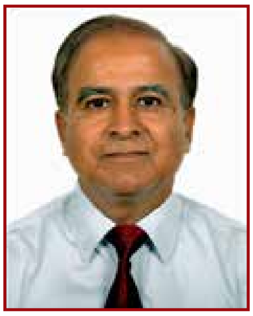
CENTRE FOR JOINT WARFARE STUDIES

Aligned with the Future ★ Victory through Joint Knowledge ★

OCCASIONAL PAPER | VOL - XII NO-3 / JUN 2018

CYBER-ALIKE NON TRADITIONAL WARS



Lt Gen Sunit Kumar, AVSM (Retd) served as DG IS (Army HQ) from 2011 to 2014 before his superannuation. An alumnus of DSSC, HC and NDC, he served in various staff, command and instructional appointments in the Army. Some of the important assignments were Sr Staff Officer (Ops) in UNOSOM-2, Director in Military Operations (MO) Directorate and Directing Staff (DS) in Higher Command (HC) Wing, Army War College, Mhow. He is currently perusing PhD in 'Cyber Warfare – Challenges and Options for India's Defence'.

> **"The victorious strategist only seeks battle after the victory has been won, whereas he who is destined to defeat first fights and afterwards looks for victory".**
>
> **-Sun Tzu**

Introduction

Cyber domain is expanding in frontage, depth and altitude, more so in techno-diversity and network-density with the emphasis shifting to technological determination rather than societal evolution, to information mobility, tailoring or exploitation rather than raw brawn power and weapon lethality, and to perception, or call it virtuality rather than widespread familiarity, or apparent reality.

Cyber warfare is fallout of cyber power, a subset of information or what Chinese term as informationization warfare and of intimate kinship to "Network Centric", "Sub Rosa", "No contact", "Unrestricted", "Electromagnetic Spectrum", "memetic" "scalar", "Cognitive", "psychological", and "Psychotronic" Warfare; besides many, indeed many, emerging variants, crossbreeds, and hybrids of the so-called irregular, or non-traditional warfare.

The technology of virtual battle arena has turned up bit-by-bit and critically, but the consequences, thereof, have surfaced at an enormous and revolutionary scale and, that too, imperceptibly. The security and warfare paradigms, though unique, are transiting ad nauseam — technologically complex in conduct, and demanding nano-second responses. Therefore, the policy perspective and action plan must follow the maxim, "Prevent or Repent".

The article covers major other non traditional wars of like genre that have caught the imagination of the soldiers and scholars. The modus operandi, that they suggest, is challenging, exigent and out-of-the-box, some even, according to the grapevine, unethical and offensive.

The War of Narratives

Modern wars are no more fought in "physical" syndrome of bare bones and guts in the battlefield. The new, nonetheless myriad ways, are astounding - some highly dexterous and sophisticated others contextually mundane, yet consequential and far reaching. The battleground is the media and the Americans refer to the hostilities as "the battle to win the narrative", wherein perception is as important to success as the actual event. For terrorists and hacktivist, the Internet and mass media have become forums for achieving their strategic and political aims. Shrewd, amongst them, lay stress on the significance of integrating combat activities into a coherent strategic communications programme.

Radical groups are not the only ones who understand the importance of dominating the media message. "It could be state" synchronising military operations with a media offensive". The battle of the narrative involve a thorough understanding of the enemy and how he attempts to influence the perceptions not only of his followers, but the global community at large. History is witness to the deeds that involve deception, convoluted endeavours to spin events, morph visuals, and spread outright lies.

Formless and deadly, the exploiters of the cyber culture are roguish avant-garde - unconventional, aggressive, and their activities often forbidden by the laws of war (jus in bello). Their targets include minorities and deprived sections of society, disenchanted youth, and people living below poverty line. The modus operandi embrace vicious cant, rumour-mongering, and inciting communal rioting.

The greatest security crisis that we face to-clay is that inflicted by media mainstream in general, "social" in particular and some privileged persona in responsible positions who use communally surcharged expressions and references like, “Islamic-terrorism”, “Jihadi-terrorism”, “Hindu-terrorism”, “Saffron-terrorism” besides, resorting to defamatory accounts about the armed forces that tell on their morale.

The debates on the TV, more so in Parliament, are battles of narrative, fought between the proponents and opponents on weighty national issues, who do not wish to listen to each other. They treat it as a forum to exhibit their psyche, borne of engrained memes - trumpeting differences on issues that are vital and critical by arguments that are trivial and irrational. Oft repeated clichés of faith and opinion certitudes are loud-mouthed. They reveal a growing discourse of politicking between those in power and those in opposition, with media anchors playing the moderator - even subjective broker. Logic is hacked by the virus of mind, carrying baggage of the past - regional, communal and castist too.

Warfare of narratives is beset by viewing history as a series of certitudes that forecloses awkward conclusions and lessons drawn. Like the present, there is no single reality that defines the past or models the future - a point to consider the next time we temperate or face a contemporary battlefield

Sub Rosa Cyber Warfare

Sub rosa is a Latin phrase that means “under the rose”, It is used in English language to denote secrecy or confidentiality. Sub rosa activities have become a byword for covert operations, usually by security services. The phrase with its allusions has been adopted by the Canadian, American and British special forces, inter alia intelligence and security outfits of other countries. In the ancient India, the epics and other literature incorporate expressions such as gupta (secret) and agyat (unknown), defining yudha (war) in the milieu, identical to sub rosa.

Martin C Libicki has written a seminal and provoking paper under the RAND label, titled, “Sub Rosa Cyber War” in which he writes, “Cyberspace offers the prospect of sub rosa warfare, in which neither side acknowledges that they are in conflict with one another or even that one side has been attacked at all. This is possible for two reasons: first, because the battle damage from some types of cyber attack may not be globally visible, and second, because attribution can be very difficult.

The reason that both sides may keep matters sub rosa is to maintain freedom of actions, on the theory that public visibility may complicate negotiations and lead to escalation. Nevertheless, sub rosa warfare has its dangers, notably a lack of the kind of scrutiny that may promote actions, which cannot bear the light of day, and the overconfident assumption that no third party is aware of what is going on between the hackers of both sides”.

Memetic Warfare

There is a chapter in Sky is the Limit: Signals in Operation Pawan entitled "Memetic Warfare". It narrates the unparallel exploits of the LTTE in the memetic warfare paradigm described as information warfare plus. Whereas information warfare is concerned with interception and manipulation of data and data processors in electromagnetic and cyber domains, memetic warfare extends it to the virtual and cognitive domains.

Meine is an information pellet, pattern or phenotype held in an individual's memory, which is capable of being passed on, replicated and propagated to another individual's mind, impacting as mindset. Although the expression is neutral, more often meme is taken to be a virus of mind, a tamsik guna. Meme warfare is a content warfare, a psychological warfare, a cultural warfare, in totality the gyan yudh, or the knowledge warfare much beyond the pale of information or knowledge warfare, the terms that have widely become popular. Strong memes are the cutting edge of cultural evolution - they change minds, alter behaviour, shift paradigms and transform societies.

The best way to explain memetics is to suggest that the brain is hardware, mind is software and meme is the data stored in it. It may be processed or unprocessed, integrity-imbued or virus inflicted. Meme is guna, whereas memeplex is sanskar, more pertinent to the collective. This could be an attribute of an "elusive mind" Or an "enlightened one," The two are mutually exclusive, the former an anti thesis of the latter, the satvik guna. Fact remains that many cyber powers and non-state terrorists, ethno religious and anti-social entities are spending a lot of money on psychotronic, cognitive and memetic warfare, much of which is hush-hush.

Scalar Warfare

"To get a basic understanding of scalar waves is to have the positive and prolific imagination suddenly run wild so as all the implications and possibilities regarding warfare fall into place. One realises with a certain horror that the world has totally changed, and that there are some very fearsome possibilities. The power for these weapons comes from the time domain, longitudinal EM waves in the vacuum of empty space - the power is tremendous and mind-boggling." Scalar electromagnetic waves are "finer than gamma rays or X rays and only one hundred millionth of a square centimetre in width. They belong to the subtle gravitational field and are also known as granitic waves. Uniquely, they flow in multiple directions at right angles off vector electromagnetic waves, as an untapped energy source called 'potentials'".

Beardon suggests, "The ordinary EM waves that we have known about, are called transverse EM waves, to distinguish them from the new longitudinal EM waves. These scalar waves do not actually exist in our "material" world, but exist only in the vacuum of empty space, or the time domain. This vacuum of space exists all through everything. Even our bodies are mostly empty space between atoms and molecules. So the gateway to this seething ocean of energy can be there at every point in the universe. This seething ocean of energy is all around us and all through us.

Scalar beam weapons were invented in 1904 by an American immigrant genius called Nicola Tesla from Yugoslavia. Since he died in 1943, many nations have secretly developed his beam weapons which now further refined are so powerful that just by satellite one can: make a nuclear like destruction; earthquake; hurricane; tidal wave; cause instant freezing - killing every living thing instantly over many miles; and cause intense heat like a burning fireball over a wide area.

The defensive weaponry can destroy an incoming nuclear missile with scalar technology before it even leaves its silo - using interference grid method it enables scalar beams to explode the missile before launch, as well as en route with knowing the right coordinates. If the target does manage to launch, what are known as Tesla globes or Tesla hemispheric shields can be sent to envelop a missile or aircraft. The envelop, so created, can chase the target. In the exploitative stratum, the weaponry induces hypnotic mind control over a whole population; or even reads anyone's mind on the planet remotely.

Chaoplexic Warfare

Chaoplexic is a derivative of chaoplexity, a compound of chaos and complexity. Scientific methods and theories have been applied to warfare since the beginning of the modern era, argues this article in the Journal of International Affairs. As a result, military thinking has evolved in tandem with scientific thinking. Currently, scientific theories of chaos and complexity, or chaoplexity, are most influential in military affairs. These stress the role of networks and the unpredictability of war.

Throughout the ages, military leaders have sought to organise and direct their armies so that they maintain order and coherence in the midst of the chaos of war. A clear parallel can be drawn with scientists' attempts to identify patterns and laws in the apparent randomness of nature. The aim, in both cases, is to increase the predictability of outcomes. "Technological innovations - from the clock to the interne - don't just change how armies fight their battles. They changed how those armies think about war", During the modern era, science has increasingly become a dominant lens through which armed conflict is contemplated. Four distinct phases of this scientific way of warfare can be identified: mechanistic, thermodynamic, cybernetic and chaoplexic.

- **Mechanistic Warfare**. This has been the overshadowing notion throughout the seventeenth and eighteenth centuries; "mechanism understood the universe as an entirely mechanical system governed by a complete and regular set of laws." By implication, 'mechanistic' warfare subscribed to the same vision, with armies emphasising rehearsed and synchronous movements, characterised by the lack of autonomy of their parts."
- **Thermodynamic Warfare**. Nineteenth century thermodynamics revolutionised the scientific worldview by contributing an understanding of the energy that drove the mechanisms of nature. Thermodynamic warfare saw the channeling of ever greater flows of energy - ballistic, motorised, industrial and moral - into war. It culminated in the Second World War and the detonation of the atom bomb.
- **Cybernetic Warfare**. Cybernetics or "the science of communications and control" emerged out of the Second World War. One of its key ideas is that the world can be understood chiefly in terms of information processing. "Cybernetic warfare saw a drive for complete predictability with the deployment of computers and automated control technologies. It was most influential during the Cold War and Vietnam War.
- **Chaoplexic Warfare**. More recently, theories of chaos and complexity (or chaoplexity) have emerged. Like cybernetics, these see information as central to understanding the world; however they stress the importance of change. Military organisation is in a continuous state of flux - continuously adjusting to its surroundings."

Chaoplexic warfare stresses the role of networks. At the turn of the 21st century, the Pentagon adopted the doctrine of, network-centric warfare and set out its vision of "swarming" and "self-synchronised" war-fighting units. Jihadist networks and insurgency movements have excelled at adopting loose, decentralised organisational structures. However, in Bousquet views, there are a number of critical weaknesses in the current application of chaoplexic ideas to warfare. There is a tendency to see information as a panacea which will permanently dispel the chaos of war, when in fact chaoplexity points to the irreducible contingency and unpredictability of war. He, therefore suggests that military strategists should focus not on particular information technologies, but on the need to organise in order to tolerate and take advantage of unpredictability."

It is heartening to observe that decision makers in India are conscious of relevance of chaoplexic warfare to employment of social media to stoke an insurgency, turmoil or disturbance. In this context, P V Kumar writes, "It illustrates how, often something innocuous can be get blown out of proportion by certain powers with an agenda using this new weapon in their arsenal. This level of social manipulation can be readily adopted by foreign powers to foment trouble well outside their own national borders. The magnitude, scale, apparent-spontaneity, decentralised nature yet well networked and coordinated nature of this attack - seem to fit well with the theories of chaoplexic warfare"

Prof Meng Xingqing suggests, "There are only a few major differences in the considerations between cyber and traditional warfare. One is in tangible space and the other intangible space. One is in virtual space and the other on the battlefield."

Unrestricted Warfare

There is a book titled Unrestricted Warfare, i.e. warfare beyond bounds, written by two high ranking colonels Qiao Liang of the PLA Air Force Political Department and Wang Xiangsui of the Guangzhou Military District PLA Air Force Political Department, published in 1999. Its primary exposition is how a nation such as China can defeat a technologically superior opponent, such as the U.S. through a variety of means. Rather than focusing on direct military confrontation, this book examines a variety of other means. Although the book is focused on the U.S. as an enemy, its advocacy of a multitude of means, particularly non-military, to strike at other enemies, which may well single out India, is equally pertinent to future conflicts.

The treatment of the complex subject displays extraordinary understanding and intellectual acuity. The authors are highly convincing in their opinions and points of view. Their examples from historical events are worth citing, and quotes merit recounting - a lot, pertinent to follow. Some forewords of translated versions and reviews have singled out the negative and unethical nuances of the work e.g., "Hacking into websites, targeting financial institutions, terrorism, using the media, and conducting urban warfare are among the methods proposed." The reviewers have, advertently, omitted, the authors' concern about these not endorsed them.

The authors rightly suggest, "The advent of bin Ladin-style terrorism has deepened the impression that a national force, no matter how powerful, will find it difficult to gain the upper hand in a game that has no rules." The U.S., on the other hand, followed the precepts in eliminating Bin Laden without any serious fall-outs or regrets in methods used.

In this age, when a surfeit of new technologies, can in turn. give rise to a plethora of new means and methods of fighting war, (not to mention the cross-combining and creative use of these means and methods), it would simply be senseless and a waste of effort to list all of the means and methods one by one. What is significant is that all of these war fighting means, along with their corresponding applications, that have entered, are entering, or will enter, the ranks of war fighting means in the service of war, have already begun to quietly change the view of warfare held by all of mankind."

Faced with a nearly infinitely diverse array of options to choose from, why do people want to enmesh themselves in a web of their own making and select and use means of warfare that are limited to the realm of the force of arms and military power? Methods that are not characterised by the use of the force of arms, nor by the use of military power, nor even by the presence of casualties and bloodshed, are just as likely to facilitate the successful realisation of the war's goals, if not more so.

As a matter of course, this prospect has led to revision of the statement that "war is politics with bloodshed," and in turn has also led to a change in the hitherto set view that warfare prosecuted through force of arms is the ultimate means of resolving conflict. Clearly, it is precisely the diversity of the means employed that has enlarged the concept of warfare. Moreover, the enlargement of the concept of warfare has, in turn, resulted in enlargement of the realm of war-related activities.

If we confine ourselves to warfare in the narrow sense on the traditional battlefield now, it will be very difficult for us to regain our foothold in the future. "Any war that breaks out tomorrow or further down the road will be characterised by warfare in the broad sense - a cocktail mixture of warfare prosecuted through the force of arms and warfare that is prosecuted by means other than the force of arms." This precisely is what cyber warfare is all about

Geophysical or Ecological War

Ecological war refers to a new type of non-military warfare in which modern technology is employed to influence the natural state of rivers, oceans, the crust of the earth, the polar ice sheets, the air circulating in the atmosphere, and the ozone layer. By methods such as causing earthquakes and altering precipitation patterns, the atmospheric temperature, the composition of the atmosphere, sea level height, and sunshine patterns, the earth's physical environment is damaged or an alternate local ecology is created. Perhaps before very long, a man-made El Nino or La Nina effect will become yet another kind of super-weapon in the hands of certain nations and/or non-state organisations.

It is more likely that a non-state organisation will become the prime initiator of ecological war, because of its terrorist nature, because it feels it has no responsibility to the people or to the society at large, and because non-state organisations have consistently demonstrated that they are unwilling to play by the rubrics of sharing the geophysical commons. Moreover, since the global ecological environment will frequently be on the borderline of catastrophe as nations strive for the most rapid development possible, there is a real danger that the slightest increase or decrease in any variable would be enough to touch off an ecological holocaust.

In an interview, Qiao was quoted as stating that "the first rule of unrestricted warfare is that there are no rules, with nothing forbidden." The authors note that an old-fashioned mentality that considers military action the only offensive action is inadequate, given the new range of threats. Instead, they advocate forming a "composite force in all aspects related to national interest," and adoption of a "grand warfare method", which combines varied dimensions and methods in the two major areas of military and non-military affairs so as to carry out warfare. "This is opposite of the formula for warfare methods brought forth in past wars."

It would be presumptuous to reason that China alone pursues "all is fair in war" precept. Colonel Charles W Williamson III "has written a paper in Armed Forces Journal to suggest that America needs the ability to "carpet bomb in cyber space" to create the deterrent Americans lack."

Fault-Line Warfare

We need to gain a deep and nuanced understanding of any conflict we are about to embark on and acquire as thorough a grasp of the nature of the adversary as possible. This includes becoming well-informed about the culture of the adversarial social and political systems.

This will help us in the future, due to the nature of what Harvard's Samuel Huntington calls "fault line wars" - howsoever he faulted in its conceptual generalisation. These are the sort of religiously divisive conflicts that our western neighbour manipulates, exploits and often bets about. Such wars are protracted, violent and highly contagious. Unfortunately, these are exactly the kinds of fights - we may be involved in the future too.

Fault-line wars place a premium on an in-depth knowledge base of the other component of a nation's strategic culture - its societal culture. This is not a new thought, as Michael Howard stressed many years ago, “Wars are not tactical exercises writ large. They are ... conflicts of societies, and they can be fully understood only if one understands the nature of the society fighting them. The roots of victory or defeat often have to be sought far from the battlefield, in political, social, or economic factors.” Cyberspace and digital zone are ideal arenas to pursue the endevour or the design.

Rudolph C Heredia has written a book called, “At the Fault Lines: Taking Sides: Reservations Quota and Minority Rights in India. This too, is in line with the Huntington’s thesis, though specifically targeted at the prevailing socio-political state of affairs in India. He maintains that governance in India has been a legacy and hang-up of its colonial past and that obfuscation of the colonial past and post colonial state forms the moral basis for revamping state-society relations for giving a call for second freedom struggle. The very idea is weird as the reviewer, Majibir Rehman rightly questions as to whom such a struggle needs to be launched against and the kind of strategies required thereof.

The academia talk of struggles and human rights but fail to address the fundamental right to security of the collectives in the form of a nation, a state or a community. The fault lines have become a metaphor by the academia to label dissensions in society in a bizarre way and sensationalise the erstwhile communal, ethnic and caste-based conflicts. Admittedly it is a legacy of the Raj, but equally a bane of the Westminster model of parliamentary system of democracy, which we have adopted - further maimed and corrupted by polarised public discourse and endemic walkouts, Media and academia are often at cross purposes to good governance, so is public woo do vis-à-vis national discipline.

Fault line war is fallout of protracted social conflict - a theoretical concept evolved by Edward Azar. It generally refers to conflicts described as protracted or intractable, i.e. as complex, severe, commonly enduring, and often violent. It denotes hostile interactions between communal groups that are based in deep-seated racial, ethnic, religious and cultural hatreds, and that persist over long periods of time with sporadic outbreaks of violence.

Hybrid Warfare

The advent of Internet attacks, especially those suspected of being directed by nations, not hackers, has given rise to a new term inside the Pentagon and the NSA, vis. “hybrid warfare.” Hybrid threat is defined by the NATO as follows, “A hybrid threat is one posed by any current or potential adversary, including state, non-state and terrorists, with the ability, whether demonstrated or likely, to simultaneously employ conventional and non conventional means adaptively, in pursuit of their objectives."

Obviously, we must not be merely content with being familiar with the term - the way it has been coined and expounded by the U.S. and since appropriated in practice by our adversaries, but that it is pertinent to us too. We in India need to understand its exploiting nuances, strategic implications and repercussions for not giving it primacy in our doctrine

Other Types of Warfare

Aside from what has been discussed above, a number and variety of other types of war, can be enumerated, which apparently are cubby-holed as non-military but directly impact on national security. In India's case, history is witness to several of these being forced, e.g., cross border raids to loot, trade wars as a prelude to Imperial designs, cartographic war as a lead up to aggression in 1962, terror attacks master-minded in Pakistan, capturing of Indian market by China - many persist and some varieties may roll up in the future. Such means and methods include:

- **Psychological Warfare**. Spreading rumors to intimidate the opponent and break down his morale.
- **Psychotronic Warfare**. Hacking adversaries' and opponents' minds.
- **Market Warfare**. Capturing markets or throwing them into confusion and imposing politico-economic disorder.
- **Media Warfare**. Manipulating what people see and hear in order to lead public opinion astray.
- **Monopoly Warfare**. Creating lobbies, and interest groups to set standards in unfair competition to the developing markets.
- **Fraud and Falsehood Loaded Diplomatic Warfare**. Presenting a poker face: counterfeit appearance of real motives and intentions to hoodwink the diplomats of adversary or neutral nations.
- **Economic Aid Warfare**. Overtly, bestowing economic favours; covertly, contriving to control matters otherwise.
- **Cultural Warfare**. Steering or exploiting ethnic cultural traditions, trends and tendencies with a view to espousing and enforcing those with intrusive and insensitive outlooks of intolerant social and cultural entities.
- **Cyber Legalities Warfare**. Cyberspace is conceptually pregnant with illogicalities and intrinsic vagaries of its stretch and scope. Essentially, it involves understanding the behaviour of

humans dovetailed in analytics of big data captured by the machine - a consummate skill a la chess masters. Obviously, it is beyond the legal cognisance of thinkers and practitioners of law.

Conclusion

Not only the raison d'être of armed forces, but also governance in all its spheres of influence and the economy in all its growth-prospects, are an upshot of the security paradigm. There cannot be inclusive growth without all-encompassing governance and there cannot be either, without inclusive, all-encompassing, and wide-ranging cyber security.

It postulates that cyber security should be proactive, rather than reactive; and inter alia, suggests dynamic decision-making and timely responses, queering the pitch of warfare in all its domains and manifestations - be they physical or virtual, territorial or global-commons, internal law breaks or external power-projection.

This calls for an understanding of world-wide overt and covert initiatives, and at home, synchrony of security, pro-active defensive and preventive offensive strategies. A comprehensive, joint and Ludo-centric "policy initiative", is the need of the hour. It would embrace all the stakeholders in its fold, identifying threats, vulnerabilities and challenges, exploring schema and stratagems and positioning structures to overcome them.

The views expressed are that of the author.

CENTRE FOR JOINT WARFARE STUDIES
Kashmir House, Rajaji Marg, New Delhi-110 001
Tel. Nos : 011-23792446, 23006535, 3306538/9, Fax : 011-23792444
Website : http://cenjows.gov.in, e-mail : cenjows@yahoo.com

www.xtremeonline.in # 9811707220