was called Operation Gulmarg, an unconventional operation to keep it below the threshold of an open war with India, which was much stronger militarily. The Pakistan Army entered the war in 1948. Eventually, Pakistan failed.

Having not learnt a lesson, Pakistan launched Operation Gibraltar by infiltrating the Pakistan Army's Azad Kashmir Regular Force (AKRF),

disguised as locals, into Baramulla, Uri, Gulmarg and other areas J&K, in August 1965. The aim was to foment an uprising with the support of the local people and annex J&K, with the intervention of the regular Army at an opportune moment. Pakistan had launched the AKRF, to be followed by the regular Army. While the covert multi-pronged infiltration plan and abetment of an uprising failed, it led to the Indo-Pak War of 1965. Once again, Pakistan failed in its mission.

With its experience of the role of the Mujahideen in Afghanistan since 1980, where they were supported, equipped and funded by the US, Pakistan indulged in proxy war-cum-cross-border terrorism in the Kashmir Valley in the late 1980s, which subsequently spread to the adjoining areas south of the Pir Panjal Range (PPR). Pakistan has continued to provide diplomatic, military, political, financial, propaganda and psychological support to the terrorists, including a large number of *jihadists* who came from the Middle East in the 1990s. The aim was to destabilise India by the doctrine and announcement of "bleeding India with a thousand cuts".[37] In 1999, Pakistan sent its regular troops (Northern Light Infantry), dressed in local attire, to deceitfully occupy the Kargil Heights, but announced to the world that they were Mujahideen. This was yet another way of unleashing hybrid war to achieve its multiple aims. The operation was a political, diplomatic and strategic failure. However, keeping in view its larger strategic objectives, Pakistan has been successful on several counts by employing appropriate hybrid tools in a calibrated manner against India.

It is common knowledge that Pakistan sponsored terrorist groups like the Lashkar-e-Taiba (LeT), Jaish-e-Muhammad (JeM), Hizbul Mujahideen (HM) and many others, carried out attacks in the hinterland at Mumbai, Delhi, Jammu, Varanasi, Uri, Samba, Pathankot, Nagrota, Sanjuwan and Pulwama with the aim of destroying the very idea of India. The terrorists attacked the financial hub (Mumbai) a number of times, religious places of worship to cause communal disharmony, the

Information Technology (IT) hubs, and the Parliament of the country – the symbol of democracy of the country. Being fully aware of India's growing economic and military strength as an emerging power, Pakistan resorted to the basic tenets of grey zone conflict, employing hybrid tools in terms of providing diplomatic, military, political, financial, religious, propaganda and psychological support to destabilise India.

Way Ahead

As a concept, a combination of the conventional and unconventional systems of war-fighting, regular and irregular, overt and covert operations, at strategic and tactical levels, is as old as the history of warfare itself. Everyone understands that the security landscape is becoming increasingly complex, multi-layered and multi-dimensional, but it is becoming more and more difficult to understand the threats being faced by nation-states. As part of their strategy, hybrid adversaries study the critical political-economic-social-military structural vulnerabilities, and plan to target them by varied hybrid elements and tools. In fact, the nature and intensity of threats keep changing, based on innovative ideas and technological advancements. Therefore, it is important to first keep abreast with the technological tools, understand and assess the nature and intensity of the threats and vulnerabilities, and the impact on one's national security.

Given the current tempo of conflicts the world over, it would be correct to agree with Margaret Bond about the role of all elements of national power. According to Bond, "War of the next century will comprise a kind of hybrid war, projecting all elements of national power along a continuum of activities from stability, security, and reconstruction operations, to armed combat."[38] The capabilities of both state and the non-state actors to engage in hybrid warfare differ, but remain the most potent threat. As hybrid warfare is primarily well-equipped and designed to exploit national vulnerabilities across the political, military, economic, social, informational and infrastructural spectra, it virtually means that it

comprises war against nation-states. India continues to be vulnerable to hybrid threats, being a large, pluralistic, democratic nation, with a huge diversity in geography, demographic profile, socio-economic disparity, and other forms and manifestations. As there is no declared war, the rules of war have also changed. Thus, in the future, we will be increasingly confronted with non-kinetic and non-contact forms of threats, which will be far more potent and lethal. It is a fact that no single element of national power – certainly, not the military alone—can address the hybrid threats of the future. There is, therefore, a need to change our 'mindset' from conventional conflict alone to a combination of conventional-cum-non-conventional methods to combat the hybrid threats of the future. There is a need to create organisations at the apex level—the Centre—to plan and synergise the activities of various organs of the state, to respond to such situations. Also, the integration of the Centre with the states would be central to our preparation for such hybrid threats. Thus, along with logistical and military preparedness, there is a need for political and diplomatic level preparedness at all stages as well, and all these preparations need to be in sync with each other if the country has to combat hybrid threats.

With varied hybrid elements, particularly information and cyber warfare, gaining prominence to target the conventional battlefield and the indigenous population of the conflict zone, there is a need to develop a strong intelligence system, with survivability and redundancy, to identify the emanating threats and take proactive actions to mitigate them. We also have to address the international community proactively to counter the propaganda narratives of the adversaries. A case in point: cyber attacks by an adversary could paralyse the economy, governance, banking, transportation systems, and military networks. Since the indigenous population is one of the primary targets of hybrid adversaries we have to promote awareness about the adversary's designs and threats to all sections of the society, including higher educational institutions

such as private, state and central universities. Such institutes should remain vigilant to report activities that may lead to subversion, abetment of people's movements, terrorist attacks, organised crime, radicalisation, recruitment for religious extremism/anti-national activities, and misinformation campaigns that lower the morale of the population at large. Simultaneously, the intelligence and police forces must be restructured, trained and equipped with modern tools to fight the emanating threats.

One of the most prominent players comprise the armed forces. Besides the need for synergy amongst them, they should also carry out a *de novo* study of their capabilities and effectiveness in hybrid or grey zone scenarios. It would certainly point to reviewing our doctrines, strategies, war-fighting concepts, command and control structures, intelligence at different levels, and the need to build matching capabilities. Just as Israel learnt its lessons in its war with Hezbollah in 2006, and carried out a review to fight against hybrid threats, India should also prepare for these with a sense of urgency. We, as a nation, should be prepared to fight a high intensity war along with the unconventional and hybrid threats. Therefore, a counter hybrid warfare strategy will be successful only if it can effectively synchronise the political, economic, military, social, cyber and informational warfare tools to defeat the hybrid adversaries in time.

Notes

1. Frank G. Hoffman, "Conflicts in the 21st Century: The Rise of Hybrid Wars", Potomac Institute for Policy Studies, Arlington, Virginia, Issue 52, 2007, p. 39.
2. Samuel C Rajeev, "Israel and the Challenges of Hybrid Warfare", in Vikrant Deshpande, ed., *Hybrid Warfare: The Changing Character of Conflict* (New Delhi: IDSA/Pentagon Press, 2018), pp.122-123.
3. Greg Grant, "Hybrid Wars: What if the Battles of the Future are Neither Conventional nor Irregular, but a Combination of Both?", *Government Executive*, May 1, 2008. Available at https://www.govexec.com/magazine/features/2008/05/hybrid-wars/26799/. Accessed on September 6, 2019.
4. Russel W. Glenn, "Thoughts on 'Hybrid' Conflict," *Small Wars Journal*, 2009. Available at https://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict. Accessed on September 5, 2019.

5. Damien Van Puyvelde, "Hybrid War—Does it Even Exist?" *NATO Review Magazine*, 2009. See also: Alexandru Constantine Apetroe, "Hybrid Warfare: From 'War During Peace' to 'Neo-imperialist Ambitions': The Case of Russia", *On-Line Journal Modelling the New Europe*, Issue No. 21, 2015.
6. Gilmar Visoni-Alonzo, *The Carrera Revolt and 'Hybrid Warfare' in Nineteenth-Century Central America* (Cham: Palgrave Macmillan, 2017), p. 13.
7. LN Rangarajan, *Kautilya: The Arathshastra* (Noida: Penguin Books, 1992), pp. 636-637.
8. Ibid., pp. 462-464.
9. Ibid., pp. 689-690.
10. P K Gautam, "Understanding Kautilya's Four Upayas", *IDSA Comment*, June 20, 2013. Available at https://idsa.in/idsacomments/UnderstandingKautilyasFourUpayas_pkgautam_200613. Accessed on September 6, 2019.
11. Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, Peace-Keeping* (Harrisburg, Stackpool Books, 1971), p. 3.
12. Visoni-Alonzo, n. 6.
13. Frank G. Hoffman, "Hybrid Warfare and Challenges", *Small War Journal*, Issue 52, 1st Quarter 2009/JFQ, p. 39. Available at https://smallwarsjournal.com/documents/jfqhoffman.pdf. Accessed on September 7, 2019.
14. Puyvelde, n. 5.
15. Sean Sullivan, "A Joint Centre to Combat Hybrid Warfare Threats", F-Secure Blog, November 24, 2016. Available at https://labsblog.f-secure.com/2016/11/24/a-joint-centre-to-combat-hybrid-warfare-threats/. Accessed on September 7, 2019.
16. Patrick J. Cullen, Erik Reichborn-Kjennerud, "MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare: A Multinational Capability Development Campaign Project", 2017.
17. Matthew Symonds, "The New Battlegrounds: The Future of War", *The Economist*, Special Report, January 27, 2018. Available at https://www.economist.com/special-report/2018/01/25/the-future-of-war, Accessed on September 7, 2019.
18. John J. McCuen, "Hybrid Wars", *Military Review*, United States Army Combined Arms Centre March-April, 2008, Fort Leavenworth, Kansas, 88(2), pp. 107-108.
19. Ibid., p. 107; Peter Pindják, "Deterring Hybrid Warfare: A Chance for NATO and the EU to Work Together?" *NATO Review*, August 5, 2014. Available at https://www.nato.int/docu/review/2014/Also-in-2014/Deterring-hybrid-warfare/EN/index.htm. Accessed on September 7, 2019.
20. Reid Standish, "Inside a European Center to Combat Russia's Hybrid Warfare", *Foreign Policy*, January 18, 2018. Available at https://foreignpolicy.com/2018/01/18/inside-a-european-center-to-combat-russias-hybrid-warfare/. Accessed on September 7, 2019.
21. Andrew Korybko, "Hybrid Wars 1. The Law of Hybrid Warfare" *Oriental Review*, April 13, 2016. Available at https://orientalreview.org/2016/03/04/hybrid-wars-1-the-law-of-hybrid-warfare/. Accessed on September 7, 2019.
22. Ivo Pickner and Samuel Žilinčk, "Military Concepts and Hybrid War", *Forum Scientiae Oeconomia*, Vol. 4, Special Issue No. 1, 2016, pp. 29-30.

23. McCuen, n. 18.
24. Grant, n. 3.
25. Abhijit Singh, "Between War and Peace: Grey Zone Operations in Asia", Australian Institute of International Affairs, February 13, 2018.
26. Symonds, n. 17.
27. Mark Galeotti, "Russia is Practicing a Form of Geopolitical Guerilla War Against the West", *Defence Matters*, 2017, Institute of International Relations, Prague,
28. Joseph Trevithickmay, "SAMs and Anti-Ship Missiles are now Guarding China's Man-Made South China Sea Islands", *The Drive*, May 3, 2018. Available at http://www.thedrive.com/the-war-zone/20616/sams-and-anti-ship-missiles-are-nowguarding-chinas-man-made-south-china-sea-islands. Accessed on September 7, 2019.
29. Symonds, n. 17.
30. World Economic Forum (n.a.), "Fourth Industrial Revolution". Available at https://www.weforum.org/focus/fourth-industrial-revolution. Accessed on September 5, 2019.
31. Symonds, n. 17.
32. Gregory F Treverton *et al.* (2018), "Addressing Hybrid Threats", Swedish Defence University-CATS-Hybrid CoE, p. 3,
33. Ibid.
34. Ibid., p. 5.
35. Kishore Kumar Khaira, *Lebanon–Yemen Marathon; Hezbollah Head and Houthi Legs, Hybrid Warfare; The Changing Character of Conflict* (New Delhi: IDSA, Pentagon Press, 2018), p. 113.
36. M Ilyas Khan, "Partition 70 Years on: When Tribal Warriors Invaded Kashmir", *BBC News*, October 22, 2017. Available at https://www.bbc.com/news/world-asia-41662588. Accessed on September 7, 2019.
37. Scott Gates and Kaushik Roy, *Unconventional Warfare in South Asia: Shadow Warriors and Counterinsurgency* (London: Routledge, 2016).
38. Margaret S. Bond, "Hybrid War: A New Paradigm for Stability Operations in Failing States," US Army War College, Strategic Research Project.