



ISSUE BRIEF

No. 231

June 2020

Manoeuvre Warfare in the Information Age

Information can be used to disorganise governance, organise anti-government protests, delude adversaries, influence public opinion and reduce an opponent's will to resist.

– Margarita Levin Jaitner
Swedish Defense University¹

Since ancient times, of the two prominent forms of warfare, namely, attrition and manoeuvre, the latter has been the flavour of great military commanders. Traditionally, as a legacy of the past, the armed forces in the Indian subcontinent were organised and structured to fight conventional wars, with 'attrition, firepower, comparing number ratios with the enemy and mechanisation' playing a predominant role. This is despite the fact that manoeuvre and indirect warfare theory have been widely advocated since the times of Kautilya (320 BCE) and Sun Tzu (500 BCE). Today, the battlefield is progressively compressed in time and space. In this era of the information age, cyberspace, advanced computing, extensive communication networks, unmanned systems and social media, are potent weapons of information warfare (IW). It is a combination of several components and each one is a separate subject by itself—operational security, electronic warfare (EW), psychological operations (PSYOPs), deception and physical attacks on information infrastructures. Though these components are both defensive and offensive in their roles, they have been integrated into one single entity. Therefore, the focus of war-winning strategies must integrate information

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent think-tank dealing with national security and conceptual aspects of land warfare, including conventional and sub-conventional conflict and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

CLAWS Vision: To establish as a leading Centre of Excellence, Research and Studies on Military Strategy & Doctrine, Land Warfare, Regional & National Security, Military Technology and Human Resource.

Website: www.claws.in

Contact us: landwarfare@gmail.com



Lt Gen (Dr.) VK Ahluwalia, PVSM, AVSM, YSM, VSM (Retd)**, superannuated as Army Commander, Central Command in March 2012. Thereafter, he served as a Member, Armed Forces Tribunal (AFT). The General commanded an infantry brigade, mountain division and corps in Uri-Baramulla, Kargil and Leh-Ladakh sectors respectively. He has also served in North East India and in the states critically affected by the Maoist insurgency in India. The General has authored a book titled *Red Revolution 2020 and beyond* and co-edited a book on Kargil – *Surprise, Strategy and Vijay: 20 years of Kargil and beyond*. Presently, he is the Director, CLAWS.

Key Points

- In this era of information age, cyberspace, advanced computing, communication networks, unmanned systems and social media, are potent weapons of information warfare (IW). Our adversaries have been exploiting our vulnerabilities in multiple domains.
- The ultimate military aim of war is to deny, destroy or degrade the enemy's war-waging potential, disrupting important elements of national power and the will to fight.
- The focus of war winning strategies must integrate information operations (IO) in its overall plans and manoeuvres. The IO should aim to exploit critical vulnerabilities of the adversary.
- All manoeuvres should ideally integrate political, economic, diplomatic, military, information and social domains, with a view to gain a position of advantage against the adversary.
- 'Information Manoeuvre' is all about synchronising multiple information-centric capabilities; thus, preventing the adversary from dominating the perceptual landscape.
- To coordinate and integrate all elements of national power, including military, an effective organisation is required at the apex level.

Manoeuvre Warfare ...

operations (IO), non-lethal and non-kinetic means, in its overall plans and manoeuvres.

Our adversaries have been exploiting our vulnerabilities in multiple domains. In the recently released *Pakistan's Green Book 2020*, policy recommendations have been made to counter India's action of August 5, 2019 to abrogate Articles 370 and 35A in Jammu and Kashmir (J&K). It advocates that "Pakistan will have to take the war into non-kinetic domains: Information/Cyber Warfare and Electronic Warfare (EW) Spectrum."² Besides China's 'Three Warfare Strategy' which focuses on psychological, public opinion (influence operations) and legal warfare, it has developed its information based warfighting capabilities. In keeping pace with US and Russia, China has developed the necessary cyber warfare capabilities, which are consistent with its military strategy and national security objectives.³ China aspires to become not only the world's largest nation in cyberspace but also among the most powerful.⁴ In 2014, Russia's annexation of Crimea was pro-actively led by an information campaign to influence the perceptions of the people and its leaders, followed by the military manoeuvres. Russia succeeded. IW and manoeuvre are not only true in military campaigns but hold far greater relevance to all elements of national power and national security. There is, therefore, a need to change our mindsets to the new realities of information operations (IO) or cyber operations.

Two senior colonels of the People's Liberation Army (PLA) of China wrote in the book *Unrestricted Warfare: China's Master Plan to Destroy America*, that if we acknowledge that, the new principles of war are no longer using armed forces to compel the enemy to submit to one's will, but are using all means, including armed forces or non-armed forces, military and non-military, as well as lethal and non-lethal means to compel the enemy to accept one's interest.⁵ Further, they mentioned, "The nature of Information Warfare is all-encompassing and unrestricted in time and space and scope." Besides radical changes in the geo-political and geo-economic environment, information and technology have become the predominant drivers of change in future conflicts. Patrick Cullen et al (2017) have pointed out that hybrid warfare is designed to exploit national vulnerabilities across the political, military, economic, social, informational and infrastructure spectrum.⁶ As part of manoeuvre warfare, the aim should be to exploit critical vulnerabilities of the adversary at all levels, to achieve political, economic and strategic objectives. Therefore, all manoeuvres should ideally integrate all elements, including military and information, to gain a position of advantage against the adversary.

This paper aims to briefly study the historical perspective, draw lessons and focus on the military strategy and

application of manoeuvres at different levels. It will also highlight the threats and challenges of manoeuvre warfare in the changing nature and character of warfare, with special reference to the "information age" on the Indian subcontinent.

Fundamental Terms: Movement, Mobility, Manoeuvre and Manoeuvre Warfare

There are numerous examples in history where manoeuvre warfare has provided the war-winning strategy in a number of military campaigns. Yet, some confusion always prevails in understanding the four fundamental terms: movement, mobility, manoeuvre and manoeuvre warfare (4Ms). In military parlance, 'movement' in simple term means to shift or move a force or a formation within the operational area by any means or mode. Broadly, 'mobility' is the ability of a combat unit or armed force to move with its weapon systems, communications and logistics for a military objective. Looking at the bigger picture, Leonhard states, "mobility is the ability to project power over distance."⁷

'Manoeuvre' aims to achieve a position of advantage against the adversary, while mobility is one of the means to execute a manoeuvre; more importantly, it is a way of intellect thinking. However, given the aims and objectives of manoeuvre at different levels, it has two important dimensions: one, at the tactical level; and the second at operational and strategic levels. At the tactical level, manoeuvre refers to the movement of forces, duly supported by firepower, to achieve a position of spatial and psychological advantage, in that order, to destroy the enemy. At operational and strategic levels, a manoeuvre would aim to target the cognitive domains: the minds of the enemy's commanders, their troops, as also the targeted population. It would aim to achieve spatial and psychological advantage to dislocate and disrupt the enemy's physical and psychological cohesion and his will to fight. It aims to delay and disrupt the enemy's decision-making ability. At the tactical level, there is a heavy reliance on firepower and weapon technology to support the manoeuvre. It may not be so at higher levels. 'Manoeuvre warfare' is a military strategy or part of the military strategy to defeat the enemy or potential enemy, by a series of manoeuvres, crushing the enemy's physical and psychological will to fight. The ultimate aim of manoeuvre warfare is not to destroy the adversary's forces but to render them unable to fight as an effective, coordinated whole.⁸

Historical Perspective

To begin with, it would be most appropriate to briefly discuss a military commander, who has been acknowledged as a legend

of 'manoeuvre theory'. Genghis Khan (1162-1227), leader of the Mongol Army, was known for charging with his limited cavalry force across Eurasia and "subjugating more lands and people in twenty-five years than the Romans did in four hundred years".⁹ Genghis Khan's conquest of Transoxiana (1219-20), the war between the Mongols and the Turks, is one of the finest examples of manoeuvre theory. The Mongols declared war on the Turks after a Turkish Governor murdered a group of Khan's merchants.¹⁰ Genghis Khan, then 57 years old, moved with his cavalry force over 2,000 miles across the treacherous terrain and sent a numerically inferior force to the Fergana Valley, the place where Muhammad II had planned to give a fight (Map 1). Khan aimed to fix Turks' major force on the Eastern flank. Meanwhile, he advanced rapidly to the West, through the 'impenetrable' Kyzylkum Desert, a rather long detour, to appear at Bukhara from nowhere, surround and capture the city with his limited force. He took the enemy by total surprise. Muhammad II died a pauper in a small island in the Caspian Sea.¹¹ Genghis Khan followed Sun Tzu's two important principles of war, "strike where the enemy is not prepared, take him by surprise" and "avoid the solid and strike the weak".

Map 1: Genghis Khan's Manoeuvre (1219)



Source: chinasa.gov.cn, Annotated by the Author.

An analysis of Genghis Khan's campaign, with numerically inferior force (mass), brings out few important lessons for the theorist of manoeuvre: correct identification of the centre of gravity (CoG) & speed, shock and surprise, resulted in huge psychological impact and loss of cohesion among the Turks (Leonhard, 1998). Khan passionately believed that the 'strategy of speed and surprise (velocity)' is the key to "maintaining operational momentum". Strategic analysts have compared Genghis Khan's campaigns to two vital facets of science and warfare: one, Newton's Second Law of Motion, i.e. Force (F) equals Mass (M) times acceleration (A), where A is the rate of change of velocity; and two, his techniques of speed and surprise to shock, dislocate and disrupt the enemy (Leonhard, 1998). While the equation force equal mass times acceleration ($F = MA$) was apt in earlier times, what should be the new

variables in the equation when information, communication and technology are playing a predominant role?

Some of the other good examples of manoeuvre warfare are German massive infiltration tactics during the Spring Offensive in 1918 against the British and French (Hutier tactics);¹² in the Second World War Blitzkrieg (meaning Lightning War), the Nazi forces (land and air) used manoeuvres to succeed in the early part of World War II; and Major General Ariel Sharon's attack across the Suez Canal to seize a bridgehead on the western bank during the Yom Kippur War in 1973; during the Burma Campaign in 1944-45, Fd Marshal Slim undertook a deep outflanking manoeuvre to capture Meiktila, cut-off the invading Japanese' logistic support, which set the stage for the capture of Rangoon;¹³ and the Indian Armed Forces manoeuvres and offensives with the support of Mukti Bahini in the Indo-Pak War 1971 that resulted in the liberation of Bangladesh. The latter was a classic case of manoeuvre in time and space, by all combined arms and services, which paralysed the mind of Pakistani commanders.

Theoretical Constructs

Sun Tzu's treatise *Art of War* propagates, "To win one hundred victories in one hundred battles is not the acme of skills.... To subdue the enemy without fighting is the supreme excellence." Similarly, Kautilya's Arthashastra (320 BCE) emphasised *Nantrayudha* (war by counsel), *Kutayudha* (concealed and psychological warfare), *Gudayudha* (clandestine and covert methods) and deception. In his seminal work, *Strategy*, first published in 1954, Sir Captain Liddell Hart, one of the world's famous military thinkers, has examined a number of campaigns to advocate the manoeuvre theory of "indirect approach" and reliance on fast-moving formations.¹⁴ Post the Vietnam War, John Boyd and William Lind looked at analysing the strengths and weaknesses of the enemy and how manoeuvre can be used against the enemy's weaknesses. John Boyd, a fighter pilot and manoeuvrability theorist, laid emphasis on the Boyd Cycle or the Observe-Orient-Decide-Act (OODA) loop, "to maintain a higher tempo and decisions, vis-à-vis, the enemy".¹⁵ On the other hand, William Lind looked at shattering the enemy's psychological cohesion to act. He too propagates that focus should not be on physical destruction.¹⁶

Centre of Gravity (CoG)

The most important principle of manoeuvre warfare is the identification of adversary's centre of gravity (CoG) at various levels. There is a dichotomy in the thoughts on CoG, whether it should be the source of strength or the critical vulnerability

of the enemy. Two centuries ago, Clausewitz, an advocate of ‘force-on-force’ battles, once called the “essential mass of the enemy” his CoG. During the peak period of Islamic State’s activities (2014-17), it has been acknowledged that its CoG was the internet and social media campaign, to achieve its multiple objectives including recruiting Jihadis. Undoubtedly, the religious terrorist organisations are exploiting digital media to indoctrinate, radicalise and recruit youth, seek financial support and organise terrorist attacks. CoG in US manuals is defined as “the source of power that provides moral or physical strength, freedom of action or will to act”.¹⁷ Leonhard (1998) argues that an enemy’s CoG is not his source of strength; it is his critical vulnerability. He further amplifies that destruction or neutralisation of the CoG must result in paralysis of his forces. It stands to logic that, the endeavour should be to apply strength against the critical vulnerability of the enemy, which would have an impact on the military operations. How would this principle be applicable to information cum knowledge-based warfare? To analyse this part, there is a need to examine what are the critical vulnerabilities of the enemy at different levels, as also Pakistan’s proxy war and state-sponsored terrorists?

Changing Character of Warfare: Information Age

With innovations and breakthroughs in the Fourth Industrial Revolution (4th IR) and technological advancements in diverse fields, there has been a change in the character of warfare. In the 4th IR, the fusion of new technologies like artificial intelligence (AI), big data, cloud computing, internet of things (IoT), cyber security and autonomous weapon systems would play a key role in organising non-contact and non-kinetic forms of warfare, duly supported by information, communication and technology (ICT). With the proliferation of imagery, satellite and terrestrial communications, most militaries have access to command, control, computers, communications, intelligence, information, surveillance, reconnaissance (C⁴ISR) architectures, with varying capabilities. As this architecture is secure, interoperable and can provide good quality data, it facilitates battlefield transparency, situational awareness and a higher speed of decision-making ability. Thus, ICT has also impacted the character of warfare.

While land, sea, air and space were the traditional war domains, IW and cyber, by virtue of their vast scope and role in future conflicts, would play a vital role. Liang et al (1999) propagates that “social spaces such as military, politics, economics, culture and the psyche are also battlefields. Warfare can be military or it can be quasi-military or it can be non-military” (Liang and Xiangsui, 1999). It implies that battlespace is omnipresent, cuts across political boundaries of states and all elements of national power would be involved

in any future conflicts. In fact, IW and social media have become game-changers, as they also effect the social cohesion of society. These tools are being used extensively both by the states and non-state actors and within societies, to engage in information campaigns, malicious narratives, propaganda and fake news.

In such an environment, dominance in intellectual and IW enables a country to operate its networks during operations and at the same time deny the same advantage to its adversary. In fact, “the goals of an offensive IW campaign are to deny, corrupt, degrade or destroy the enemy’s sources of information on the battlefield”.¹⁸ Therefore, in an information age, the essential features of the current and future conflicts are fourfold: first, it’s “omnidirectionality” meaning battlefield is everywhere and in multiple spheres (Liang and Xiangsui, 1999); second, information (predominantly cyber, electronic, psychological), AI, space and the role of other emerging and disruptive technologies; third, hybrid threats with the increasing role of irregular and non-state actors in a grey zone environment; and the fourth, a greater focus on non-contact and non-kinetic warfare. With the use of emerging technologies to minimise casualties by confrontations, the traditional ‘force-on-force’ engagements have given way to multidimensional (multiple spheres and types of forces) forms of warfare with the added role of precision guided munitions (PGMs) replacing the platform-based systems, surgical airstrikes, unmanned aerial vehicles (UAVs), swarms of drones, stealth technologies, IW, space-based enhanced ISR capabilities, with greater roles to airborne and special forces.

Manoeuvre Campaigns: Information and Communication Age

Revolution in information and communications has seen manifold increase in information-based technologies, IoT, social media and the envisaged fifth-generation communication technologies. Not only does IoT increase interconnectivity, but it also ensures the transition of a high volume of data with incredible speed. In fact, within IoT, actions take place in nanoseconds and occur billions of times daily.¹⁹ IT consists of systems and resources (hardware, software and infrastructure). These facilities would find innovative applications in multiple domains – both by civil and military leadership. Moore’s Law (1965), says that the growth of microprocessors is exponential. We will continue to see improved connectivity, increased processing capability, and limitless data of information, which can be shared in real-time, at an exponential rate. While quoting certain concrete examples of Pentagon and others, William Gery et al (2017) reiterated that the number of attacks on information systems

has increased each year, reinforcing the fact that warfare is currently being conducted in the information space via IT.²⁰

Undoubtedly, IW, along with other developing technologies like war-related material, PGMs, weapon systems, autonomous systems and biotechnologies will pose the biggest threat in future conflicts. War strategist Sun Tzu said, “Information gathering is the essence in warfare—it is what the armies depend on for their every move.” In recent years, IW and cyberspace have been used pro-actively, before and during the military operations, to achieve multiple advantages by non-kinetic methods: to target the technical data and cognitive domain of leaders and population, use strategic communication campaigns to influence population perceptions, create psychological fear and dilemmas and delay the decision-making cycle. A few examples of recent times are:

- The Allies’ victory in the Gulf War is a direct result of their ability to obtain and exploit critical information about their adversary, using all available means including space-based systems. While the US forces used intense air power and experienced success during the 1990 Gulf War against Iraq, a few military strategists have attributed this success to manoeuvre warfare tenets like deception, pre-emption, dislocation and disruption. Resultantly, they distorted, influenced and delayed the Iraqi decision-making through IO.
- During NATO’s aerial campaign against Yugoslavia, it declared Radio Television of Serbia (RTS) headquarters, a legitimate military target as it “was making an important contribution to the propaganda war which orchestrated the campaign against the population of Kosovo”.²¹ It bombed RTS on April 23, 1999.
- During the annexation of Georgia in August 2008 and as a part of the hybrid warfare, Russians effectively used cyber and IW along with the military application. Russian IW in Crimea and eastern Ukraine in 2014 has been acknowledged as highly successful due to innovative techniques and methods adopted by them. Russian IW strategy, known as ‘Reflexive Control’, can be used against either human-mental or computer-based decision-making processors.²² Also, the “insignia-less armed fighters” who were operating in Crimea were referred to by the Ukrainian side as the “little green men” from Russia.²³ It was a well-planned strategic communication campaign and cyber attacks in which Crimea was annexed without firing a shot.²⁴
- US has acknowledged that “Operation Glowing Symphony” was the biggest offensive cyber operation carried out by the US Cyber Command. It specifically

targeted the Islamic State of Iraq and the Levant (ISIL) use of social media, internet propaganda and prevented its members from communicating amongst the groups.²⁵

Information Operations: The Manoeuvre Arm

Even in the information age, the ultimate ‘military’ aim of war is to deny, destroy or degrade the enemy’s war-waging potential, disrupting important elements of national power, and the will to fight, to achieve one’s political and/or military objectives. IW and cyberspace will be the most potent weapons of the future to provide that advantage. It would be prudent to say that targeting the cognitive domains—the human mind—would remain a high priority. This strategy conforms to the British armour theorist, JFC Fuller’s belief that attacking the brains of an organisation and severing it from the remainder of its organisation would produce enough chaos to create what he called “strategic paralysis”.²⁶ George Gilder, author of *Microcosm: The Quantum Revolution in Economics and Technology* (1990), also lays emphasis on the human mind. According to him, “the most valuable capital is now the capital of [the] human mind and spirit.”²⁷

According to Charles Pindjack, “a hybrid war takes place on three distinct battlefields: the conventional battlefield, the indigenous population of the conflict zone and the international community”.²⁸ To succeed, it is expedient to exploit the non-lethal information environment at all levels, including strategic, operational and tactical. To take advantage of IO in manoeuvre warfare, there is a need to analyse four crucial issues: first, obtain detailed information and intelligence about adversary’s entire range of IW, social media (Facebook, YouTube, WhatsApp, Twitter, etc.) and perception management capabilities; second, analyse adversary’s CoG at the international, national and military levels; third, formulate a policy at the national and military level to protect own IW resources and exploit adversary’s vulnerabilities; and the fourth, techniques to be adapted to achieve ‘information superiority’. At the national level, cyber networks are being used extensively, ranging from financial, transportation, intelligence, communication systems, air space management, etc. These lend themselves to digital manipulation. In network-centric warfare, information superiority will be a crucial ingredient to give a decisive edge in a theatre of operations. Again, it must be linked to own research organisations to develop capabilities to exploit the enemy’s vulnerabilities. It must be remembered that non-indigenous software and networks are most susceptible to cyber attacks. Therefore, “Make in India” should be given the necessary impetus to facilitate failsafe information superiority. We have a lot of ground to cover!

Concept of Information Manoeuvre

'Information Manoeuvre' is not a new concept. The British Army has a concept of 'Information Manoeuvre', which is about fusing and synchronising multiple information-centric capabilities under one command (6th Division). Information Manoeuvre allows UK to generate options to mitigate risks and seize opportunities in the information age. It aims to prevent the adversary from dominating the perceptual landscape and gaining operational surprise in the grey zone. It is achieved by worldwide engagement, both physical and cyber, through collecting intelligence and challenging the adversary's incremental gains in the physical, virtual and cognitive spaces.²⁹ Joint Publication of the US defines IO as the "...integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt or usurp the decision-making of adversaries and potential adversaries while protecting our own."³⁰

At the international level, the diplomatic community should study an adversary's history, culture, language, ethnic composition and leanings of the population and its faultlines to manage the perception of foreign audience to serve own national interests. At the national level, the IW strategy must be modified based on a deliberate study of the adversary's capabilities and vulnerabilities in political, economic, military, internal security, social fabric, environmental, historical and cultural heritage, etc. Therefore, it would be prudent to analyse an adversary's capabilities and modus operandi to protect its information and processes and to organise offensive actions like EW, PSYOPs, deception, influence operations, physical destruction of IW infrastructures, etc. With the extensive application of AI, digital media penetration supported by social media, an adversary is likely to exploit fake news, propaganda and PSYOPs in unique ways and extent. Therefore, there is also a need to analyse adversary's digital culture, social media campaigns and the techniques adopted to target human minds by misinformation campaigns, malicious narratives, subversion, the spread of communal disharmony, instigating ethnic strife, etc. Identification of the targeted population and/or systems, who are affected by subversion or trolling, would help to counter its impact.

From the military point of view and to derive information advantage, there is a need to understand in detail the capabilities, capacity and trend of the flow of information of the potential adversaries to plan for IO. In a theatre of operation, all available data pertaining to the adversary's C⁴I²SR assets, fire control networks, air defence systems, communication facilities, other network-centric platforms, and war-waging machinery should be analysed. Most suitable offensive IW tools should be used pro-actively to attack the

enemy's C⁴I²SR assets, to degrade his ability to collect and process information from satellites as well as airborne and ground-based systems. On several occasions, civil resources like digital, information systems and infrastructure are utilised by the adversary to spread malicious and fake news among the population. Wherever required, such stations and infrastructure should also be declared military targets and be neutralised/engaged with PGMs, a swarm of armed drones and other means.

Based on the overall plan of operations and the movement of troops, CoG should be analysed at different stages of the battle. Deception is an extremely important facet of information manoeuvre, which should be suitably integrated with the plan. Drones are excellent platforms to be employed for reconnaissance, intelligence gathering, deception, decoys, etc. To support its own plans, the Command Information Decision Support System (CIDSS), the primary architecture that provides command, control, communications and information support for different functions at tactical, operational and strategic levels, should be protected and used extensively.

Coordination and Integration: The Game Changer

To coordinate and integrate all elements, an effective organisation is required at the apex level. IW action plan should be based on doctrine, strategy, customised organisation, its capabilities and a system to evaluate the effectiveness of own strategy; integrate and coordinate activities of all elements of IW strategy; promote research on IW and techniques employed; promote awareness of adversary's designs to the population and military personnel alike; create balanced, positive, credible ideas and narratives to counter misinformation campaigns; organise training for experts of IW organisation, cyber warriors, legal experts, media personnel and journalists; and build a network of experts to counter disinformation and malicious narratives. Towards this, developing Space and Cyber Commands and enhancing existing IW capabilities will help to address some of the requirements of conflicts and influence operations in the future. The requisite data shall ride on the backbone of Network For Spectrum (NFS) to provide increased bandwidth and seamless connectivity.³¹ Suitable interfaces with the National Information Infrastructure (NII) and Central Government Agencies will integrate them into an advanced high-speed, interactive, broadband and digital communications system.³² It will enable better coordination and exploitation of the information available at the strategic level. At the level of armed forces also, there should be an integrated organisation and approach to remain pro-active in perception management and psychological operations.

Here again, the aim of IW should be to strike at an unexpected time and place as well as create an environment of helplessness and psychological fear. IW should be employed innovatively to neutralise various networks of the adversary during critical phases, to paralyse the system for the planned duration. It would require an integrated effort by all elements of national and military power.

Terrorism and Insurgencies

India continues to remain impacted by terrorism and insurgencies, in which ICT plays a vital role, especially in J&K. Religious terrorism is a huge industry with an extensive communication network and use of the internet and social media to influence the population in real-time and to radicalise the youth and recruit them for terrorist attacks. Some would refer to them as “Digital Jehadis”. Their specialised sections carry out detailed planning to conduct propaganda and psychological operations, create narratives, and counter narratives, host malicious videos and sell credible ideas and fake news. China has been successful in imposing censorship of the internet, blocking foreign websites and social networking sites and filtering URLs. They use techniques to scan URLs and web page content for blacklisted keywords.³³ Though it is extremely difficult in India, an effort must be made to scan the digital data and malicious one should be blocked or interdicted and countered. Such digital (Jehadi) literature and virtual data should be studied by experts to formulate a strategy to deal with it effectively in a dynamic manner.

To combat terrorism and prevent religious radicalisation, the drivers of such operations like networks of funding (digital funding using Bitcoin network, etc.), terror communication networks and destruction of certain transmitting stations by technology-led systems should be targeted pro-actively. Radio transmissions, a global positioning system (GPS) as well as communication networks of terrorists should be targeted across and astride the borders to isolate them. Satellite-based systems, unmanned aerial vehicles (UAVs) and drones should be employed extensively to gain information about the terrorists, their networks and radars emitting electromagnetic waves and radio signals. These should be jammed and interdicted at crucial periods of terrorist activities and infiltration on and across the line of control. AI should monitor data, people’s identification and variation in the flow of communications and social media messages, both astride the borders and in their hinterland.

Conclusion

On balance, if offensive actions like deception, EW, PSYOPs, influence operations and physical attack on information

processes and infrastructure are employed innovatively against the adversary’s CoG, it will provide the necessary deterrence, delayed decision-making and psychological advantage. When a combination of kinetic and non-lethal IO is integrated and used as a part of the manoeuvre to gain a position of advantage against the enemy and terrorists, both in conventional and low-intensity conflicts, it will pay rich dividends. To remain ahead in mental agility and tempo of operations in all terrains, it is time to “think information and exploit information”.

India continues to face both external and internal threats and challenges to its security. The major focus of the leading militaries is in the fields of IW, cyberspace, outer space and the fusion of technologies of 4th IR. The conflicts continue to be decided by mental agility, speed and manoeuvrability of the mind. Considering the rapidly changing thrust towards information-based warfare systems in our immediate neighbourhood and to exploit the advantage of the non-kinetic information environment, our armed forces also require a cultural change to adopt the latest technologies. The security challenges presented by the information manoeuvre in multi-domain spheres and weaponised social media are an important component of cyber operations, which will require customised organisations and specialists to act pro-actively. There is, therefore, a need to revisit our doctrines, strategy, organisational structures and warfighting philosophy. IW and cyber should be a critical part of our national security architecture. An early formulation of “Doctrine of Manoeuvre in the Information Age” would be in order.

Given the variety of media capable of using [the] information to influence, coerce or deceive, it is conceivable information operations may surpass fire and manoeuvre in importance at times.

– Nick Brunetti-Lihach (2018)

Notes

1. Margarita Levin Jaitner, ‘Russian Information Warfare: Lessons From Ukraine’, Swedish Defense University.
2. *Pakistan Army Green Book 2020*, Islamabad: Crystal Printers, p. 40.
3. Lyu Jinghua, ‘What are China’s Cyber Capabilities and Intentions?’, *Carnegie Endowment for International Peace*, 1 April 2019.
4. IISS, Chapter five, ‘China’s Cyber Power in a New Era’, *Asia Pacific Regional Security Assessment*, May 2019, pp. 77-90.
5. Qiao Liang and Wang Xiangsu, *Unrestricted Warfare, China’s Master Plan to Destroy America*, 1999.
6. Patrick J Cullen and Eric Reichborn Kjennerud, ‘MCDC Countering Hybrid Warfare Projects: Understanding Hybrid

... in the Information Age

- Warfare, A Multinational Capability Development Campaign Project', 2017.
7. The US Department of Defence (DoD) defines strategic mobility as 'the capability to deploy and sustain military forces worldwide in support of national strategy'.
 8. US Marine Corps Doctrinal Publications (MCDPs) 2016.
 9. Jack Weatherford, *Genghis Khan and the Making of the Modern World*, Year, p. xvi.
 10. R Leonhard, *The Art of Maneuver*, The English Book Depot, 1998, p. 35.
 11. *Ibid.*, p. 38.
 12. Martin Samuels, *Doctrine and Dogma German and British Infantry Tactics in the First World War*, Greenwood, 1996, p. 149.
 13. William Slim, *Defeat into Victory*, Barnsley, UK: Pen and Sword Military Classics, 2005.
 14. Liddell Hart, *Strategy*, Faber and Faber, 1967, pp. 14-16.
 15. John Richard Boyd, *Destruction and Creation*, US Army CGSC, September 1976.
 16. William S Lind, *Manoeuvre Warfare Handbook*, Westview Special Studies in Military Affairs, Boulder, Colorado: Westview Press, 1985, pp. 7-8.
 17. DoD Dictionary of Military and Associated Terms, Joint Publication, 2008.
 18. Brian Nichiporuk, *US Military Opportunities: Information Warfare Concepts of Operation*, Ch. 7, p. 179.
 19. Julie Hirschfeld Davis, 'Hacking of Government Computers Exposed 21.5 Million People', *New York Times*, 9 July 2015.
 20. William Gery et al., 'Information Warfare in an Information Age', *Joint Force Quarterly* 85, NDU Press, 1 April 2017.
 21. McCormack et al., *Yearbook of International Humanitarian Law - 2003*, The Hague: TMC Asser Press.
 22. Timothy Thomas, *Russia's Reflexive Control Theory and the Military*, Francis and Taylor.
 23. M Jaitner, 'Russian Information Warfare: Lessons From Ukraine', Swedish Defense University, pp. 89-90.
 24. M Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, Rand Publication, p. 32.
 25. National Security Archive, USCYBERCOM After Action Assessments of Operation Glowing Symphony, November 2016.
 26. *Air Command and Staff College Seminar Book*, vol. 3, ver. 9, pp. 10-77.
 27. George Gilder, 'Microcosm: The Quantum Revolution in Economics and Technology', 15 July 1990.
 28. 'Hybrid Wars: Military Review', p. 107; Peter and Pindjak, 'Deterring Hybrid Warfare: A Chance for NATO and the EU to Work Together?', *NATO Review*, 5 August 2014, available at <https://www.nato.int/docu/review/2014/Also-in-2014/Deterring-hybrid-warfare/EN/index.htm>, accessed on 7 September 2019.
 29. Simon Goldstein, John Kendall, and Pragyant, Army International Seminar, 4-5 March 2020.
 30. Nick Brunetti-Lihach, 'Information Warfare: Past, Present, and Future', *Real Clear Defence*, 14 November 2018.
 31. Network for Spectrum Project for Defence Services: CCEA Approves Enhancement of Budget, 17 May 2018. The NFS project aims at laying [an] alternate communication network for Defence Services. It will lead to enhanced national operational preparedness.
 32. Department of Electronics and IT, available at https://meity.gov.in/writereaddata/les/NII_EFC_Note_and_Memo.pdf
 33. Chris Hoffman, 'How the Great Firewall of China Works to Censor China's Internet', 10 September 2017, available at <https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/>

The contents of this Issue Brief are based on the analysis of material accessed from open sources and are the personal views of the author. It may not be quoted as representing the views or policy of the Government of India or Integrated headquarters of MoD (Army).



CENTRE FOR LAND WARFARE STUDIES (CLAWS)

RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010

Tel.: +91-11-25691308, Fax: +91-11-25692347, Email: landwarfare@gmail.com

Website: www.claws.in

CLAWS Army No. 33098