<u>AN INTEGRATED APPROACH TO INFORMATION WAR - INDIAN CONTEXT</u>

We live in an age that is driven by information. Technological breakthroughs . . . are changing the face of war and how we prepare for war.

--William Perry, Secretary of Defense, USA

Post Pulwama terrorist attack, the Indian Air Force precision strikes at Balakot once again demonstrated a Politico-Military resolve for punitive action against Pakistan perpetuated terror attacks. The Balakot Air Strikes were like the Sep 2016 surgical strikes, well executed achieving the intended objectives with no collateral damage. However, there is a major difference between the 2016 surgical strikes post Uri terror attacks and the Balakot Air Strikes.

The surgical strikes were and are a total and complete success in all domains. Well planned and executed much like Balakot Air Strikes, Indian DGMO went public over the surgical strikes within hours of the successful termination of operations, categorically signaling to Pakistan, the international community and the Indian Public that the strikes were executed successfully and operations terminated. The information operations were well thought out and planned in concert with the military operations, taking Pakistan by surprise, who continued to be in denial mode, a story which did not go down well even within Pakistan. India for once had not only demonstrated a politico-military resolve at the strategic level but also achieved synergy between all elements of National Power i.e. Diplomatic, Informational, Military and even economic. This of course was not the first time that information domain was fully optimised and exploited by the national leaders and the armed forces. The media played a stellar role during the 1999 Kargil war acting as a force multiplier, contributed in achieving the near impossible - recapturing the Kargil heights. The Army was quick for once to comprehend the power of IW quickly establishing and empowering the Army Liaison Cell (ALC) under the Director General Military Intelligence. Gen (then Colonel) Bikram Singh became the face of the army operations during the Kargil war conducting the daily briefings with a frankness and finesse rarely associated with the military, contributing to the much needed credibility of operations furthering a well thought out narrative. The ALC went on to become today's ADGPI.

The key question remains as to what happened post Balakot. Indian Air Force executed the effective strikes but as a nation we won the battle but seemingly lost the war, on account of inaction/ paralysis in the informational domain. Pakistan on the other hand apparently having learned the lesson post URI was the proverbial 'Fastest Finger First' with the DGISPR Maj Gen Gaffoor taking to twitter, within hours, announcing to the world that though Indian Air Force carried out strikes at Balakot, the strikes however failed to cause any damage whatsoever harming a few trees. The Indian action or rather reaction was slow with a crisp statement by the foreign secretary later in the day. Post Balakot the Pak DG ISPR was constantly and continuously briefing the media including the 27th Feb so called retaliatory strikes by PAF and the Dog flight.

For reasons best known the Indian Official machinery pressed the mute button, giving rise to speculations and conjecturing and a skewed perception of the unfolding events. Starved of official briefings the media was left with no choice but to feed the public what in their perception was contributing to the national objectives. In fact India lost the information war even though the Balakot strikes were a total success. The centrality of the narrative should have always remained 'Pulwama' like 'Uri' as it was the jus ad bellum. However, due to a lack of Information War (IW) structures and a well thought out plan, the narrative kept shifting from Pulwama to Balakot, and from Balakot to downing of F-16 to Wing Commander Abhinandan's capture and return. The international media bought the Pakistan narrative for no other reason, but as that was the only narrative forthcoming. India needs to revisit, study and learn the right lessons and create effective structures and information war plans for the future.

Information wars have been historically an integral part of all wars. The earliest recorded account of exploiting the Information domain can be traced back the epic ‘Mahabharat’. On the 10th day of the war, after Bhisham falls, Drona is named the supreme commander of the armies. Krishna knew that it was not possible to defeat an armed Drona. So, Krishna suggested to Yudhishtra that if they can convince Drona that his son Ashvatthama was killed on the battlefield, then his grief would leave him vulnerable to attack. Krishna hatched a plan for Bhima to kill an elephant by the name Ashvatthama and then asking Yudhishter to announce the death of Ashvatthama, knowing well that Drona will believe whatever Yudhishter says to be true. This announcement convinced Drona that his son Ashvatthama is dead, thus leading to the fall of Drona and Kauravas. Information warfare, while a relatively new doctrinal term in the military lexicon, is as old as warfare itself. The Trojan horse of Homer’s *The Iliad* is one the most well known examples of classical information warfare in literature, but military history is filled with non-fictional examples [1].

According to Sun Tzu, the ancient Chinese military theorist and philosopher, believed that “all warfare is deception,” in essence stating that warfare itself is based on the use or misuse of information, as well as military prowess. In the 20th and 21st centuries, the nature of information warfare further evolved, especially in the areas with mass communications, radio and electronic communications technology, and the application of marketing techniques to influence specific and general audiences.

New age warfare is equally a war of narratives, where fires are brought to bear not only in the kinetic domain but also in the virtual domain.

---

[1] War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century Hardcover – November 14, 2017

by David Patrikarakos

Today's world is an interconnected networked world with billions having easy and instant access to numerous apps feeding their narratives and perceptions of events and happenings around the world. Whether you are a strategist or a terrorist, if you don't understand how to deploy the power of social media effectively you may win the odd battle but you will lose a twenty-first century war. Journalist David Patrikarakos draws on unprecedented access to key players to provide a new narrative for modern warfare. He travelled thousands of miles across continents to meet a de-radicalized female member of ISIS recruited via Skype, a liberal Russian in Siberia who takes a job manufacturing "Ukrainian" news, and many others to explore the way social media has transformed the way we fight, win, and consume wars-and what this means for the world going forward. Social media has given rise to millions of keyboard warriors and will shape public opinions as also outcomes of future conflicts. The key battle areas in future wars is not in the five known domains of warfare (land, air, sea, space and cyber) but is in public perception. The target of the information war is not only the armed forces but the whole nation, the world at large and the domestic opinion. Perceptions are significantly more important than reality and manipulated perceptions can change the narrative built on facts.

Today, the information age offers new challenges and opportunities. Cyberspace, Artificial Intelligence, advanced computing, mobile networks, unmanned and autonomous systems, and social media present a military revolution in information warfare. To leverage its full potential, militaries need cultural changes to reconcile institutional aversion toward non-lethal information warfare. To aggressively shape, influence, control, and manipulate information, change is essential in military mind sets toward information warfare. This can be realized through better training and education, and deliberate integration of information operations across the military services during planning and operations.[2]

[2] https://docs.google.com/document/d/1WrVkxJvDBglACrKqabgjPoXVhxGn_IJ9cGyOK-a1Ox4/edit

The Basic Features of Information Warfare are :-

- *Low entry cost:* Unlike traditional weapon technologies, development of information-based techniques does not require sizable financial resources or state sponsorship. Information systems expertise and access to important networks may be the only prerequisites.
- *Blurred traditional boundaries:* Traditional distinctions--public versus private interests, warlike versus criminal behavior--and geographic boundaries, such as those between nations as historically defined, are complicated by the growing interaction within the information infrastructure.
- *Expanded role for perception management:* New information-based techniques may substantially increase the power of deception and of image-manipulation activities, dramatically complicating government efforts to build political support for security-related initiatives.
- *A new strategic intelligence challenge:* Poorly understood strategic IW vulnerabilities and targets diminish the effectiveness of classical intelligence collection and analysis methods. A new field of analysis focused on strategic IW may have to be developed.
- *Formidable tactical warning and attack assessment problems:* There is currently no adequate tactical warning system for distinguishing between strategic IW attacks and other kinds of cyberspace activities, including espionage or accidents.
- *Difficulty of building and sustaining coalitions:* Reliance on coalitions is likely to increase the vulnerabilities of the security postures of all the partners to strategic IW attacks, giving opponents a disproportionate strategic advantage.[3]

Information warfare (IW) represents a rapidly evolving and, as yet, imprecisely defined field of growing interest for defense planners and policymakers. The source of both the interest and the imprecision in this field is the so-called information revolution--led by the ongoing rapid

---

[3] **Strategic Information Warfare: A New Face of War**
Roger C. Molander, Andrew S. Riddile, Peter A. Wilson

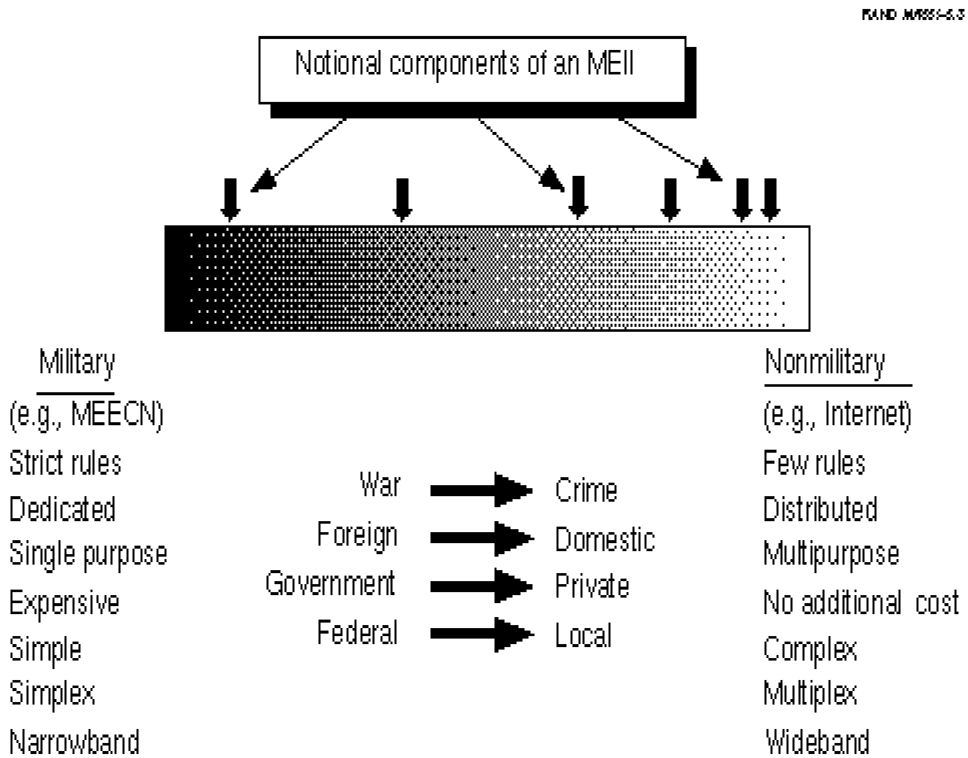
evolution of cyberspace, microcomputers, and associated information technologies. The US in January 1995 through the Secretary of Defense formed the IW Executive Board to facilitate "the development and achievement of national information warfare goals."[4] The IW Board widely agreed that an immediate and badly needed first step is the assignment of a focal point for federal government leadership in support of a coordinated U.S. response to the strategic IW threat. This focal point should be located in the Executive Office of the President, since only at this level can the necessary interagency coordination of the large number of government organizations involved in such matters--and the necessary interactions with the Congress--be effectively carried out. This office should also have the responsibility for close coordination with industry, since the nation's information infrastructure is being developed almost exclusively by the commercial sector. Once established, this high-level leadership should immediately take responsibility for initiating and managing a comprehensive review of national-level strategic information warfare issues.[5] The US has created structures for this all crucial domain of IW with directions and control resting at the White House itself.

A recommended structure elaborated in a RAND paper of a Spectrum of National Security Preparedness in the IW domain is as under:-

---

[4] Information Warfare: A Philosophical Perspective
Mariarosaria Taddeo, Springer-Verlag 2011

[5] Ibid



https://www.rand.org/pubs/monograph_reports/MR661/index2.html

India and Indians contribute to a vast majority of smartphone users the world over, touching 50 million and growing exponentially. This resource needs to be tapped, and for that we not only need understanding and assimilation of this domain of warfare but formal structures to exploit IW as an essential element of not only National Power but a strategic tool of war fighting. In addition, what is equally important is that the structures also defeat the designs of adversaries in manipulating the perceptions of Indian public. social media platforms are also being used by pro-Pak lobbies to circulate misinformation and fake videos to create apprehensions, exploit and manipulate perceptions and public opinion. Information is so heavily bombarded with aggregated impressions through social media platforms that it becomes almost impossible not to be influenced by the constant flow of impressions being made with images, headlines and fake videos. The impact of cyber –led influence operations can adversely affect the decision making process and in critical times it can seriously limit the options.[6] Hence, countering them is a necessity. The disinformation campaign cannot be countered by mere refutation but needs credible alternate narratives.

This demands an integrated effort not only by the armed forces but at all levels of the Government with directions emanating from the very top. The Control and coordination has to flow from the apex level which is the office of the Prime Minister. At the governmental level, India needs a clear strategy to counter this threat with a defined responsibility to an organisation to deal with both defensive and offensive operations in this sphere. The real challenge for the nation is to prepare to fight in fifth (cyber) and sixth domain (perception) of warfare.[7]

The nation and armed forces need IW structures to effectively exploit the IW domain as an integral component of our war fighting strategy as also counter the inimical designs of our adversaries. The PMO with the NSA as the pointsman should head the integrated IW Board comprising of the three operations chiefs of the services ie DGMO, VCAS, VCNS, Director General Defence Intelligence Agency, Director General Information Warfare, secretary of the Ministry of Defence, Home, External Affairs, Finance and I&B. The IW board could also eminent media persons either as members or advisors. The IW Board should draw its authority and take directions from the CCS and function directly under the PMO. The IW board should have the requisite mandate, authority and constitutional sanctions to project and protect Indian national interests.

At the services level the Headquarters Integrated Defence Staff (IDS) should have the mandate and authority to synergise IW. The need is to raise a Director General Information Warfare under the IDS with three verticals, Additional Director Generals of Social Media, Psychological

---

[6] **https://timesofindia.indiatimes.com/blogs/ChanakyaCode/balakot-and-after-pakistan-intensifies-information-war-against-india/**

[7] Ibid

Operations and Public Information. The Armed forces should not shy away from appointing subject matter experts in the three verticals and should willingly accept the induction of media and other experts as an integral part of IW.

Finally, however, it must be acknowledged that strategic IW is a very new concept that is presenting a wholly new set of problems. These problems may well yield to solution--but not without the intelligent and informed expenditure of energy, leadership, money, and other scarce resources that are required to integrate and exploit the all critical IW domain.

WORDS -2299

Lt Gen Vinod Bhatia, PVSM, AVSM,SM (Retd)

Director CENJOWS