SYNERGY

JOURNAL OF THE
CENTRE FOR JOINT WARFARE STUDIES

CENJOWS
(Established : 2007)

Centre for Joint Warfare Studies (CENJOWS)
Kashmir House, Rajaji Marg, New Delhi 110011
Telephone Nos : 011-23792446, 23006538/9
Fax : 011-23792444
Website : www.cenjows.gov.in
E-mail : cenjows@cenjows.gov.in

Synergy is a bi-annual Journal that is published in Feb & Aug every year. It is supplied to the members of CENJOWS. Articles, Book Reviews, abridged version of Research Papers and Dissertations may be sent to the Editor as per the guidelines contained in the Journal. Advertisment enquiries concerning space and charges may also be sent to the Editor.

The Centre for Joint Warfare Studies (CENJOWS) is an independent, professional research institute established in 2007, in pursuit of strengthening the concept of 'jointness' within the defence force, as well as with other agencies that jointly contribute towards a nation's war fighting capability. SYNERGY is the CENJOWS Journal that strives to expand and deepen the understanding of issues concerning defence, national security and civil-military interface which are so very essential for joint war fighting.

Price : **Rs. 200/- INR or US 10$**

INFORMATION WARFARE AND INFLUENCE OPERATIONS IN INDIAN CONTEXT

CONTENTS

FOREWORD

Information Warfare (IW) represents a rapidly evolving and, as yet, broadly defined field or growing interest for defence planners and policy makers. This information revolution is led by the ongoing rapid development of cyberspace and associated information technologies.

Extensive use of television during the Gulf War of 1991 brought war to every household for the first time in history. The concept of embedded TV reporters started since then. The same concept was adopted during the Kargil conflict of 1999 and this methodology apart from telecasting war live, also helped shape public perception about the 'Just Cause'.

Employment of information warfare and influence operations prior to, during and after the conflict situation bears a resemblance to the election propaganda. Adversaries try every possible means to convince the opponent, international fraternity and their own population about the righteousness of their cause, the wrong done by the opponent and upper hand achieved during the process. Information warfare is indeed closely linked to Psychological warfare. Sun Tzu, wrote many years ago that "The supreme art of war is to subdue the enemy without fighting", and that best suits Information Warfare (IW) and Influence Operations (IO) as, IW and IO take place without kinetic violence, below the threshold of armed conflict.

India has also used the information resource to its advantage on all possible occasions. During the 1999 Kargil war, the media too

played a battle winning role. The Armed Forces fully exploited the potential of IW, facilitating the visit of media teams to the frontline and feeding the media with daily updates and press briefs. India has faced the onslaught of an adversary's information war on several occasions. Chinese propaganda during Doklam standoff is one recent example. Manipulation of information to its advantage by the Pakistan post Balakot strike by the IAF is another example.

Information has been used by the adversaries in almost all wars. India established the National Information Board (NIB) in 2002, which is chaired by National Security Adviser. The NIB is the highest policy making body for cyber security and IW and periodically reports to the Cabinet Committee on Security. The NIB's capabilities for countering Information Warfare and Influence Operations need to be enhanced significantly. There is a felt need for synergizing the Indian Govt apparatus to fine tune India's Information Warfare and Influence Operation Strategy. The Aug 2019 issue of the synergy journal is devoted to "Information Warfare and Influence Operations in the Indian Context". The subject has been studied from all angles by renowned experts and nine articles on different aspect have been compiled in this issue. I am sure readers will find the articles interesting and informative.

(PS Rajeshwar)
Lt Gen
CISC & Chairman CENJOWS

INFORMATION WARFARE IN KASHMIR

Lt Gen Mukesh Sabharwal, PVSM, AVSM (Retd)*

The Changing Nature of Conflict

The end of the World Wars and the closure of the Cold War in the last Century have brought about a paradigm shift in the nature of conflict. In an increasingly globalised world, the new security challenges are products, not of conventional inter-state rivalries, but of economic, demographic and societal tensions that are trans-national in nature. With its neighbourhood being politically unstable, India faces a monumental challenge of increasing involvement in sub-conventional and asymmetric warfare.

Technological advances in capabilities; communications, trans-national travel and networking have enabled a global access to terrorists. A younger, better educated, indoctrinated, probably radicalised and intellectually proficient profile is one that fits the modern day terrorist. In the past twenty years, the probability of a terrorist organisation detonating a chemical, biological or nuclear weapon has risen sharply. Terrorists are in a better position to acquire critical technologies and transport them internationally using clandestine means. With greater dependence on the internet and social media as part of the Information Warfare, it is presumed that manufacture, deployment and initiating such a weapon to cause a WMD attack is much easier and possible today than ever before. Cyber warfare is no longer in the realm of imagination but is being employed as a preferred form of attack.

Popular support in an insurgency is not only desirable, it is essential to the terrorist. He looks for crowds to close around him to engage the security forces and people to give him shelter. Public panic magnifies the terrorist's power manifold. One of the methods of disseminating the effects of a terror attack has always been the media. Unfortunately, these channels of awareness and information also become carriers of fear. As experienced with the 9/11 and the 26/11 attacks, terrorism entails a prolonged urban confrontation that exposes the inability of security forces to cope with the volatility of the terrorist due to the completely unexpected nature of the attack. Even though they are eventually successful in eliminating the terrorists, initially the security forces have to deal with combating them. The violence is covered extensively by news channels, reaching audiences across the world and indirectly multiplies the number of targets. Vernacular media has wider acceptance amongst the population and plays a critical role in swaying the fence sitters.

The bigger menace these days is the exploitation of the social media by the terrorist organisations. Mobile phone and laptop savvy youth are easily influenced and the reach is wider and quicker. The veracity of information being authentic is doubtful but perceptions can be altered irrespective of its credibility. For the security forces to wean away public support from the terrorist, their perceptions will have to be changed. Psychological operations therefore form an intrinsic part of the long-term information warfare and counter terrorism strategy. On one hand it should be transparent and overt to indicate the necessity of the political or military actions being undertaken; on the other hand, it will have to undertake activity that gradually alters public perceptions or undermines the values and ideology of the extremists and terrorists. This should eventually lead to lowering the morale and effectiveness of the terrorists and their supporters as well as instill confidence in those combatting insurgency and terrorism.

The terrorist philosophy is to provoke an over-reaction and if that happens, blame the Government for being repressive. The overall response to terrorism has to be a holistic, whole of government approach. It is absolutely essential to harmonise and coordinate diverse responses to terrorism in a comprehensive, all-encompassing policy for effective implementation. Following democratic processes within the framework of the Indian Constitution and rule of law will be the cornerstone of the counter terrorism policy, to include any strategy on sub-conventional warfare, information warfare or the like.

Information Warfare

Any branch of warfare has some basic fundamental concepts that must be followed in order to succeed. Whereas information is concerned, the first and foremost step is to acquire every bit of knowledge about the adversary. The second step is to ensure that he does not know about you or your intentions, that is denial of information. To deny such information, one has to employ passive or preventive measures as well as active or deception measures to thwart the enemy's attempts. The most important aspect of information warfare however, is to access into the mind of the opponent, discern his intentions and disrupt his plans before they are unleashed or take pre-emptive actions to reduce their effects.

Information warfare has been defined as "all actions taken to defend the military's information-based processes, information systems and communications networks; and to destroy, neutralize or exploit the similar capabilities of the enemy within the physical, information and cognitive domains".[1] The United States Department of Defense defines Information Operations (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"[2]

Monitoring media networks and the progress of changing sentiments gives military planners an opportunity to better understand how and where these agencies and individuals are working to influence public opinion. Not only does this data help to counter their campaigns, but they also reveal the issues that adversaries find most important. One medium that is unique in its ability to rapidly spread images, though these images are often misleading or posted without context is social media. A single photo or short video can act as a powerful device to alter how the public conceptualizes an issue.

Social media is used as a tool of information warfare, a weapon of words that influences the hearts and minds of a target audience, and a weapon of mass disruption that can have effects on targets in the physical world.[3] Low-cost, easily accessible social media tools act as a force multiplier by increasing networking and organizing capabilities. The ability to rapidly disseminate graphic images and ideas to shape the public narrative transforms social media into a strategic weapon in the hands of terrorists, insurgent groups, or governments engaged in conflict. Facebook, Twitter, YouTube and the like are used to identify, radicalize, and recruit new warriors; provide training tools and resources for the radicalized; raise money; publicize successes; and shape public perception regarding ongoing hostilities.

However, if one was to define “social media” as a term, it could be summed up either as a “collection of online communication channels dedicated to community based input, interaction, content sharing and collaboration”[4] or as “web-based communication tools that enable people to interact with each other by both sharing and consuming information”.[5] Social media doesn’t just give information, but interacts while giving information. Regular media is a one-way function where the user has very limited ability to interact. Social media, on the other hand, is a two-way function that gives you the ability to communicate too.[6]

The ever-present, instantaneous nature of social media with its deep penetration makes it perfect for application in numerous areas of military establishments. In addition, the Internet has highlighted the power of information operations. Internet fueled social media platforms are the most seamless, swift and substantial, thus making them the most influential tools of communication.

Analysis of the Influencing Perceptions in the Kashmir Valley

In early 2008, there was a general feeling all around that normalcy was returning to the Kashmir Valley. Violence levels were low, infiltration well in check, the line of control relatively quiet and the Muzzafarabad–Srinagar bus service operating smoothly. Other indicators of normalcy like the tourist inflow into the Valley over the previous couple of years, the pilgrim numbers for the Amarnath yatra, and encouraging trade figures further reinforced this belief. The situation however received a setback when the Shri Amarnath Shrine Board land transfer controversy sparked off widespread agitations. The separatists led by the hardliner Hurriyat leader Syed Ali Shah Geelani and moderate Mirwaiz Umar Farooq declared that the land transfer order was an attack on Kashmiri identity aimed at demographic reorientation of the Valley. This led to large-scale protests forcing the State Government to relent and revoke the order. It was hailed as a triumph of street power in the Kashmir Valley, but the same order sparked violent unrest in the Jammu region with political parties and interested groups whipping up religious and regional passions.

The land controversy acted as the accidental trigger that was cleverly exploited by the Hurriyat who prior to the agitation were effectively marginalized. The main regional political parties too tried to extract maximum political mileage in an election year. The crowds were not spontaneous but were spurred by the separatists, even by coercion, intimidation and money power. The protests in Jammu as a

consequence created panic of an economic blockade and came as a shot in the arm for the separatists who got an opportunity to polarize the Kashmiris by portraying the land transfer row as a “Kashmir versus India” issue. The separatists succeeded in reviving the latent sentiments of regionalism, communalism and separatism in the State. Many Kashmiris believe that the movement has failed to achieve anything politically viable despite the sacrifice of tens of thousands of Kashmiris in the two decades proxy war waged by Pakistan. The discontentment, therefore, keeps simmering and gets ignited by trivial issues. Even normal protests against any administrative failure also start echoing the Azaadi sentiment. A large majority demand Azaadi, but not all among them know what exactly it means. Azaadi does not necessarily mean secession from India except to Geelani and his followers. For most it implies freedom from police atrocities and security forces against whom they have perceived or real grievances.

The following two years were traumatic only in parts but had a significant impact on the normalcy that was threatening to wash away the separatists’ influence. 2009 saw the alleged Shupiyan double rape and murder controversy and 2010 witnessed the unfortunate death of a young boy called Tufail Mattoo, who was a victim of a hit by a tear gas shell. If this was not enough, the Macchil fake encounter case raised a public outcry. Each of these incidents led to stormy stone pelting especially by students and the inevitable police actions that resulted in more casualties. The elusive peace was shattered by the news of the hanging of Afzal Guru in 2012 and there was yet another opportunity for the separatists and terrorists to act within the Valley.

By the middle of 2015, the security situation was relatively under control as a result of concurrent factors. The most significant reason was the high tempo of security forces operations and steady attrition of terrorists within J&K. Whereas statistical inputs of terrorist strength indicated a downward trend, local recruitment, agitation incidents and radicalisation increased significantly, especially in the Kashmir

Valley. Pakistan continued to project the insurgency as indigenous and supported the call for azaadi.

What is evident to note here is the transition to the use of technology and a variety of media by the militants aided by the Pakistan ISI and the ISPR to quicken communication and spread of information and misinformation particularly in Kashmir. Unprecedented crowds gathering for funerals from across the entire Valley in a rather quick time frame suggested a well-coordinated exercise using all types of communication including social media and mobile phones that had been introduced in Jammu and Kashmir in the year 2003. Today there are more than 10 million cell phone connections due to the availability of affordable mobile phones. NIA has said, that besides phones, WhatsApp is being extensively used to encourage and provoke stone pelters and collect instant flash mobs, and the sponsors incite them to near hysterical behaviour.

2016 saw a sharp increase in local support, specially the youth being attracted to militancy and joining terror groups, mainly Hizb-ul-Mujahideen. Social media has gained tremendous appeal and it gets accentuated due to unemployment, corruption and lack of education. Closure of cinema halls and other means of entertainment being largely unavailable, participation in agitations and stone throwing is an attractive occupational engagement that also provides some monetary incentive.

There was increasing communal and political polarisation and even a minor incident could potentially trigger a sensitive situation to explode in both the Kashmir and Jammu divisions. Anti-India statements by leaders were on the rise. Even a supposedly moderate leader like Mirwaiz Omar Farooq issued over a dozen anti national pronouncements in that year itself. There was a sharp growth of madrassas and masjids without any accounting or monitoring. Friday prayers were always significant but stone throwing at the end of it

started becoming a regular affair primarily due to the indoctrination spread amongst the congregation. Radical groups freely used social media for their propaganda and the authorities were unable to stop them, as the servers were located outside India, beyond their control. Also, any attempt at curbing social media creates a furore in the civil society, making the task of the authorities and the armed forces that much more difficult. A small incident or event can be blown out of proportion and context in no time, resulting in knee jerk reactions at all levels. The incident of a Kashmiri youth tied to front of an army jeep spread like wild fire creating negative publicity for the Indian Army even before the context and purpose could be determined. This just showcases that the party who is quick enough to exploit the power of social media and post in its point of view first is able to sway public opinion and sentiment irrespective of the facts.

The Pulwama attack of 14 February 2019 has important lessons for the nation. Adil, the suicide bomber, was seen speaking in a video clip that went viral. The video was maliciously recorded, with a criminal intent, circulated and made viral for purposes of disinformation and virulent propaganda. It is also noteworthy, that Adil was radicalised to the extent that he became a suicide bomber, even though suicide is strictly forbidden in Islam.[7]

The Strategy

Having understood the philosophy and concept of information warfare in this day and age, it was important to first identify the problem and analyse the changing perceptions both within the Valley and externally. The strategy to take control over the information space has to be adopted akin to a boxer fighting in a ring. Starting from acquiring knowledge of the opponent's acumen; carrying out adequate preparation; fending off blows while taking some on the chin; outwitting him mentally and finally defeating him by employing calculated offensive technique with grit. As is known, the boxer is not alone in this effort but has a complete team

backing him up for the purpose. Inevitably it has to be a holistic, whole of government approach.

While the overall strategy would cover many dimensions, this paper shall address a few significant issues like counter radicalization, counter narratives and changing mindsets by effectively harnessing the power of social media.

Counter Radicalisation

Radicalisation is considered to be a process whereby a person increasingly accepts the use of violence including support to terrorism and other forms of extremism to achieve political, ideological or religious goals. Drivers of radicalisation are ideology, narratives and religious literature communicated by means of latest technology. Amongst the many advantages of the Internet exploited by the terror groups are: lack of regulation of censorship; anonymity; no physical contact; fast transmission multi media information; geographically dispersed audience; and ease of access. The process of radicalization occurs at the levels of the individual, the group or entire community although in a varying time frame and degree. Fighting radical elements and ideologies is as important as rehabilitating those who are misguided or exploited.

Counter radicalisation addresses the source of the radicalisation or the process whereas de-radicalisation addresses the individual. Thus a counter radicalisation programme is a proactive action compared to de-radicalisation, which is more of a reaction to an external activity. This can be achieved by exploiting the Internet and social media; confronting the radical narrative by empowering the local teachers, respected clergy and wise old folks of the community.

Ideology plays a very significant role in alienating the population and it is also very clear that radicalization is a major driver of alienation.

Speaking at the Chandigarh Literary Festival in December 2018, Gen Ata Hasnain, a seasoned expert on Kashmir, opined that radicalisation couldn't be neutralized without a full involvement of the clergy, elders and supporters of traditional Sufi Islam that always existed in Kashmir. An elaborate information machinery is required to counter the radical campaign that has already taken a head start. Information operations need to be conducted in a structured manner with clarity of purpose. The military and intelligence agencies could provide the leadership but the basic element must be civilian in essence as part of an overall government approach. India has no dearth of learned Islamic scholars of international repute and credibility. The government should galvanise and have a dedicated group of Islamic scholars, who should operate round the clock and address every piece of poisonous information that is being spread by Pakistan and ISI. They can demystify perpetrated myths and provide the true interpretation of terms like jihad, jannat and fidayeen.

Sentiment analysis is a vital aspect of social media domain that needs specialized attention. The player who gauges the sentiments of the populace and turns them in his favour is most likely to succeed. Generating appropriate content and designing relevant, contemporary themes has to be entrusted to experts, usually young creative minds who enjoy doing this kind of a job as it provides them an avenue of release and contentment. To remain ahead in the OODA loop, every social media platform needs to be leveraged to defeat the sinister designs of the adversary.

Counter Narratives

Digital media platforms have emerged as the new tools for alienation. The total absence of any Indian agency to either control its outreach or check the veracity of the information has only accelerated its spread and strengthened its influence. According to Parjanya Bhatt a compelling storyline is crucial to any communication strategy as it has the ability

to convincingly differentiate the truth from misconceived notions generated through false propaganda.[8] The Burhan Wani episode is a classic example of effective communication strategy by the terror outfits. Wani had become the poster boy of terrorism in Kashmir much before his encounter, primarily because he succeeded in narrating his side of the story through the social media.

Influenced by online propaganda, young boys were mobilised to pelt stones, set schools on fire and act as human shield for terrorists to escape. Since 2014, there has been a steady rise in local recruitment. Till 2013, the figures ranged from single digits to about 20 odd. In 2014, this figure jumped to 53 and to 66 in 2015. Immediately after Burhan Wani's encounter in 2016, this number climbed to 90 and in 2017 rose to 120. In an attempt to control the cycle of radicalisation and recruitment, nearly 10,000 boys involved in stone pelting incidents between 2008 and 2017 were given amnesty. However, this is no reprieve for the bruised Kashmiri mindset. India's success or failure will be decided on the basis of its ability to ideologically influence the Kashmiri society. Terrorism and violence has always been an effective way to communicate, which can be dealt with militarily, but shaping behaviours of friends, adversaries and the general population in between, is of utmost importance. Social Media allows the armed forces to manage the perceptions of the target audience thus allowing them to control the narrative. It allows dynamic modifications of the themes to shape the environment based on the feedback.[9] Information void following an incident gives rise to doubts that are at best avoided. Not involving the media at an early stage may lead to conjectures that will benefit the adversary. Our response should be truthful and with least amount of delay. Structures and policies must be created to ensure an immediate response mechanism. Lack of transparency invariably creates panic among all stakeholders leading to unwarranted speculation.

A good illustration of changing narratives can be gauged by the Home Minister's (HM) address during a debate in Parliament in July

2019. In reply to the Opposition's charge that the Government was unable to continue the erstwhile PM Vajpayee's policy on Kashmir, the Minister did some plain speaking. He said that during the UPA's rule for almost three decades in Kashmir, Kashmiriyat was ignored by permitting fundamentalism and Wahabism to flourish at the cost of the traditional Sufi culture and by overlooking an exodus of Kashmiri Pandits who are its integral part. As far as Jamhooriyat is concerned, why were Panchayat elections not conducted in the State during that period? He gave an assurance that process was already underway to alter dubious narratives and change perceptions. The HM's visit to Kashmir soon after his assumption of office has also been able to communicate the government's clear intent.

Two years ago the National Investigation Agency (NIA) was probably tasked to target the financial networks through which money flowed from abroad into separatist coffers even through legitimate channels but utilised for anti-national activities. A much more synchronized and focused effort to neutralise the financial networks was in the offing. A parallel effort is likely to be launched against OGW networks. The Jammu and Kashmir CID has enough information on these and needs only empowerment and backing to execute its campaign. Another visible change is the large Kashmir media's consternation at being deprived of government advertising whereas it has no qualms about constantly taking a stand against the nation.

Changing Mindsets

Social media's uniqueness in reaching targeted audiences is especially valid in case of adversaries in hybrid domains. Terrorists use social media primarily for spreading propaganda, in the form of multimedia communications providing ideological or practical instruction, explanations, justifications or promotion of terrorist activities. The terrorist organisations have been regularly using virtual messages, presentations, magazines, treatises, audio and video games

developed by their organizations or sympathizers. The Internet is used for promotion of violence by such entities encouraging the audiences to engage in role-play or act as a virtual terrorist. Thus, social media platforms being used especially for propaganda are very vital to control as it has major ramifications for the security forces.

Following a six-month probe into incidents of unrest in Kashmir in 2017, a team of National Investigation Agency (NIA) identified 79 WhatsApp groups, having 6,386 phone numbers, used to crowd source boys for stone pelting. Of them, around 1,000 numbers were found active in Pakistan and Gulf nations. The remaining 5,386 numbers were found active in various parts of the Valley and neighbouring States. Many of these groups had administrators based in Pakistan. According to a media report, more than 300 WhatsApp groups operated to crowd source mobs to disrupt anti-terror operations in 2017.[10]

While the terror organisations make optimum use of social media to successfully lure the youth towards terrorism, the government agencies unable to counter the surge of information and instant warfare, resort to E-curfews. There are suggestions that free publicity should be denied to the terrorists and hence partial censorship may be imposed to curb this. Censorship encourages rumour and apart from its repugnance to democratic traditions, should be enforced only if absolutely essential and that too for a limited period of time. The U.S. military appeared unsure whether to ban access to social media. Later it was reported that social media would not be banned. As with the Israeli military, the U.S. Army also provided a social media program where soldiers could post their experiences and allow direct interaction with the troops. The Russian Federal Security Service has banned its active members from certain social media websites over security concerns.[11]

It is a matter of satisfaction that the government has finally clamped down and restricted the activities of various separatist

organisations in Kashmir that were employing disinformation, fake news and social media to incite the youth. The State should not shy away from arresting individuals working against the interest of the nation and should release them on very stringent conditions, imposing strict conditions on their basic liberties. Well-coordinated information operations could potentially undermine India's ability to set the political and strategic agenda bilaterally with Pakistan, multilaterally with other powers, and even domestically, with its own public.[12]

Besides poor education and unemployment, the existing environment of stress and conflict has generated considerable tension in the youth of Kashmir. They fall easy prey to the designs of Pakistan and ISI sponsored network and internet platforms peddling drugs. Statistics reveal, that only five per cent of Kashmiri youth was hooked to drugs in the year 2008. The figure shot up to 40 per cent ten years later. This is an alarming situation exacerbated by easy availability of drugs making it difficult for law enforcement agencies to contain. The social media platforms are the favourite sales counters of drug peddlers. The police and NCB would do well to neutralise this by getting at them through cyber experts and decoy customers. Other proactive measures like organising awareness programmes and running de-addiction centres is the need of the hour.

De-alienation of the population requires a concerted effort by the Government with a political, social, economic and ideological content. The military civic action programme carried out by the Army over decades could serve as a foundation to build on with an enlarged scope and vision. The return of the Kashmiri Pandits to a situation in which they can sustain without threats and without existing in clusters is equally important. Their premature return to an insecure environment would only be counterproductive.

Conclusion

The Ministry of Home Affairs (MHA) reported in Parliament on 09 July 2019 that in the first six months of 2019 the situation in Jammu and Kashmir has witnessed improvement with terror-related incidents seeing a 28 percent decline; infiltration reduced by 43 percent, local recruitment declined by 40 percent and neutralisation of terrorists increased by 22 percent. It should be remembered that in a hybrid conflict scenario, neutralisation of terrorists addresses only the periphery of the problem. Once the security situation has been brought under control as has been done several times before, the political machinery has to step in with purpose and ensure consolidation. This has to be done with efficient governance and taking the people of the State into confidence. Just being able to conduct peaceful elections and electing a government is not even half the battle won, amelioration of the pent up discontent of the populace is still a far cry. The actual work of fulfilling promises and administrative implementation is the critical part. Conflict resolution shall need all elements of national power to be used in synergy in a well-crafted manner at the apex level.

To effectively leverage the social media space, a long-term strategy has to be worked out encompassing all facets of structures, policies, training and oversight mechanism. Social media management needs an integrated and holistic approach, incorporating the academia, industry, concerned ministries and relevant agencies of the Government. The aspects of public information, media management, information warfare and social media are closely inter-related and need close coordination and management. Ideally these should be clubbed under one umbrella organization. Comprehensive and judicious media guidelines covering print, electronic and social media are absolutely mandatory as part of an overarching Information Warfare policy. Its implicit implementation and enforcement is the greater need of the hour.

***Lt Gen Mukesh Sabharwal, PVSM, AVSM (Retd)** is former AG and GOC 15 Crops & a Distinguised Fellow of CENJOWS, New Delhi

1. Catherine A. Theohary, Information Warfare: The Role of Social Media in Conflict, CRS (ctheohary@crs.loc.gov, 7-0844) March 4, 2015 (IN10240)

2. Joint Publication 3-13, *Information Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, November 20, 2014.

3. Ibid CRS

4. Wigmore Ivy. ”Social Media”. http://whatis.techtarget.com/definition/social-media

5. Nations Daniel. “What Is Social Media? Explaining the Big Trend”. “Lifewire”. 30 May 2017 https://www.lifewire.com/what-is-social-media-explaining-the-big-trend-3486616

6. Brig Deepak Malhotra, Social Media and the Armed Forces, *Centre for Joint Warfare Studies (CENJOWS), New Delhi, 2016*

7. Vikram Singh, Information Warfare – The Winning Edge, TimesNowNews.com, 11 March 2019. https://www.timesnownews.com/india/article/information-warfare-the-winning-edge-india-social-media-sun-tzu-art-of-war-isis-jammu-and-kashmir-terrorism/380396

8. Parjanya Bhatt, Building effective counterterror narratives in Kashmir, ORF, 18 September 2018, https://www.orfonline.org/expert-speak/44307-building-effective-counterterror-narratives-in-kashmir/

9. Maj Gen Umong Sethi, “Social Media - A Tool for the Military”. ‘Scholar Warrior’, Spring 2013. Pages 125-129. www.claws.in.

10. Parjanya Bhatt, Cyber Jihad: The biggest challenge in Kashmir, PTI, 13 July 2018

11. Brett van Niekerk & Manoj Maharaj, Social Media and Information Conflict, International Journal of Communication 7 (2013) pp1167

12. Akhil Deo, Fog of War: A first time glimpse of wartime information operations, ORF, 01 March 2019. https://www.orfonline.org/expert-speak/fog-war-first-glimpse-wartime-information-operations-48662/

ORGANISATION AND STRUCTURES FOR INFORMATION WARFARE AND INFLUENCE OPERATIONS IN INDIAN CONTEXT

Lt Gen PR Kumar, PVSM, AVSM, VSM (Retd)*

Multi Polar World, International Security Environment leading to 24X7 Multi Domain Operations by All Nations

Post WW II, cut to the present, the World has witnessed the change from a bipolar (USA and USSR) to unipolar USA which is now transforming into a multi polar world. This has happened mainly due to gradual weakening of the comprehensive national power (CNP) and isolationist trend of USA, coupled with the rise and status of China, resurgence of Russia and emergence of regional powers like EU, Turkey, Iran, India and Nigeria. This dynamic world order automatically creates an unstable security environment, leading global and smaller powers alike to carry out strategic balancing (internally by growing stronger, externally by strategic alliances and using soft power) to maintain/ create strategic space to fulfil their National aspirations and vision. While USA was focused on its GWOT, many countries concentrated on finding ways and means to probe and find out the security and military vulnerabilities of USA and her allies. Concurrently, niche technological innovations which are available COTS (commercially off the shelf) like AI, EMS (electromagnetic spectrum), big data, hypervelocity systems, swarms, satellite and anti-satellite systems; and multiple non kinetic/ cognitive domains to include cyber network operations (CNO), network centric operations (NWO), information influence operations (IIO), space,

under sea have paved the way for smaller nations, NGOs and even individuals to compete in multiple domains with other nations. Nations which do not necessarily agree with the USA and its allies on their vision of liberal democratic world order like Russia, China, Iran, Iraq, Venezuela, North Korea have started asserting themselves regionally creating regional security zones further aggravating the tenuous security environment. The trigger can be attributed to the Chinese domination of its surrounding maritime waters [South and East China Seas and lately forays into Indian Ocean Region (IOR)] by creating artificial islands and military infrastructure and deploying armaments and surveillance systemsringing alarm bells in the USA, which has been the net security provider of the Asia Pacific region ever since WW II. The trigger for US alarm has been the rapid modernization and rising combat potential of China, establishment of A2AD (Anti Access Area Denial) systems and modernisation of PLA specially its rocket forces, PLA Navy, and development of new kinetic and non-kinetic systems with niche technologies.This focus on non kinetic domains can achieve strategic objectives with proactive actions but staying within the redlines/threshold of conflict of USA and other affected Nations. Russia, Iran, Turkey and other countries have also followed suit and this new multi domain approach to security and strategic space domination is being keenly watched and copied by many smaller nations and even MNCs, NGOs and individuals who have the capacity and capability. USA starting 2017, has reacted/responded by analysing and propogating the concept of 'Multi Domain Warfare (MDW)', and since it is timeless and operational 24X7, and operable during times of peace, confrontation and conflict has nowrenamed it Multi Domain Operations (MDO). The lines between peace, confrontation and conflict are blurring. Adversarial competition always leads to a cycle of action and reaction and naturally other nations led by China and Russia are embarking on countering US moves to prosecute MDO, thus creating capabilities to conduct their own MDO. A geo political and strategic reality for India, an aspiring regional power, is its acknowledged adversarial relationship with China in its immediate geographical area with a collusive

strategic partnership with Pakistan (both nuclear powers) and trying to dominate/influence India's immediate neighbourhood and IOR, and undoubtedly prosecuting MDO against India. In case of a confrontation escalating, our adversaries specially China will prosecute MDO as it maximises CNP and also allows for achieving strategic and military objectives without engaging in actual combat operations. In fact,even a stand-alone face off with Pakistan will now invoke MDO by China which will be almost as effective as combat operations preventing India from employing its full combat power (India will no longer be able to depend on its strategic reserves deployed/oriented towards its Northern Borders) and multi domain potential which will undoubtedly prove a serious challenge to us.By now it is apparent that the domain of Information Warfare could be considered the evolved form of warfare through attrition and manoeuvre phases with the primacy to any one (or combination) in gaining asymmetry over the adversary. It does not undermine the value of the other two phases, but enhances it. IIO of which electronic warfare is a critical component will play a decisive role during competition and conflict. India needs to prepare a road map, prepare, procure/create technology and equipment, train, form organisations and structures to achieve optimum synergy and operational effectiveness specially for the newer emerging domains like IW and IIO.

IW Vs IIO: Present Org and Structures of Own and Foreign Armed Forces and Envisaged Futuristic Force Structuring

Examining Structures Established by US and China

US. It needs no elucidation, that the US Armed Forcesdue to geo-strategic position and dominance as a superpower, has taken the lead in exploiting the domain of IW and IIO. With no intention of emulating the US Army (their strategic and operational thrust being deterrence, and deploying expeditionary forces globally),but learn how they synergise and operate, we need to study their organisational structures and how

they have evolved. Like most armies, the US Army has very similar functional branches[1], akin toour combat, combat support and Services; they have Manoeuvre, Fires, and Effects (MFE), Operations support (OS), and Force Sustainment (FS) Branches. Apart from the known basic branches (like armoured corps, infantry, artillery, air defence, engineers, army aviation ect), some specialised basic branches which the US Army based on their operational necessity for current and future wars specially for a multi domain competition/conflict have established needs highlighting.

Chemical Corps (part of MFE; Jun 1918). As on May 2018 193 Nations including USA have ratified the Chemical Weapons Convention (CWC) which is an arms control treaty that outlaws the production, stockpiling, and use of chemical weapons and their precursors. Their role would be more of global vigilance and investigation, I presume.

Psychological Operations (part of MFE; Oct 2006). The fact that it is a basic branch and forms part of the combat arm group clearly indicates the prominence attached to it for MDO, after all human minds (specially leaders and military commanders and local populace) are decisive cognitive elements of decision making.

Civil Affairs Corps (part of MFE; Oct 2006). Provide guidance to commanders in a broad spectrum of activities ranging from host–guest relationships to the assumption of executive, legislative, and judicial processes in occupied or liberated areas. In the Indian context, we are increasingly aware of the very important task of administrative control post operations of captured territory, but based on our national policy and strategy and having no hegemonic aspirations, this task can be managed by tasking Commanders and troops specially earmarked

1 'Wikipedia online'; How the US Army is Organised, https://www.army.mil/info/organization/ Chapter 3 Army Organisational Structure, GlobalSecurity.org; accessed on 27 Jun 19; and numerous other online articles field manuals of US Army

and trained (operational necessity). Our conduct before, during and after operations has a major bearing on IIO.

Signal Corps (part of OS; Jun 1860). I am highlighting this as Signals Branch is responsible for space operations apart from Information systems mgt and telecommunication systems engineering services. Surprisingly not part of MFE. The Corps will need to play a major role in IW and IIO as cyber, telecommunications and internet are the medium and grid on which maximum IW and IIO are conducted.

Military Intelligence Corps (part of OS; Jul 1962). The Corps also takes care of strategic plans, nuclear and counter proliferation, force mgt, ORSA and simulation operations. Naturally the Branch has a pivotal role in IW and IIO.

From FS Branch. Apart from the expected AGs,QMGs, Ordinance, Logistics, Transportation Branches, they have also established the Finance Corps (as early as Jun 1775!) and the Acquisition Corps.

As per open source inputs, the US Army is currently carrying out review and revamping of Organisation and Structures specially related to IW,IIO, and Cyber including functional and basic structure. Since these operations have a large canvas and scope and extends to multi domain and levels (strategic to tactical), a synergized structure for optimum operations (including multi services and agencies, training and cadre allocation) has to be well thought out, implemented in phases (to prevent career mgt and organizational upheavel) and top driven. The US Army is preparing to carry out major, organizational changes to its force structure within the next five years, according to the Futures and Concepts Center Director.“There is going to be a fundamental change in the organizational structure to conduct multi domain operations, the new concept of warfighting,” Lt. Gen. Eric Wesley told an audience at the Center for a New American Security in Washington on O4 March

19[2]. Open sources state that they are focusing on non-kinetic forces like cyber, information, computer, big data, PSYOPS, deception, operational security etc and examining how to create functional structures by clubbing and combining into basic Corps.

Organisation and Structures. In terms of organization and structures the US Army has both integral Information Ops staff above Division and also has the following: -

- **1st IO Ops Comd (Land).** Provides distinctly tailored IO and cyberspace operations planning, synchronization, assessment, and feedback support to the Army. Apart from HQ, Detachment and two battalions, it augments mil forces with tailored IO and cyberspace operations support provided through deployable teams. It can be termed as the Army HQ reserve which also conducts specific training and conduct of exercises.

- **56th, 71ST and 151st Theater Info Ops Gp (TIOG).** TIOGs maintains regional focus but can deploy elsewhere too. It has same composition as the 1stBn, and deploys purpose-built IO field support teams designed to provide the necessary IO support required by the requesting comd. You can call it a theatre resource.

China. The Chinese White paper of 2004 classifies operations as 'local war under informationalised conditions'' and states the main objective of PLA as[3]:

2 'The US Army is preparing for major changes to force structure' by Jen Judson on 06 Mar 19; https://www.defensenews.com/land/2019/03/06/major-army-force-structure-changes-afoot/

3 Chinese Concepts and Capabilities of Information Warfare, IDSA Strategic Analysis, October 2006, Volume: 30 Issue: 4 by Brig Arvind Anand (Retd) from "China's National Defense in 2004", White Paper, at http://english.people.com.cn/whitepaper/defense2004/defense2004.html. See Chapter III, Revolution in Military Affairs with Chinese Characteristics.

"The PLA, aiming at building an informationalised force and winning an information war, deepens its reforms, dedicates itself to innovation, improves its quality and actively pushes forward the RMA with Chinese characteristics with informationalisation at its core." They have in 2019 further consolidated to fight under hi-tech conditions[4].

Though the term 'informationalisation' has not been clearly defined, what can be inferred is that it covers a wide ambit and includes intelligence-based weaponry besides all elements of command, control, computer, communications, intelligence, surveillance and reconnaissance (C4ISR) and traditional components of information warfare. Information warfare is a sub-set of informationalisation and at the national and strategic levels it transcends the military aspects and becomes an important tool for shaping perceptions and belief systems of adversaries and competitors on a higher plane. Forms of IW accepted by the Chinese (i.e. operational security, military deception, psychological warfare, electronic warfare, computer network warfare and physical destruction). Chinese theorists have coined the term "Integrated Network Electronic Warfare" (INEW). President Xi made three bold changes to ensure PLA is ready for future wars; firstly, created five Theatre Commands similar to the US for better synergy and I3 (interoperability, integration and inter-dependence), secondly, right sizing of PLA Forces with maximum pruning of PLA Army and strategic growth of PLAN to start growth of a blue water navy [initially dominate the East and South China Seas and Indian Ocean Region (IOR)] and lastly creation of Strategic Support Force which directs space, cyber, EW, IW including psychological warfare (PSYOPS) and a strategic Rocket Force (upgrade of erstwhile Second Artillery) which combined establishes the A2AD (Anti Access, Area Denial) shield in the Asia Pacific region. Regular exercises under 'complex EW and

4 DoD, USA "Annual Report to Congress: Military and Security Development involving the People's Republic of China 2019", https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_China_ Military_Power_ Report.pdf accessed on 28 Jun 19.

IW environment' is being conducted very realistically where the 'Blue Team' now routinely wins against highly scripted affairs earlier. Joint operations encourage decentralized command and control for today's swift MDO.IIO, IW and PSYOPS against Chinais going to be a real challenge. They remain opaque, protected and have their own social media platforms like Beidou and We Chat equivalent to google and WhatsApp. Their country has the maximum surveillance systems over their own public and much more for outsiders and countryside. Facial recognition, satellites, CCTV coverage even in remote areas and real time data passage, intelligence, information and monitoring systems. However, this very closed information environment if penetrated can reap mega dividends. Our cyber warriors, hackers and cyber and IIO must carry out 24X7 operations, as also MDO.

Kinetic Change of Social Media. Social media has undoubtedly become a pivotal and often decisive game changer in MDO! Through the weaponization of social media, the internet is changing war and politics, just as war and politics are changing the internet[5]. Just one recent event which shook the world amply illustrates the point. The fall of Mosul to ISIS is a classic case of social media winning a war and actually enabling its fall. Sunni Youth copied the brutal acts of ISIS even before ISIS arrival, Turks, Sunni and Shia neighbours eyed each other with suspicion, and five battle hardened Iraqi Army Divisions stood defending Northern Iraq with fear, and even before ISIS arrival, wondered if they should fight or flee. Slowly the trickle became a flood as both the Iraqi Army and Police slipped away along with more than half a million civilians. The actual invading fighting force was about 1500 and they stormed the city and got their hands on enormous amount of war waging material (even Humvees, M1A1 tanks, black hawk helicopters and countless vehicles)[6]. Social media impact can

5 Like War: The weaponization of Social Media by PW Singer and Emerson T.Brooking, An Eamon Dolan Book, Houghton Mifflin Harcout, 2018

6 ibid

be gauged by the fact that four to five fully trained and armed Iraqi division by the US had just evaporated into thin air). It will gain even more potency, and influence as a game changer in MDO.

IW and IIO in Own Armed Forces

Globalization, hi-tech and disruptive technology, multi polar and 24X7 MDO has dynamically changed the global security environment, which should be factored in nationally, and seriously impacts our Armed Forces and its modus operandi, as we review our IW and IIO functional organisations and structures. These operations have always been conducted from time immemorial, but has basically devolved upon the Commander to evolve and execute with generally adhoc structures suitable to individual commanders by employing staff based on their aptitude and availability. For example, in active HQs Northern and Eastern Command and their affiliated Corps,adhoc cells are actively engaged in IIO operations with special focus on social media which is slowly emerging as the most potent, widespread and influential source for IIO and IW. The basic tenet of information organisation is to reach the right information to the right person in the right place at the right time in the right form (to aid comprehension and further exploitation) securely. It requires networks, data, applications and security. An essential and initial requirement is capability building for capture, storage, processing and presentation of information. It needs networks and applications along with databases. Databases comprise own and adversary information. Own data is organizational and, hence, structured. Adversary data is people or machine generated and unstructured. Own data can be captured in terms of personnel, equipment, stores, finance, terrain and infrastructure. They can be slotted as per units and formations they belong to. Adversary information cannot be so organized. It can broadly be classified as static or semi static data, dynamic data comprising daily or such periodic reports, streaming data from surveillance resources and assessments at each level. While

the SO-in-C (Corps of Signals) would be responsible to provide the network infrastructure for storage, communication and security of data, the architecture of data storage and algorithms to make sense out of them would currently vest as the responsibility of the DGIS. The DGIS needless to say has a long road ahead of him, and there should be no hesitation to turn to professional and even commercial assistance for optimization. I am saying this with experience, that the initial setting up is a gargantuan task of creating one data base for the Army, and later tri-services. This information will be used by the commander, operations, intelligence, logistics branches across the spectrum of the tri-services (at Army apex level DGMO, DGMI and DGOL equivalent)[7].

In the Indian scenario IW and IIO have a distinction in their operational context. In IIO, actions are taken to affect adversary information and information systems while defending one's own information and information systems. Information operations is 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, while in IW operations are conducted during time of crisis/confrontation or conflict to achieve or promote specific objectives over a specific adversary or adversaries. IIO/IW covers activities such as electronic warfare (EW), cyber warfare and perception management to include social media exploitation [public information (PI)] and PSYOPS.As would emerge later, cyber domain having become very large in scope has rightly been placed separately under Cyber Defence Agency, and exclusively even by individual Service HQs. IO may be understood as such operations involving exclusive use of information, through any chosen medium, to target adversary's information or cognitive dimensions. In my opinion, currently both terms (IO and IW) are being used for the same domain

7 In conversation with Maj Gen Ravi Choudhery, Sigs, on 21 Jun 19, currently deputed to NTRO while discussing Organisations and Structures

and tasks. There is also some diffusion and overlapping of information and intelligence by all agencies dealing with the subject (there always will be). It will be interesting to note that as per Lt Gen Michael Flynn (Head of US DIA), before the rise of social media 90 percent of useful intelligence came from secret sources but it was the exact opposite with the same percentage coming from open sources that anybody can access[8]. This significantly increases the importance of organisations tasked for intelligence and information.

At the national level, for EW, we have various types of SIGINT units (including for external and internal EW and SIGINT) which operate under the ADG SI (Signal Intelligence)/DG DIA who in turn reports to the NSA; for Perception mgt/PI we have the NIB (National Information Bureau) reporting to the NSA. This is supplemented by inputs from NTRO, R&AW, IB and NIA (National Intelligence Agency). For EW, the Army has EW Groups and Sub Groups under the Theatre Commander and one to two Sub Groups with active Corps (along LAC, LC and IB) which carry out EW tasks envisaged by the theatre and corps commanders. As stated earlier, strategic and tri-services tasks are planned and executed by ADG SI (along with services assets) with independent EW resources (under DG DIA/COSC/NSA). Keeping the EW groups modernized so they function and fulfil their mandated tasks is a challenge in this fast-paced technological field. A review of its affiliation (should it become a part of DGIW?), organization, number of units to meet strategic and operational tasks, modern technological equipment and manning/career growth needs to be carried out expeditiously.

Presently in the Army, we have the ADG PI operating under the DGMI and the ADG IW under the DGMO. IW branch has a section looking after communications including strategic and an IW section,

8 Social Media Is Revolutionizing Warfare, dated 08 Oct 18, theatlantic.com, accessed on 30 Jun 19, https://www.theatlantic.com/international/archive/2018/10/likewar-internet-new-intelligence-age-flynn/571903/

along with an autonomous unit operating under the DGMO looking after cyber defence and whenever mandated limited cyber offence. The DGMI too has cyber warfare capabilities. The IAF similarly has the ACS E&IW (Electronic and Information Warfare) at Air HQ and the IN has ACNS (Ops and IW) who apart from coordination operations operates an IW Cell comprising of a dozen officers and 20 odd seamen, and an independent SIGINT unit. At the theatre level we have a BGS (IW) looking after IIO. There are no formal or institutionalized units below that in all three Services. There is a certain amount of ambiguity existing in specific nuances in terminology and tasking, which naturally leads to some diffusion in operations. With the advent of MDO, we will need to bring more clarity in the organisation and structures as also operational employment.

Cyberspace is the technical foundation on which the world is increasingly relying to exchange information (and to facilitate social networking, extend influence from afar, and so on). As a collection of mediums, it is rapidly consuming the information environment's landscape[9]. Therefore,controlling cyberspace (and the intersecting electromagnetic spectrum) could eventually be tantamount to controlling the information environment. Our Armed Forces must prepare for that possibility. Obviously, it is intrinsically linked to IW and IIO. However, the growth in size and importance cyber network operations (CNO), computer network operations, and cyber operations as a whole render them too large and fast-moving, and prudence suggests that it be kept independent of the IW and IIO framework. Acknowledging this and the emergence of a transformation in security architecture globally where 24X7 MDO persists, with a focus on non kinetic, cognitive domains (cyber, EMS, information influence including social

9 Redefining Information Warfare Boundaries For An Army In A Wireless World by Isaac R Porch III, Christopher Paul, Michael York, Chad C Serena, Jerry M Sollinger, Elliot Axelband, Endy Y Min, Bruce J Held; Rand Arroyo Centre, 2013

media) the Govt has ordered setting up a Defence Cyber Agency,[10], Space Agency and Special Forces Division which will be tri-services organisations. Regarding cyber, it could operate under the DG DIAto be truly tri-services and incorporation of multi-agency assistance; or at the apex level it would operate under CISC (IDS) reporting to the COSC; there should be major components under each service HQ and elements at Command and initially even at active Corps level (Corps under Northern and Eastern Command). It will certainly have a defensive role against nations carrying out cyber-attacks and probes (specially China and Pakistan) and would in all probability be given a specific offensive and counter offensive mandate. I am sure inputs, components, resources, and technical equipment and advice of govt organisational capabilities and expertise like DRDO and NTRO will be available, and from our very vibrant IT industry, and youth with special aptitude for cyber operations will be inducted/co-opted. As per online inputs, currently IDS along with NTRO, R&AW, NTRO are carrying out series of exercises to test defence establishments (specially critical and sensitive installations like nuclear delivery assets, long range missile units, active field formations deployed in sensitive areas etc) to test their cyber protection systems. Rear Admiral Mohit Gupta who is heading the newly created Cyber Defence Agency will initially need to draw up a doctrine for cyberwarfare, and formulate/draw up framework for its organization and structures at apex and subordinates' level. There is an urgent inescapable requirement of looking at our major dependence on foreign software and hardware given the history of cyber spying using these very same technologies, which obviously would prove extremely disruptive in times of confrontation/conflict. Here, it bears mention that when it comes to cyber operations (accumulation of cyber information and intelligence), it is not restricted to adversaries but all nations, as in the world of realpolitik there are no permanent friends or foes, only permanent national interests.

10 India to have Defence Cyber Agency in May; Rear Admiral Mohit to be its first chief; Asian News International dated 30 Apr 19 and numerous national mainstream media

Media inputs have also reported that the Defence Ministry has approved a new Information Warfare branch in the army under a DGIW (with both PI and IW responsibilities)to combat misinformation and false propaganda being spread through social media for adverse psychological impact, and while not stated hopefully specific offensive IW/IIO also. This implies that ADG PI and ADG MO (IW) currently under DGMI and DGMO will move under DGIW. Their role would certainly be expanded to be a vital domain of MDO engaged in full spectrum operations 24X7[11]. The DGIW operates under a new DCOAS (Strategy) having DGMO, DGMI, DGIW and DGPP under him. There are pros and cons to this structural change (creation of DCOAS (Strat)) but theoretically synergy will be created between operations, intelligence, information and perspective planning provided the COAS will assure some degree of autonomy, freedom and flexibility to operate to the DCOAS (Strategy). Ironically, the very 'real time' nature of IIO (TV and social media) where inputs reach all affected actors starting from PMO, RM, NSA, Defence Secretary etc may put pressure on the hierarchal system, and I reckon with personal experience that the linkages will be a mix of direct communications and structured communication.

PI and IW operationsbeing the two main verticals of IIO, will be supported by sections looking after different aspects. In PI one can think of tv and print media, social media/online inputs with EW, PSYOPS, operational security, military deception under IW. A cogent strategic IW plan specifically against nations, groups or even individuals, during Competition phase and specific and more focused plan closer to confrontation and conflict stage of MDO would be an operational necessity. The plans would need to influence, disrupt, corrupt, or usurp the decision- making of adversaries and potential adversaries while protecting our own. While writing out the pioneering

11 Defence ministry approves information warfare branch for Indian army' by Shaurya Karanbir Gurung, The Economic Times, 09 Mar 19;army/articleshow/68329797.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

paper due thought must be given to ab initio structures upto corps level, for SF Div and units, long range missile/rocket formations with bricks for lower formations and contingencies. We need IW/IOs (Information Warfare/Operations Officers, JCOs and NCOS) deployed at all levels of seniority and formations upto brigade level in a phased manner.

Till such time the basic branch of Information Operations is established, officers and OR from all arms and services with adequate aptitude and training can man these appointments. Subsequently too, in addition to basic branch staff, others can man posts just like we do in operations, intelligence and logistics branches. Due thought on training, creation of tri-services and individual services training nodes for conduct of basic and advanced courses for Officers and all ranks be given and put down to make it a comprehensive time bound phased organization and structure for IIO and IW. Serious consideration needs to be given to creating basic corps for IO, IW (including EW), Cyber, PSYOPS, Space and Strategic Forces by grouping of similar fields (need not have basic corps individually but similar functional and interrelated fields can be grouped). This will ensure clear career growth prospects, meet HR aspirations and optimize officer and soldier HR mgt. Here, we have the option of creating a tri-services IO Corps abinitio which will be a very complex process given the lack of jointness as also diverse IO requirements. It has great advantages as intrinsically IO are essentially tri-services specially at the strategic and operational level, and in future,MDO and conflict will be joint operations. Second option which is more pragmatic and implementable is to create individual Service oriented IO Corps. Attri-services, operational and training structures like ANC, IDS, NDA, CDM, tri-services war centres and command posts (CPs), post staff on pro rata basis as hitherto fore. We need not carry this out in haste but carry out dynamic planning after observing how the systems and operational synergy can be optimized. More detailed inputs and recommendation on organistion and stuctures would prove

infructuous as IDS and Service HQs are already working on it and frankly not open to suggestions, or thrown it open to debate/discussion or sought inputs which one feels should be done before cementing the structures.

Training and Courses. They are based on operational necessity. As envisaged,like the basic functioning and manning, training and courses too can be tri-services oriented and individual Service specific. One tri-services training institution can be established which initially conducts orientation (one to two weeks), basic (two to three months) and advanced (nine to twelve months) courses. The course should involve practical on ground training and for advanced course attachment time with all three service formations. In case our Armed Forces goes onto tri-services IO Corps, the same Institution/Academy can graduate to a Training Centre like other Corps in the Army. Virtually the same structure is envisaged for each Service. We have quite recently started specialized collective training for specific future war scenarios like training to operate under a nuclear backdrop with a brigade plus force exercising per command with participation of specialized units and HQs like SF, NBC School, specialized engineer and medical support units intra Army and even some civil administrative organisations and staff participating, in selective phases. Since IIO is already an intrinsic part of MDO, all units and formations need to factor it in and conduct individual and collective training exercises accordingly. Creation of IO specialized formation and battalions at Army and Theatre level, if required, can form part Phase 3 of IO growth (I personally will not be surprised if we feel the operational necessity of these field units due to game changing and decisive role of IIO in future wars).

Conclusion

To conclude IIO/IW has both kinetic and non kinetic/cognitive impact, reinforces other domains including manoeuvre and attrition warfare,and will increasingly gain pre-eminence in national strategic actions to meet national objectives. In the security architecture and emerging 24X7 MDO, where peace and conflict has blurred, IIO would prove decisive to achieve objectives short of war, as also create asymmetry during conflict, and last but certainly not the least allow smaller and less powerful nations/groups to close the power asymmetry and compete for strategic space. For our Armed Forces and Army, establishment of basic branches, organization and structures for IIO/IW is an operational necessity and must be developed to provide maximum synergy and effectiveness to fight MDW.

***Lt Gen PR Kumar, PVSM, AVSM, VSM (Retd)** is a renowned Defence Analyst

INFORMATION AND INFLUENCE PARADIGM IN TODAY'S FLAT WORLD

Air Mshl PP Khandekar, AVSM (Retd)*

> "We are opposed around the world by a monolithic and ruthless conspiracy that relies primarily on covert means for expanding its sphere of influence- on infiltration instead of invasion, on subversion instead of election, on intimidation instead of free choice, on guerrillas by night, instead of armies by day."
>
> - JFK

If we look at the last US elections, we may have to re-word the statement by JFK in ways more than one. Information warfare (IW) and Influence Operations (IO) have always been the instruments of the warfare in the mind of the Commanders since Ramayana and Mahabharata days. In fact, deceit has been one of the fulcrums around which many mythological stories have been built around the world at different points in time. Sun Tsu way back had said, "If you are far from the enemy, make him believe you are near." With ICT and RMA not to speak of Disruptive technologies, the digital battlefield of today and tomorrow is faced with challenges of a different kind. The ideological fight between democracy and totalitarian/ authoritarian form of governance has intensified amongst major power competitors with rising scrutiny in digital domain. The successful deployment of the Stuxnet worm, a malicious software of unknown origin that was used to attack centrifuges in Iranian nuclear facilities, has raised questions on whether a terrorist group may be able to develop a similar cyber

weapon. Terrorists could employ the Internet and social media to study the Stuxnet code and tailor it to attack computers that control critical infrastructure and commerce.

Matt Bishop and Emily O. Goldman in "The Strategy and Tactics of Information Warfare" have comprehensively covered IW issues. Information as 'content', as distinct from information as 'conduit' has always been a critical dimension of strategy in combat and competition, whether due to its absence or presence. It was Carl von Clausewitz's scepticism about the reliability of information and intelligence at the tactical and operational levels that led him to emphasize, in On War, the need to maximize and concentrate one's troops, maintain reserves, and ensure that leaders possessed intuition and experience. For Sun Tzu, on the other hand in Art of War, deception, disinformation and knowledge of the enemy's innermost thoughts and plans are the keys to surprise and victory, perhaps even a bloodless victory.

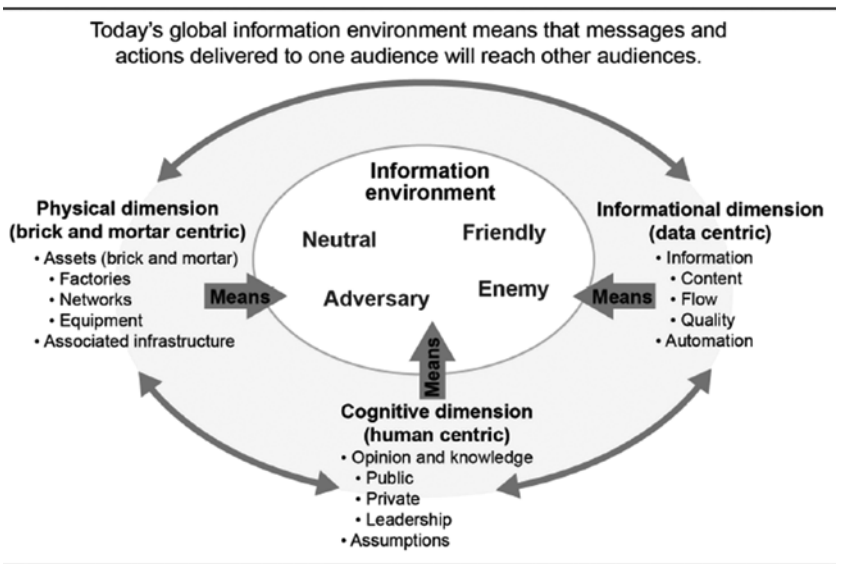
Techniques of information warfare simply provide attackers with a broader array of tools and ability to target more precisely and by non-lethal means the lifelines upon which advanced societies rely-power grids, phone systems, transportation networks, and aeroplane guidance systems. IT can also make conventional combat more accurate, thereby improving the efficiency of high explosive attacks. Here again, IT continues to contribute to trends in warfare that have improved the lethality of military force over time.

Information is power and as Joseph Wong said, "Influence is the compass and Persuasion the Map."One can say Information is subset of Influence in this context. The line between information warfare and influence operations is becoming blurred day by day. In this article therefore, no separate treatment is given to IW and IO. Margot Asquith has stated that it is easy to influence strong than weak character in life. It may look as a paradox but for an action, strong characters once convinced can achieve faster and more effectively. Dale Carnegie's

book on “How to win friends and influence people” is a ready reckoner for some, though written in a non-military context. Sun Tsu has said that the whole secret lies in confusing the enemy, so that he cannot fathom our real intent. Planting Information and influencing the populace can confuse the enemy following the dictum ‘if you cannot convince, confuse’. Russow (1986) attempts to explain the cognitive state of a deceiver by stating that An organism S can be said to deceive D if and only if S’s effect on D is a causal factor in D’s having a false belief that it is in situation A, where D’s acting on that belief is more advantageous to S than D’s acting on the belief that it is situation B (the actual situation).Also An agent’s behaviour is deceptive if and only if the agent intends that, because of its behaviour, another organism will come to (and perhaps act on) a false belief. These definitions are applicable to both the animal and human worlds.

The emergence of terrorists and extremist breed has to do something with the philosophy- “I know you are bad influence, but….. damn you are fun.” Simon Sinek has rightly put it that there are only two ways to influence human behaviour- you can manipulate it or you can inspire it. It is known that values are long lasting, attitude changes as per the environment and behaviour is the response to the stimuli. Influence can be enduring such as that of the parents or the teacher or it can be for a limited period. The influence of Mao and Lenin- Marx is

found even today in intelligentsia. In Indian context, Naxalite movement, Anna Hazare movement are a few examples while ISIS, Al Qaeda, JeM and others are the examples world wide. It must be understood that the core reason behind such outfits is a sense of injustice- right or wrong- that the leadership is able to convince, influence and motivate the cadre to follow to achieve the desired objective.

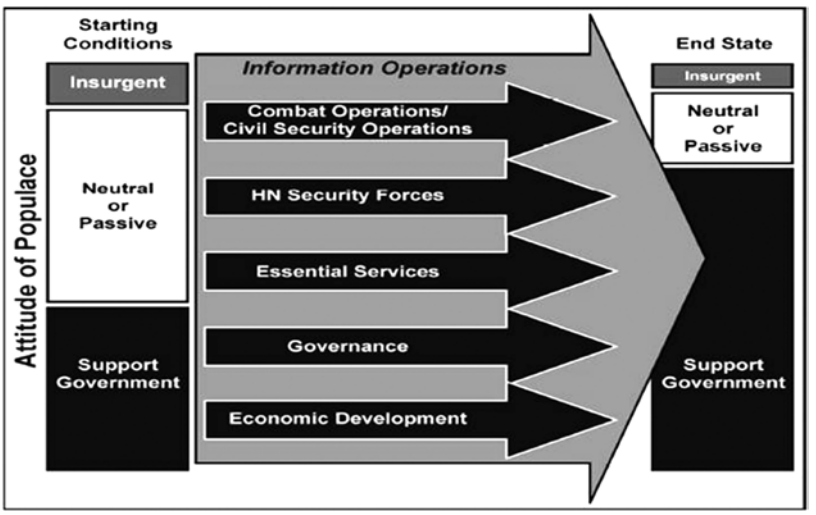


John C. Maxwell's quote "Leadership is influence" is well known in military circles and corporate world while Kenneth Blanchard said, "The key to successful leadership today is influence, not authority." In military leadership, due to the hierarchical structure, influence is attached to the authority or the appointment. Hence in the strictest sense of word, military leader rarely brings an influence. There are many cases of "undoing" by the successor on measures- small and big- introduced by the predecessor.

In the Battle of Thermopylae in 480 BC, Persian ruler Xerxes used intimidation tactics to break the will of Greek city-states. Alexander the Great used cultural assimilation to subdue dissent and maintain

conquered lands. Genghis Khan and his men planted rumours about their cruelty and the number of their horsemen to spread fear and to weaken the enemy's resilience, long before the printing press made it possible to mass-produce information. Information Warfare (IW) was defined by Dr Thomas Rona in 1976 while Libicki amplified the concept by defining Command and control; Intelligence based operations and Electronic Warfare as well as hackers and psywar. Winn Schwartan author of Info warfare with "computers everywhere" in Info Age in 1991 spoke about Electronic Pearl Harbour. Information warfare's origins are electronic warfare, military deception, psychological operations and information/operational security. IW and Information Operations (IO) with military and civil dimensions encompass - according to Kenneth J Knapp and William R Boulton- security demands for aspects such as personal, commercial, economic, political, criminal justice system and so on. The issues become complex due to the societal reliance more on Cyber technologies that pose dangerous sources of information extraction. These are low cost cyber weapons and since conventional military missions are not applicable to commercial and civil world, this type of warfare poses challenges due to hi tech espionage, perception battles being fought by ordinary hackers or sponsored groups of hackers to conduct organised crimes. In the hybrid environment of cyber/ info tactics and military strategies, Public Safety Organisation needs to be established for information flow. The debate on legislative responses reflects the ethical dilemma of protecting the information ecosystem without compromising fundamental rights. Due to lack of proper legislation Petro Romos in 2018 observed emergence of Transactional Criminal Organisation (TCO) for money laundering, gaming thus germinating illicit market. The Department of Defense introduced the concept of Information Operations in 1998 proposed to revolutionise the ways in which warfare, diplomacy, and business were conducted. Two identified gaps were between policy and theory, and between the funding needs of IO initiatives and the actual funds the federal bureaucracy was willing to provide to support these operations. These two discrepancies were central to the overall discussions of

"Information Operations Matters". Leigh Armistead explains why these gaps existed and suggested ways to close them. Also in discussing best practices in IO, he clarified how the key agencies of the U.S. government can use the inherent power of information to better conduct future strategic communication campaigns. His book presents a more pragmatic approach to IO, recommending that IO policy be made surrounding usable concepts, definitions, theories, and capabilities that are attainable with the resources available. To meet the threats of the future as well as those facing us today, Armistead argues, it is necessary to use this new area of operations to the greatest extent possible. Interested reader is advised to read this seminal work on IO. Catherine A. Theohary, Specialist in National Security Policy, Cyber and Information Operations in2018 submitted a report to Congress suggesting a conceptual framework for understanding IW as a strategy, discusses past and present IW-related organizations within the U.S. government, and uses several case studies as examples of IW strategy in practice. Countries discussed include Russia, China, North Korea, and Iran. The Islamic State is also discussed.



Randal Martin in 2014 coined the term Terroredia and studied how English and French Canadian newspapers pushed for war on

Iraq and so was Obama's response assuming the N weapon with Iran for Israel. In 2017, Chris Mensah- Ankrah in Eriksonian Analysis of Terrorism in West Asia- Path to Radicalisation brought the concept of the Melting Pot of integrated highly segregated extremist communities and the need to revaluate teaching and learning models of Islamic Institutions. This year A. Walter Dorn compared cyber security with peace keeping and suggested application of peace keeping principles to be suitably appropriated for cyber security. Jeffrey Kurekwa and Prosper Muchkabarwa carried out a study on the media images of Islamophobia by CNN. It was proved that the media has the power to influence human perceptions toward stereotyping Islam as Terrorist Organisation and conflating that religion and culture with terrorism. It suggested to eliminate offensive communication and religious intolerance as well as the immediate requirement for the media houses to establish policies and laws for the reporters on the aspects of religion, race and culture reporting. Ethics for the media houses are a must. Benjamin James Knox from Norwegian Defence Academy brought out the need to educate cyber engineers the responsibility of their job and the cyber power effects with adaptive higher thinking skills.

David Ormrodetal devised Military Cyber Security Model with Information Assurance approach that is complete and comprehensive. He assumes the adversary to be intelligent and technically capable to design each cyber attack for different requirement resulting in different outcome, affecting different assets and processes in varying degrees. Lanier Watkin devised Next Generation Scientific based Risk Metrics in 2016 that considered severity of individual vulnerabilities and overall vulnerability of the networks with probability assigned for compromise due to a given vulnerability and employee non-adherence to the company policies and other internal threats.

Influence Operations of Russia and China

A lot of literature is available on the subject in open source. Peter Mattis in 2018 has at length given details of the way both the countries operated in the Cold War style for influencing the governments and making the narratives. China's approach has been Human centric while that of Russia Op centric. The different approaches can be summarised as follows:-

S.N.	China	Focus	Russia	Focus
1.	Playing the Man	Individual and not effect	Set-piece Ops	Objective Specific
2.	Service-Facilitated Ops	Party's Elite	Service Lead Ops	Intelligence Agencies
3.	Influenced Agents	Gatekeepers	Agents of Influence	Intelligence Officers

The Xi'an incident of 1936 provides the lesson "By building relationships, unexpected opportunities arise." The history of Chinese Communist Party (CCP) is replete with such examples. Zhou's conversation with Henry Kissinger in 1971 is a good case of the officer playing to the ego, elicitation, switching between dominance and deference and controlling the tone and tempo of conversations. Russia operated on disinformation system of varying degrees of sophistication such as forged/ manipulated documents to discredit the target, planting rumours such as US unleashed AIDS virus as a biological programme. Kevin Mc Cauley noticed in the Russian Influence Campaigns against the West that Russians developed objective, scientific framework following Reflexive Control Theory with two broad classifications under Psychology and Cybernetics.

Both countries approach Influence ops and active measures as a normal way of doing business- a hallmark of totalitarian and Leninist pasts. US on the other hand, treats covert action as something distinct from routine business of foreign policy requiring special authorities and oversight or legal documents over whether Tile 10 or Tile 50 applies.

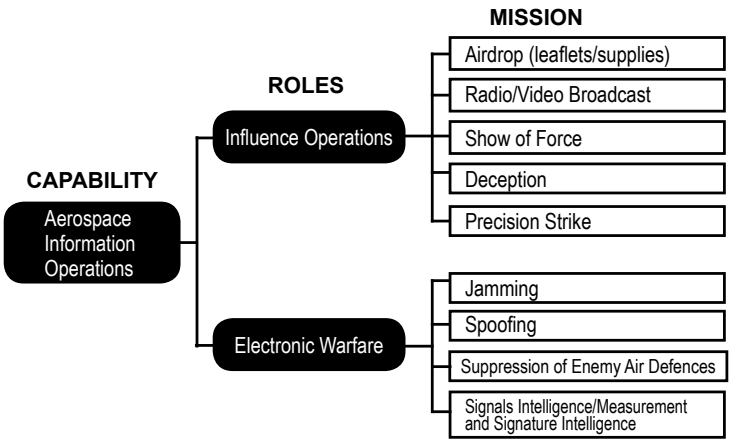
The role of Intelligence agencies is up front in Russian approach as they have the skills to operate clandestinely. Service A undertakes active measures for foreign intelligence operations using the governments, societies and events. Covert operations are assigned to KGB while overt operatives are within the party. Chinese approach is to assign the job to the party's diplomatic arm elite and not to intelligence officers. Xu Jialu was enmeshed in a web of ties to Liaison department and its Taiwan focussed operations. He established Confucious Institutes closely connected to China's influence apparatus.

Russia heavily depends upon the ability of the intelligence officers to pound the pavement, socialise, recruit/ hire agents, cultivate collaborators to produce manipulated cultured products to discredit the political figures and hostile institutions including doctored/ forged documents leaked to the media. The CCP approach is softer with formal intelligence organisation playing lesser role. Gatekeepers who open doors for the foreigners, facilitate inroads are more common than the intelligence officers thus creating confusion about innocent, dubious or routine gatekeepers. Mao Zedong story of how he shaped Chinese revolution is a good example.

Prashanth Parameswaran in his 14 May 2019 article on China's Influence Operations in Asia has observed that first time Pentagon document has a separate section on China's Influence or Interference Operations. PLA has three warfare strategy in op planning viz. Psy warfare, Public Opinion warfare and Legal Warfare. It has the concept of INEW- Integrated Network and Electronic Warfare. Asia has open door advantage with elite, broader society and governments malleable. In Pacific, Australia and New Zealand have been found vulnerable due to lack of rules and laws governing financing with transparency in politics and media. In South Asia Cambodia and Phillipines seem to be leaning towards China with offer of technologies, information and networks including 5G. Cultivation of Belt & Road Initiative by media is another example of increasing influence. China used IW effectively for

Taiwan to come under its influence without kinetic war and IO ensured delay in US response to interfere which was so late that it had no effect.

Naja Bentzen has authored a treatise on Foreign influence operations in the EU for the European Parliament. Having had limited success with their soft power efforts, both Russia and China – according to a 2017 study by the National Endowment for Democracy – recognise the potential for reaching their goals by making democracy, human rights and fundamental freedoms appear less attractive through 'sharp power' (which some researchers see as 'forced attraction' based on coercion, as opposed to soft power, which is based on attraction and persuasion). At the same time, the focus of leading democratic public diplomacy state actors, such as the US, on countering third-country propaganda, has declined since the Cold War ended (whilst the 9/11 attacks sparked new measures to counter propaganda from non-state actors such as Al-Qaida and, more recently, ISIL/Da'esh).'Sharp' influence efforts aiming to undermine the adversary are not new; but the information disruption 'toolbox', which includes a number of often overlapping covert and some overt instruments, keeps growing. New technologies have increased the speed at which disinformation can be spread, for example, often in combination with cyber-attacks (including hacks and selective leaks). The expanding hybrid toolbox also includes



assaults, corruption, energy coercion, and ideological and religious influence. While the Global Engagement Center (GEC) has begun outreach to allies in Europe, the U.S. government appears not to have a strategic plan to comprehensively counter Russian government influence and interference, including but not limited to disinformation. There are several institutions in Europe working on countering disinformation that could benefit from additional U.S. engagement, and U.S. leadership and coordination among donors could also help maximize the effectiveness of existing assistance.

Joe Hodnick has highlighted the Russian influence in elections in US, France and Germany with contemporary info war embracing increasingly in the digital world. Conclusion of Volodymyr Lysenks and Catherine Brooks on Russian Info troops, disinformation and democracy is telling. Digital hacking has been found to be the cheap and easy road to disrupt and interrupt the democratic process. The line has blurred between government sponsored hackers and individual ready for the money. Putin has a Geopolitical advisor deciding the areas of concern. His acceptance of “Patriotic hackers” in 2017 is an index of they getting hacking assignments in three ways- FSB, GRU and SVR, or by paid “civil trolls” or by unpaid “cyber-petrol volunteers”. There are curators who have distributors with a chain of command to achieve well defined aims and objectives.

William R. Gery, Se Young Lee and Jacob Nina in 2017 have discussed various aspects of IW in Info Age. The organisation needs a change to be as flexible and agile as say Google, Apple and Facebook. US has come out with DIME- Diplomatic, Info, Military and Economic Model. IOT and Moore’s Law have questioned the validity of Westphalian design of society and order based on logical modelling with principle of international law and orderly division of nations enabling sovereignty over territory and domestic affairs. There have been 10 Million hacks/ attacks per day on Pentagon. IT ensures sharing of info in near real time at exponential rate anonymously and perhaps with adequate security.

Russian Ops in Cremea could be directly contributed to principles and capability of IW following reflexive control philosophy. Russia has the ability to take advantage of pre-existing dispositions among its enemies to choose its preferred course of action. However in Estonia 2007 and Georgia-2008, Russia went into denial mode though the troops were caught. Terms such as "maskirovka", denial and deception, "little green mess" convey the

Russia's Social Media Influence Operations – Multi-Platform Full Spectrum		
Objective	**Platforms**	**Purpose & Advantage**
Placement	Primary: 4Chan, Reddit Secondary: 8Chan, You Tube, Facebook	• Insert forgeries into social media discussions • Seed conspiracies into target audiences • Spread kompromat on targeted adversaries, both true & false information • Hides Kremlin attribution, provides plausible deniability
Propagation	Twitter	• Spread narratives through overt Kremlin accounts & covert troll farm personas • Amplify select target audience stories & preferable narratives supporting Kremlin goals (computational propaganda make falsehoods appear more believable through repetition & volume) • Inject stories into mainstream media worldwide • Attack political opponents, foreign policy experts & adversarial media personalities
Saturation	Primary: Facebook Secondary: Google, Linkedin, Instagram, Pinterest	• Amplify political & social divisions, erode faith in democracy through discussions & ads • Pull content from other platforms into trusted friends & family discussions • Recruit target audience for organic propaganda creation/ distribution or physical provocations (protests, rallies or even violence)
Hosting	You Tube	• Overt propaganda post obscuring Kremlin hand (RT) • Sharing of video content to target audience via producers & reporters rather than standard television channels
Source: C.Watts (Foreign Policy Research Institute, Alliance for Securing Democracy, Centre For Cyber & Homeland Security)		

underlying principles. Russians followed the Sun Tsu dictum "To subdue the enemy without warfighting is the acme of skill."

A minority staff report prepared for the use of the committee on foreign relations United States senate on Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S. national security in 2018 has brought out issues concerning U.S. due to fake news and

information and influence operations conducted by Russia.

The global trends suggest that the world is grappling with the dangers of asymmetric fight in peace and no peace situations due to extensive use of IW and IO especially by Russia and China. The ideological fight between democracy and authoritative regime has taken different dimension after the end of Cold War. Due to transcending of borders, the ICT has found extensive utility for this unique warfare that can severely affect all spheres of individual and nation alike. Organisational structures, character building, technologies to ensure adequate checks and balances and safety are being contemplated.

Zag Rogers, Emily Bienvenue and Maryanne in their commentary on Influence Operations in Digital Age have said, “The central myth of Silicon Valley ideology was captured in Stuart Brand’s maxim that “information wants to be free.”This must by now be understood for the “falsehood“ that it is. If information “wants” anything, it is to be controlled. As Scott Malcomson has shown, states are now competing for the political geography of cyberspace in a way that has fragmented a short-lived global Internet. Influence in these networks is spread across the ‘digital stack’, from the submarine cable to the human-computer interface, but the primary hub of power is at the level of network ‘routing’. Controlling the flow of information at this level is the state’s business again, and it will likely “kill off” all remaining hubris about a global online community, not to mention the absurd notion that greater connectivity is an unalloyed good.

> “Be selective about your external influences. Your multidimensional brain is influenced by everything you see, hear, read, smell, touch, feel or say.”
>
> Brian Tracy

***Air Mshl PP Khandekar, AVSM (Retd)** is a former AOM (Air Officer Maintenance) of the IAF

INDIA'S INFORMATION WARFARE CHALLENGES AND THREAT PERCEPTION

Vice Adm HCS Bisht, PVSM, AVSM (Retd)*

Introduction

Information warfare (IW) is a concept involving the battlespace use and management of Information and Communication Technology in pursuit of a competitive advantage over an opponent. IW is the manipulation of information trusted by a target without the target's awareness so that the target will make decisions against their interest but in the interest of the one conducting IW. It may involve the collection of tactical information, assurances that one's own information is valid, spreading of propaganda or disinformation to demoralize or manipulate the enemy and the public, undermining the quality of the opposing force's information and denial of information-collection opportunities to opposing forces. Information warfare is closely linked to Psychological warfare.[1]

Whilst IW has been used in battles since times immemorial under various pseudo names, the concept of IW was officially introduced in the US Deptt of Defense in 1992. According to the US Joint Chiefs of Staff Instructions, IW is defined as "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks

1 https://en.wikipedia.org/wiki/Information_warfare

while defending one's own information, information-based processes, information systems and computer-based networks. Techniques of IW simply provide attackers with a broad array of tools and ability to target more precisely and by non-lethal means, the lifelines upon which societies rely, e.g. power grids, phone systems, transportation networks and aircraft guidance systems etc.

IW involves both offensive as well as defensive measures. Offensive measures are those taken to affect adversary's information and information systems, whilst defensive measures are those that protect our own informational assets. Martin Libicki of the National Defense University, Institute for National Strategic Studies proposes in his book, that IW is not the technique in itself but rather there are seven forms of IW. They are: Command and Control Warfare, Intelligence-Based Warfare, Electronic Warfare, Psychological Warfare, Hacker Warfare, Economic Information Warfare, and Cyber Warfare. Each form requires its own rules of engagement, own methods, objectives, and technologies. [2] Modern IW seeks to plant seeds of doubt and distrust to confuse, distract, polarize and demoralize the enemy. Accordingly, the creation and dissemination of misinformation, disinformation; commonly known as 'fake news,' is a vital component of IW offensive strategy and is being followed by certain nations.

Examples of IW in earlier Battles/Wars

During the Normandy Landings or 'D'-Day Landings, extensive Deception and Information Warfare Operations were undertaken by the allied powers. They used combinations of physical deception, fake wireless activity, leaks through diplomatic channels, dropping of leaflets and double agents. Though the name of the overall operation involving the biggest amphibious operation in history was 'Operation Overlord', the reliance on IW was such that the Deception and IW Operation was

2 http://www.iwar.org.uk/iwar/resources/belvoir-iw-course/infointro.htm

given a separate codename called 'Operation Fortitude'. This operation relied heavily on wireless transmission and utilization of network of double agents etc. Some examples of effective IW undertaken during Normandy Landings are as follows:-

- Physical deception: to mislead the enemy with nonexistent units through fake infrastructure and equipment, such as dummy landing craft, dummy airfields, and decoy lighting.

- Controlled leaks of information through diplomatic channels, which might be passed on via neutral countries to the Germans.

- Wireless traffic: To mislead the enemy, wireless traffic was created to simulate actual units.

- Use of German agents controlled by the Allies to send false information to the German intelligence services.[3]

IW was also used by the US Navy during the ' Battle of Midway' in 1942. The US Navy under Admiral Nimitz was able to crack the crypto code used by the Japanese Navy by which the US Navy exactly knew the position and movement details of the Japanese carriers and battleships. Based on information about the Japanese forces, the US Navy were also sending deception messages about their own movements. Thus IW was used very effectively to win the 'Battle of Midway' by the US Navy. Closer home, during the Kargil Conflict as well, an example of IW being used by the Indian Navy also came to the fore. During the initial stages of the conflict, the Indian Navy was also deployed in the North Arabian Sea. To augment the resources on the western seaboard, the Navy's Eastern Fleet was sailed from Visakhapatnam and they were supposed to rendezvous the Western

3 https://en.wikipedia.org/wiki/Operation_Fortitude

Fleet in Kochi. From there both Fleets were to sail to the operational area. It is learnt that this story appeared in some major Indian newspapers and apparently created a commotion in Pakistan Navy and their Naval ships didn't venture out to sea. A very recent case of cyber warfare, which is also a form of IW, has been reported from Iran. Consequent to the Iranians shooting down a US Navy drone in the Straits of Hormuz, the Pentagon had reportedly undertaken cyber warfare against Iranian Missile and Command and Control systems. The cyber strike against the Iran Revolutionary Guards was apparently coordinated with the US Central Command. Although it disabled Iran's military command and control systems, the operation did not involve casualties nor were any missiles fired.[4]

Perception Management

Perception Management is an important component of IW. Information Warfare, psychological warfare and perception management are factors which complement each other. In the Second Iraq War of 2003, journalists were 'embedded' in the American Forces as combat cameramen. The purpose was not to give the world a ringside view of the war but to give it the 'American' view. As the Washington Post of 24 March, 2003 put it, "Almost by definition…a war waged on live television is a war in which political and public relations considerations become inextricably bound up with military tactics and strategy…How victory is won is almost as important as victory itself." Another significant event, the toppling of Saddam's Statue in Baghdad, made great news with extensive TV coverage. The reporters, Sheldon Rampton and John Stauber wrote in ' In These Times on 8 April 2003' that "As US tanks stormed into Baghdad on April 9, television viewers in the United States got their first feel-good moment of the war – a chance to witness the toppling of a giant statue of Iraqi dictator Saddam Hussein. The

4 The Middle East Monitor, Trump approves cyberattacks on Iranian Missile Systems, June 23, 2019

problem is that the images of toppling statues and exulting Iraqis, to which American audiences were repeatedly exposed, obscured a larger reality. A Reuters long-shot photo of 'Firdous Square' showed that it was nearly empty, ringed in by US tanks and marines who had moved in to seal off the square before admitting the Iraqis." These instances were a very powerful demonstration of the use of Perception Management in international affairs. Simply defined : Perception Management is 'Information' operations that aim to affect perception of others to influence their emotions, reasoning, decisions or actions.[5]

Another example of perception management is that on 3 Oct 1993, an American Special Operations team was sent into Mogadishu to arrest two Lieutenants of Mohammed Aididi, a warlord who controlled the city. The raid, estimated to last about 30 minutes, continued for 15 hours. Thousands of Somalis were killed while the U.S. lost only 18 soldiers. The casualties on the US side were not heavy but as TV footage of slain US Army Rangers being dragged through the streets of Mogadishu was aired, it created uproar in the American public and the American public at large was horrified. Public pressure so weakened the US political resolve that they pulled out of Somalia in six months.

Operations 'Desert Shield' and 'Desert Storm' were two operations where all elements of contemporary warfare were present, which also included cyber war as part of IW as a major element. A team of U.S. intelligence operatives slipped several virus-laden computer chips into a French-made computer that was smuggled into Baghdad. The viruses injected helped degrade command and control functionality of the whole system. The 4th Psychological Operations Group (Airborne) handled propaganda broadcasts and leaflet campaigns for U.S. Central Command. Information warfare is therefore real and it is much more potent than cyber attacks. Data is not only the new oil,

5 The Art of Perception Management in Information Warfare Today, - by Brigadier B M Kapoor, USI

but also a potential weapon. As the cost of saving data plummets, more and more information is being stored about individuals. These huge databases, when combined with the growing power of Artificial Intelligence, wield enormous power.[6]

Perception Management through Media Reporting

The Gulf war of 1991 brought war to the bedrooms of common citizens for the first time in history. The concept of embedded TV reporters started since then. The same concept was adopted during the Kargil conflict of 1999 and this methodology apart from telecasting war live, also helped shape public perception about 'Right' and 'Wrong'. The impact of strong TV visuals helps shape opinions across the board. This was seen during the Kargil Conflict, during Operation 'Parakram' and also recently during the IAF strikes. Whilst telecasting TV footage helps shape opinions, media reporting from the frontline also has its own challenges of inadvertent information dissemination, at times to the detriment of its own side. During 'Operation Desert Storm' both civilian and military leaders were particularly displeased with the CNN reporter 'Peter Arnett's' broadcasts from Iraq, wherein he gave more information than what was required. Coalition planners went so far as to indict him as a conduit for Iraqi disinformation. Images of the "Highway of Death" in newspapers and on television screens played a key role in President George H.W. Bush's decision to end combat after only 100 hours.[7]

6 Swift wars are a myth, India needs to prepare for other modern forms of Warfare as well, The Print, Lt Gen DS Hooda (Retd) Updated: 25 October, 2017

7 https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/ The United States Needs an Information Warfare Command : A Historical Examination- by Conrad Crane, June 14, 2019

India's IW Threat Perception

Whilst in the short term we have an IW threat from Pakistan, India's primary threat perception relating to IW and cyber warfare is from China. In 2003, China's Central Military Commission approved the concept of 'Three warfares' namely, (a) Coordinated use of strategic psychological operations (b) Overt and covert media manipulation and (c) Legal warfare designed to manipulate perceptions of target audiences abroad. [8] China has been using the philosophy of IW with great dexterity and even the Pentagon is worried about its intent and capability. Indian Armed Forces are particularly vulnerable primarily because of Chinese historical inimicality with us and also since Chinese electronics and communication equipment have flooded the Indian market.

China is on the verge of becoming the biggest manufacturer of chip technology in the world, which serves as the brain of any computer and smartphone. Beijing is also scrambling to buy the world's biggest chip-making companies by hook or by crook. Out of the fifty largest chip-making companies, China owns ten. They also export 48% of the world's mobile phones and nearly 41 % of world's computer devices. They are trying to outdo every competition in cellphone tower business and now one can see same desperation in cellphone 5G dominance. Chinese company 'Huawei' have taken the lead in 5G technology, even ahead of the US and though US wants to blacklist the company, the same may not be very easy.

As per a 'University of Toronto' report, the Chinese government is not only monitoring their own people but a great deal more beyond their borders. Any browser/application used on a smartphone, laptop or

8 Preparing for China's Information Warfare,
by Claude Arpi, 24 May 2018
http://www.indiandefencereview.com/preparing-for-chinas-information-warfare/

a tablet made in China transmits back to host server, details like hard drive serial number, GPS coordinates of the user, user search terms, websites visited and details of the wireless network being used. While downloading free applications, we never realize that they come with 'Software Development Kits' (SDKs). These SDKs have just about entered every household and office environment keeping a close tab on our every activity. All the above activities have one aim, collect data. How the Chinese intend using it, is not clear, but surely if they want to keep track on a specific person or organization, it becomes very easy.

The Chinese work on many fronts simultaneously and on a long-term basis, to tighten their grip on Chinese citizens and to spread disinformation internationally, where it helps them. They have conceived some very powerful and effective tools for that purpose. In India, the Chinese app 'Helo' was found displaying false quotes or graphic images designed to provoke outrage along religious lines, manipulating the longstanding tensions between Hindus and Muslims in the country. China is deeply involved in the fourth state businesses around the globe following top-down imprimatur from president Xi Jinping to "tell China's story" to the world. China has recently leaped into the front ranks of global media by launching its 'Voice of China' *s*uper-network. With over 14,000 journalists and staff employees, this Asian blitzkrieg in the information war is deployed to neutralize American influence and spread disinformation on every continent.[9] China perceives India to be a close Defence Partner of the US and with their technology and proficiency in hacking IT systems, our networks both civil and military are definitely vulnerable.

9 https://insightful.co.in/2019/01/24/chinese-information-warfare-a-threat-to-free-world/, Chinese Information Warfare – A Threat to Free Worldby Sandomina, 24 Jan 2019

India's IW Challenges and Measures to Address them

Whilst the age old techniques of IW like use of undercover agents, decoy activities/messages etc are still relevant; it has been more or less taken over by the domain of cyber warfare and social media. India is getting rapidly wired to the information superhighway. As India gets connected to the global village, asymmetric IW threat posed by our adversaries as well as non-state actors would be on the rise. With broadband connections always 'on' and proliferation of networks, widely spread across homes and offices, the cyber threat potential, has become much more pronounced than before. India's Computer Emergency Response Team (Cert-In) is the most important constituent of India's cyber community. Cert-In is a functional organization of Dept of Information Technology, Ministry of Communications and Information Technology, Govt of India, operational since 2004, with the objective of securing Indian Cyber space. It serves as a national agency for computer incident response.

India also needs to have a Cyber Command to holistically look at all IW and cyber functionalities of the Armed Forces. An example from the US is very relevant to mention here. Considering the importance of Cyber warfare, the US had set up a Cyber command in June 2009, within the Strategic Forces Command and accordingly revised its military doctrine. In the latest official military doctrine, the US has declared cyberspace to be the fifth dimension of warfare after land, air, oceans and space, and reserved the right to take all actions in response, including military strikes, to respond to cyber attacks against it. The US Cyber Command (USYBERCOM) plans, coordinates, integrates, synchronizes and conducts activities to "direct operations and defense of specified Department of Defense information and prepare to and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to their adversaries." The Command is charged with pulling together existing cyberspace

resources, creating synergy and synchronizing war-fighting effects to defend the information security environment. It comes under the Strategic Command, which also has the Space Command as a constituent.

In case of India, whilst IW has been used in combat, it has not been institutionalized as an important element of warfare and not given the due that it deserves. There is an agency called the Defence Information Warfare Agency (DIWA), which functions under the Defence Intelligence Agency (DIA), one of the wings of the HQIDS. The Defence Information Warfare Agency (DIWA) handles all elements of the information warfare repertoire, including psychological operations, cyber-war, electronic intercepts and the monitoring of sound waves. Considering the importance of cyber and information warfare, it is only necessary that a Cyber Command should be created in the Armed Forces, initially under the aegis of HQIDS and later tweaked suitably when the institution of the Chief of Defence Staff (CDS) and Theatre Commands are created. The proposed Cyber Command, which probably will also cover aspects of IW in all its forms, should be part of the CDS organization but under the larger ambit of the National Security Council Secretariat (NSCS) so as to cover a larger canvas of Information Security/Information agencies in the country. The good news is that a beginning has been made with a Defence Cyber Agency (DCA) having been created in Delhi recently, with a two star officer heading it. The DCA will include a lot of existing capability with the Armed Forces for tackling threats in the cyber domain and will also have the elements of DRDO working in it[10].

The issue at hand is the lack of an integrated approach to this important aspect of national security. The problem is exacerbated due to lack of awareness and the culture of cyber security as also lack of trained manpower at various levels. We also have too many cyber

10 Asian News International New Delhi, April 30, 2019

security and information security organizations, which have become weak due to 'turf wars' and financial compulsions. IW and Cyber warfare must be dealt with at the national level rather than at individual services level. The individual services have their respective Information Warfare Directorates operating. As far as the Services are concerned, training the IW and Cyber Warfare operatives and ensuring their continuity on job is a very important requirement for ensuring effective IW. This also needs to be integrated with other forms of intelligence gathering and collection like Human Intelligence (HUMINT) and Technical Intelligence (TECHINT).

While cyber warfare is an ongoing activity during peacetime, there is a dire need to develop this capacity for a warlike situation. Cyber warfare in a manner is part of our Net Centric Warfare (NCW) and will form an essential part of preparation of the battlefield in any future conflict. Building this capability will take time and must remain covert and ambiguous. It could also form part of the strategic deception process. This should be the responsibility of the Armed Forces (HQ IDS) along with DRDO and other experts. The proposed cyber Command, mentioned above, should comprise of not only the three services but personnel from the DRDO and scientific and technological community. It should work in close concert with the NTRO as also with the Space command, when formed, to obviate aspects of overlap and also to obviate duplication of resources.

To determine the structure, it would be prudent to study the mission and objectives of USCYBERCOM as a guide. A similar structure for India could be considered, especially as the US have evolved their structure, based on many years of practical experience. The structure should be need-based and flexible and cater to the requirements of all three services. It should also, in a manner, be charged with protection of critical IT and Communication infrastructure of each service, i.e. communication backbone, power systems, high-priority networks etc. The structure thus envisages a Defence CERT which works in concert

with each service CERT. Intelligence gathering is another very important component of IW and an accepted reality and cyberspace possibly provides the best scope for this as also information operations. Whilst each service has its own Defence Communication networks and own Communication Directorates, Joint operations, strategic communications as also high-security networks need to be coordinated under HQ IDS and the proposed Cyber Command. Cyber operations which are required for preparation of the battlefield should be a tri-service organization, with additional experts from the DRDO and also legal fraternity, since the issue of whether cyber attacks can be termed as acts of warfare and whether international law on warfare applies to cyber warfare also. The issue becomes extremely complicated because attacks in cyberspace cannot be attributed to an identifiable person and the attacks traverse several computer systems located in multiple countries. The concept of cyber deterrence is also being debated but it is not clear whether cyber deterrence can hold in cyberspace, given the easy involvement of non-state actors and lack of attribution.

In keeping with current needs, the Defence services, DRDO, NTRO, CERT-In, RAW, IB, C-DAC, Ministries, NIC, NASSCOM, private industry etc. have to work in concert. The impact of this on every aspect of electronic media requires a coordinated and integrated approach. Given its all encompassing nature and secrecy involved, it also follows that control of all cyber and IW activities at the national level must fall under the purview of the National Security Council and controlled by its Secretariat i.e. the NSCS, as also mentioned above. Within these lead agencies for executing offensive cyber operations inter alia could be the NTRO and the services.

Conclusion

Information Warfare coupled with cyber warfare is a tool which can win wars with least effort and resources. However, it has not received the due focus that it deserves in India. Whilst there is a need to sensitize

the common man about the pros and cons of IW as also information security, the same needs to be covered under a law or an act and the Govt should have the will to implement it stringently. There is also a need to educate the common man about the dangers of cyber terrorism. Cyber security should not be given mere lip service and the organizations dealing with the same should be given all support, without any bureaucratic interference being permitted. Agreements relating to cyber security should be given the same importance as other conventional agreements. During allocation of budget it is usually seen that whilst IT sector gets suitable budget disbursement, there is a lack of budget allocation for aspects related to IW. As a matter of fact there needs to be greater investment in IW, being a specialized job. This is also required so that Indian agencies working after cyber security should also keep a close vigil on the developments in the IT sector of our potential adversaries.

***Vice Adm HCS Bisht, PVSM, AVSM (Retd)** is Leading Defence Analyst and Author

RADICALIZATION AND DERADICALIZATION STRATEGIES IN THE SOCIAL MEDIA AGE

Lt Gen Syed Ata Hasnain, PVSM, UYSM, AVSM, SM, VSM (Retd)*

'The advance of an army used to be marked by war drums. Now it's marked by volleys of tweets'

As part of warfare physical aspects such as subjugation and destruction of war machinery are considered essential for victory. That is what war is normally related to in common perception. However, the securing of the undying commitment of soldiers to the cause, the synergization of the commitment of the society from which the soldiers are drawn and the cultivation of both the society and soldiers of the adversary towards own belief, are also important facets employed to contribute to eventual victory. There also exists the entire domain of winning wars without firing a bullet; this is the domain enabled by information and conditioning of the minds of the adversaries. All kinds of ways were sought in yester years to influence the target minds through information; radio broadcasts, dropping of leaflets, the print media and later visual electronic media were a few of them. With the current information revolution underway networks and the coming of social media has enable direct outreach to the individual, the organization he belongs to and its hierarchy, all at once and with mass communication. If any media of communication is vibrant, 24x7, popular for entertainment, carries sufficient information and knowledge and helps in management of personal affairs, it becomes an ideal conduit for capturing minds. That is what social media is and that

is why its exploitation for propaganda and influence through information or disinformation is now being extensively researched and organizations created to cater to its potential. Equally the neutralization of the negative potential is being sought with vigour.

It was always presumed that the targeting of the mind would be a war winning factor. In the Information Age, as war rapidly moves from the conventional to the hybrid realm, and encompasses commitment of more irregular elements outside the organized component of armies and paramilitaries the necessity of ideological bonding has increased even further. As a corollary the breaking of these bonds and the psychological shielding of vulnerable populations is as necessary when targeting adversaries, both the state and non-state variety.

It's important to understand the means of communication and the progressive dynamics in this field but it is equally important to understand the ideologies of today that are attempting to be emplaced in vulnerable minds. Violent extremism of the modern age is an ideology which has developed over time. It encompasses radical faith which believes in no right of any alternative ideology or faith to exist. It reserves a self-believed right to employ unbridled violence to coerce the other towards its line of belief. Violent extremism is a phenomenon across boundaries of faith and different ideologies although in recent times it has come to be most associated with a percentage of followers of a sect of Islam due to the phenomenon of the Islamic State, the Al Qaida and a host of other local and international terrorist organizations. The use of the term radical extremist is best understood from the example of a young suicide bomber in Pakistan. When the suicide vest he was armed with malfunctioned he was captured by the security forces. On being queried as to why he was endeavoring to blow himself apart in public where those who would suffer would only be his co-religionists. His response was -"I am a true believer of the Islamic Faith. None of these people are Muslims because Muslims are only those who are like me and have my belief". In

other words his was a philosophy which sanctioned the persecution and targeting of anyone not of his faith or belief, not even those who followed Islam in different other ways. The intent of this segment of people is to influence the minds of others to draw them away from existing beliefs and align them to their philosophy of existence and value system. This intent can be exploited in an organized way by states and non-state entities such as terror organizations or simply by radical religious organizations to spread their faith and hold over larger number of believers. The best example is the manner in which the IS held hostage a large number people across age, gender, religious or social profiles and changed their beliefs, all through social media. 40,000 fighters and supporters were reported to have flocked to the IS as recruits to help achieve its aims of capturing and retaining territory. Scores of them across the globe remained in their home states promoting the cause through a series of web oriented instruments. Even after the defeat the IS suffered in Iraq and Syria it has remained in clandestine networked state running its campaign through social media and aspiring to rejuvenate itself in another territory where governance is poor, the people disaffected and a state of physical turbulence exists. The meaning of defeat and victory in hybrid war conditions of the type that the IS proliferated in, has apparently changed. A radical organisation believing in violent extremism can now hope that even after physical eviction and military defeat it remains alive to fight another day in another part of the world in a highly networked state through which it can emerge to original effectiveness.

Social media therefore is the new vehicle for promotion and spread of radical belief involving violent extremism. It is only going to increase manifold as the technological threshold rises and ease of accessibility enhances; with 5G on the cards in India and elsewhere, lightning speed of information transfer, larger video content and more modern ways of secrecy are likely to emerge. Visible chat rooms of the past may be passé. Ability to possess multiple accounts and concealment of identity is likely to increase.

Who are the vulnerable elements of society that are likely to be identified and subjected to communication of information with intent to influence their belief and garner their cooperation towards violent extremism? There remains an eternal debate whether poverty contributes to vulnerability to radicalization. International experience does not bear this out. However, in India and rest of South Asia it could be a truism although the ardent followers of the IS in Bangladesh, killed after the famous Dhaka Holey Artisan bakery case were all well to do young men. This leads us to conclude that vulnerability may exist across the board and no clear segmentation cannot be resorted to; the IS example bears this out where people from different backgrounds were influenced towards its cause.

Obviously a region under threat of separatism such as J&K will have higher vulnerability to radicalization and especially because it is politically high profile with a greater international interest. Besides that since Pakistan has selectively decided to employ faith as a weapon to garner support in J&K its agencies such as Inter Service Public Relations (ISPR) research and seek ways of influencing opinion and drawing target minds to the cause. Proxy war capability gets multiplied by religious radicalism embedded in the minds of the target population.

Sentiments relating to revenge and retribution for any specific acts perceived to be against the interests of a community will always contribute to enhanced vulnerability of individuals of that segment. Such identified individuals will be the target of radical organizations. It becomes far simpler to identify them and attract them towards a cause.

In generic terms, those who are unemployed, less employable or less capable of rationalizing good from evil due to poor exposure and having high orientation towards faith would be vulnerable. Those with unrealized aspirations and seeking alternative empowerment also get a release of pent up sentiments and grouses through ideas related to

radicalism. The medium of social media gives them a means of reflection with like-minded people and empowerment through acceptance of what they express. Mature and democratic orientation in social media interactions is rare. A thread may commence on a thought but swiftly people who perceive being outnumbered in their thoughts move out leaving the threads of discussion to those who express strongly, employ abuse or simply seem inflexible in thinking.

One of the major reasons why social media is a virtual revolution in learning, positive or negative is the ease of access and the shield of identity it provides. Smart phones are in the hands of anyone and everyone and new threads emerge every few seconds, keeping individuals rooted to it in habit forming commitment towards access. That is what helps radical organizations to keep scouts on the lookout for vulnerable accounts. The internet's highly advantageous purpose as an easily accessible information portal and communication channel is that it was designed to maximize simplicity of communication, not security of communication. The price for this has been the increasing opportunity to wrongdoers to exploit the vulnerabilities of the internet for their own ends. The real advantage of the communication capabilities of the internet through social media that radical semploy includes recruitment, propaganda dissemination and global linkage between terrorists as well as coordination of propaganda material through digital communication technology. In terms of recruitment to a cause the ability to transcend international boundaries is the big take away here. The best recruiting talent can be used from obfuscated IDs located in remote parts of the world without any personal danger.

Procedures and Formats Employed by Radicals

There are a couple of ends which are sought by radicals with acts of engaging people online through social media. First is a generic seeking of support to the cause or ideology espoused. If mass surveillance of IDs is done even physically it isn't difficult to pick up those who have

some orientation towards ideological vulnerability. Identification can be done through accounts on Facebook, Twitter and the like by initiating issues and keeping a watch on the threads of debates and discussions as they develop. However, with increasing development of deep data mining software, mass vulnerability can be picked up far more easily through just use of frequently used text. Identified elements are then focused upon to enhance their commitment and ultimately themselves become the conduits of spread of the message. Identities on social media are studied with the background information which is available. Social media enables 24x7 engagements in virtual anonymity especially through the plethora of messenger formats available. Identified IDs are drawn into private chats on messenger and then to the email format where persistent cajoling and motivation on the quiet and in anonymity is a guarantee. The messenger format includes text, photographs and video. In any form of information warfare, which is what this use of social media really is, knowledge about the subject which is to be used as the theme has to be comprehensive. For example if hatred against Indian security forces in Kashmir has to be spread then enough research has to be done to allow the targets to be sufficiently impressed by the overkill of knowledge, logic and the religious content which is splashed on them. In the background there is usually an organization which researches extensively to provide the required material. The internet helps keep all these elements physically far apart. The IS Twitter handle @shamiwitness functioned with total anonymity from Bangalore for fairly long espousing the cause of the organization and motivating youth towards recruitment in India besides contributing to the same in Europe. The use of preachers from the clergy with video clips and even direct talks through Skype like formats is used for reluctant but potential candidates. Blogs, Youtube accounts and email are used to communicate. The major advantage is that countermeasures, such as censorship or control of websites, have not reached levels of any surety. Below the surface and on the ‘dark net’ it is always possible to continue communication whenever internet is switched off in areas affected by violence or potential violence.

The second area of impact that radical organizations seek is home grown recruitment and extremist violence, amounting to virtual terror. Borders being reduced to status of being no obstacle to promotion of violent extremism do not need to be crossed by a large number of fighters as was in the past. Classically Kashmir is the best example of this. In J&K except for leadership which may be provided by some experienced Pakistani terrorists, there is little need for foreign manpower as motivation through social media continues at all times. Many of the local recruitments reported in South Kashmir are attributed to events such as funerals of terrorists killed by security forces where young men swear retribution and go into the bush. However, to arrive at that state of mind and take a final decision many of these youth are already radicalized through the medium of social media and clandestine meetings with clergy or like-minded people.

We have yet to witness a lone wolf event in J&K unless the Pulwama IED attack is classified as one. The young suicide terrorist was actually the end effect of a network which controlled him from Pakistan and within the Kashmir Valley and was not really a classical lone wolf. The latter are seen to be alone in more ways than one and largely self-motivated. Their motivation again is through social media and many of them may never really post anything except an odd agreement or disagreement. Yet they absorb a lot, learn the mechanics of violence and remain under cover far better than larger networks. Many of them like to record last messages or as in few recent cases even like to use head cameras networked to provide a live running video coverage of an act they perpetrate.

The importance of social media to radical organizations is best summed up by Ahmad al-Wathiq bi-Llah, an Al Qaeda member, whois quoted as describing what he calls Al Qaeda University graduates, as follows - “…graduates of the Al-Qaida University are specialists in electronic jihad, media jihad, spiritual and financial jihad, passing

through the 'faculties' of both morale and explosive package technology, and exploding cars and trucks".

Neutralizing the Social Media Oriented Violent Extremism

The approach towards the neutralization of the exploitation of social media by radical organizations has to be based on a set of principles and measures but before that a few core truths need to be recognized. The first is that if the radicals can employ the facilities of the internet to their cause and effectiveness, the same internet can be used by the state to neutralize everything they seek or do. There is a need for focus. The advantage that the state has is that it can institutionalize counter measures much more effectively and with far more resources. The handicap they face is the speed of response, bureaucratic laziness and lack of accountability for failure. An environment of awareness has to be inculcated in the plethora of agencies that abound in most states. Centrality of strategy is a must but a degree of flexibility and decentralizationis a core necessity. To add to this is the need for adequate research. To this end one of the nations which has demonstrated a will and followed it with action at a very early stage is Singapore. Its strategy is worthy of deep study and emulation.

Singapore has a small population of Muslims, many of them transient or temporarily in existence. It's a largely satisfied society where disaffection is least. However, it identified a couple of areas where penetration of radical thought is possible. Among them are centres of concentration of young male population; jails and prison houses, labour camps where migrant labour resides, schools, universities and clubs. It commenced with an outreach program done with physical engagement of Muslims, spelling out the virtues of Islam and explained the correct narratives the faith stands for. It brought in well-educated, multilingual and articulate Islamic scholars from Indonesia, Malaysia and within Singapore,and networked for research with the Nanyang Technical

University's International Centre for Political Violence and Terrorism Research, under the Rajaratnam School for International Studies (RSIS). The entire campaign is also online making use of what are called Internet Imams or moderate members of Islamic clergy capable of interpretations of the Hadiths and the Holy Quran to create positive narratives in young restive minds which are capable of taking a wrong turn in their development. With fake news becoming a phenomenon after rapid expansion of social media platforms the RSIS undertook greater research academically to support the state. Singapore's approach towards neutralizing any attempt by radical elements has been proactive but it's also largely because of the nature of its polity, size of population and levels of education.

The methods towards countering radicalization being spread through social media can be listed with description as under:-

- **Creation of Conducive Environment for Education and Debate.** Although not directly related to the issue of social media it's the start point and a contributory factor. A saner discourse on print and visual media platforms helps create the right environment to neutralize radicalization and dilute the 'othering' of minority elements who may feel isolated leading to brooding.

- **Sanity in Visual and Print Media**. Social media narratives draw a lot upon the print and electronic media with insertion of news clips, articles and photographs which are viewed and read by many people who could be gullible to propaganda or severely insensitive to others with alternative but not radical beliefs. Within the constraints of democracy it is always possible to issue advisories to media houses on what could be perceived as sensitive in the interest of national security.

- **Institutional Approach**. Counter radicalization using social media has to have an institutional approach. It has to form a part of part of a larger central body of experts who would frame policy and be constitutionally empowered to execute counter information warfare (communication strategy policy). Within this body a sub body focused on social media instruments needs to be formed. The dangers of not giving these efforts a legal framework could be unwarranted intrusion into privacy of individuals which is counterproductive.

- **Necessity of Research**. Among the major challenges in execution of strategy is that initial enthusiasm is based upon limited domain knowledge about only visible narratives which by themselves could be decoys to mislead counter efforts. There is a need for academic research on this with advice of historians, scholars, psychologists, legal experts, intelligence personnel and security specialists including armed forces personnel. Informed clerics who can provide information on the legitimacy or otherwise of radical religious issues, will be an added advantage. A campaign without the availability of such research and advice is likely to flounder in a short time. Technical expertise on software would also be necessary, especially in the ability to monitor and carry out data analysis.

- **Progressive Engagement**. The exact methodology employed by radical organizations of progressively drawing in identified IDs into discussions, isolating them and engagement through one on one debate, is the one which should also be the one employed to counter these efforts. Once the narratives being spun by handlers are identified, carefully crafted counter narratives need to be drawn up and used in a progressive manner. There should never be an attempt to use 'in the face' methodology to confront identified IDs or use threats.

- **Generic Narratives**. These should be used to flood the sites through accounts which appear friendly and credible without giving them an official colour. The life of such accounts is usually limited.

- **Using Existing Credible Accounts**. Credible accounts of many personalities who use social media as hobby or simply for expression of ideas and thoughts can always be harnessed for the national good. Personalities with larger followings can be provided sufficient material to project the counter views. These must not run counter to the ideas expressed in the account over a period of time. Hits to these accounts classify as generic outreach with moderate narratives.

- **Event Based Counters**. The adversaries who are either state based, or state supported non state entities will exploit events of a negative nature to pedal their narratives. The counter efforts must be prepared for this and not be overwhelmed by the sheer volumes of information which may flow.

- **Intelligence Support**. The involvement of intelligence agencies is inevitable as they have the means of discernment of threats and the ability to employ other means of gathering information on identified IDs and synthesizing inputs which are as essential. A counter effort against the use of social media cannot be in stand-alone mode.

- **Role of Local Police**. Intelligence agencies monitoring social media accounts must at some stage hand over details to local police authorities once coordinates have been confirmed. Local police may decide to handle the case on its merits by approaching parents, educational institutions and even associates, all discreetly. The approach towards someone getting radicalized or already radicalized may not always be the last resort of arrest

and incarceration. A reformative approach could be helpful in passing the message but it would all depend up in the merits of the case and the threat envisaged from such an individual or set of individuals.

India is at the cusp stage of exploitation of social media by adversaries of different colours who consider radicalization and pedaling of wares of violent extremism bearing non-state imprint. Not much has yet been lost. However, development of social media is taking place at a fast pace and unless countermeasures are institutionalized we may be overwhelmed. Our formal efforts thereafter may be unable to handle the opening of floodgates of information and the change in mindsets of vulnerable segments of the population.

Conclusion

The penetration of internet in India is deep and there are an increasing number of social media users across the country. Many of them do not possess the faculties to discern the negative ways in which social media can be exploited by adversaries. With religious radicalization and violent extremism becoming one of the major means of unobtrusively entering into existing and potential hybrid conflict zones the exploitation of social media to spread these ideologies among gullible sections of society is going to be endemic. While education is a good security against such threats the volume of effort and achievement cannot defeat the trends prevalent. Even well educated people remain novice at the realization on the potential of social media as a tool for anti-national activity. An effort has been made above to outline the nature of threats and how these work against the individual and the state while suggesting a series of measures to counter them. Prime among them is the need for institutional efforts on a national scale rather than depending on small efforts by agencies and other organizations.

***Lt Gen Syed Ata Hasnain, PVSM, UYSM, AVSM, SM, VSM (Retd)** is a Delhi based Defence Analyst

SAFEGUARDS IN DIGITAL INDIA

Maj Gen Umong Sethi, AVSM, VSM (Retd)*

"Cyber warfare is the biggest threat to national security which will render even the Inter-Continental Ballistic Missiles (ICBMs) insignificant as a security threat" - Dr APJ Abdul Kalam[1]

Digital India (DI)-An Overview

'Digital India' is an umbrella programme to transform India into a digitally empowered society. It weaves together a large number of ideas and thoughts affecting functions and activities of the state, economy, society and individuals into single comprehensive vision.[2] Focus is on three key areas. First, to provide digital infrastructure as a utility to all. In that, endeavour is to make available to all citizens secure cyber space, a unique digital identity, access to internet and space on public cloud. Second, deliver governance and services on demand. This vision envisages creationof an eco-system that is seamlessly integrated across departments, jurisdictions and is capable of providing all services and entitlements in real time on mobile and online platforms. Aim is to transform 'ease of doing business,' make financial transactions cashless and leverage GIS for decision making.

1 Air Mshl Anil Chopra, PVSM AVSM VM VSM (Retd), "Cyber: The Next Cold War", 2016,http://www.defstrat.com/cyber-next-cold-war quoted by E. Dilipraj andRamnath Reghunadhan Organisational Governance of Cyber Space In India, pp115 Air Power Journal Vol. 13 No. 1, spring 2018 (January-March)

2 MeitY presentation on Digital India.

Third, vision area is digital empowerment of citizens so that they can participate in governance. Here the exertion is to make citizenry digitally literate and capable of accessing documents as well as services available on collaborative digital cloud-based platforms in their preferred Indian language.

The scaffolding on which the program hangs comprises nine pillars. These are, development of broadband highways and national information infrastructure; universal access to mobile connectivity; internet access to the general public; promoting e-governance; electronic delivery of services; make easy access to all relevant information to all citizens; promote manufacturing as well as research & development of electronic goods within the country with a view to achieve net zero imports; use this platform to create jobs in the IT related sectors and undertake early harvest programmes to showcase utility.[3]

Transformative Outcomes of DI

Digital India has the potential to provide an incremental 20 to 30 percent increase in India's GDP by 2025.[4]An appraisal of the progress of rolling out of 'Digital India' initiative clearly brings out a steady increase in the internet and mobile users. According to McKinsey Global Institute (MGI), India's Digital Index rose by 56 percent during 2014-2017. This has placed the country second in terms of growth among 17 emerging and mature Digital economies.[5] In 2017 the number of mobile phone users in India was estimated 730.7 million. This figure could reach almost 468 million by 2021. India is now adding close to 10 million

3 ibid

4 Deloitte presentation for ASOCHAM Digital India Unlocking the Trillion Dollar Opportunity November 2016

5 3 years of Digital India – Here's what has worked and what hasn'thttps://www.peoplematters.in/article/industrial-relations/3-years-of-digital-india-heres-what-has-worked-and-what-hasnt-18332

daily active internet users every month, the highest rate of addition to the internet community anywhere in the world. Interestingly, nine out of every ten new internet users are exploring the online content only in their native language, heralding the dominance of a non-English internet user base in the country. Increased internet access, means increased digital services and growth of digital economy.[6] The growth is attributed to private players for making it affordable. As per data available in December 2017, 64 percent of urban India was on the internet, while only 20percent of rural India. This urban-rural divide is accentuated by lower digital literacy and rural electrification initiatives not having fully actualised.

Digital India is improving quality of life of citizens. People can apply online for licences, appointments at hospitals or access other services and receive updates on the status of their request. Initiatives aimed at students and farmers are gaining popularity. Efforts are showing results in crime tracking and police modernisation. VAHAN a highly flexible and comprehensive system is ushering computerisation of over 1100 Road Transport Offices (RTOs) across the country and is facilitating issue of e-registration certificate for vehicles and driving license online.[7] An online Motor Vehicle Coordination system, “Vahan Samanvay” is designed to coordinate stolen and recovered motor vehicles. Many State/UTs are also operating motor vehicle enquiry counters for public.[8]Even private businesses are finding it imperative to adopt multichannel delivery models in tune with changing times.

Digital payments have witnessed an upswing. Citizens have transitioned to transactions through credit/ debit cards, digital wallets, Unified Payments Interface (UPI), online banking and transfers. Use of mobile apps has greatly facilitated the shift. Government is making a

6 Ibid, Rituparna Chakraborty, Executive Vice President, TeamLease.”

7 Vahan Website https://vahan.parivahan.gov.in/vahan/vahan/ui/login/login.xhtml#navbarhttps://vahan.parivahan.gov.in/paidnrservices/

8 http://ncrb.gov.in/VahanSamanvay/Motor_Vehicle.htm

push towards cashless economy where citizens are able to pay taxes, bills and the like online with help of internet banking, credit cards and other non-cash mediums. However, digital literacy being low, security concerns, lack of understanding of benefits and large cash economy are causing some impediments.

Aadhaar is a 12-digit unique random number issued by the UIDAI to the residents of India after a verification process.[9]Government has introduced a number of initiatives under the DI where bank accounts, mobile phones and Aadhaar number are linked to get direct transfer of funds to the beneficiaries under various schemes. Aadhaar is used to create repository of 'cloud based' platform to safe-keep and easy to access documents electronically under 'Digi locker' initiative among others.

As per 2018 edition of 'E-Government Survey' of the United Nations titled, 'Gearing E-Government to Support Transformation towards sustainable and resilient societies', India, which was ranked 118 in 2014, 107 in 2016 jumped 11 places to be ranked 96 in 2018. The jump shows how digital technologies and innovations are impacting the public sector and changing people's everyday lives.[10]

Enormity of Digital Transformation Challenge

The five big core platforms that have citizens' information are 'Goods and Services Tax Network 920 million),' 'Income Tax Network (60 million),' 'Passport Network (250 million),' 'E-Governance Network

9 UIDAI website https://uidai.gov.in/what-is-aadhaar.html

10 E-Government Survey in Media https://publicadministration.un.org/egovkb/en-us/Resources/E-Government-Survey-in-Media/ID/1958/India-breaks-into-top-100-in-UNs-E-Government-index

(700 million)' and 'Aadhaar Network (1.2 billion)'. [11]Data across systems and agencies is increasing every minute. A few lakh people apply for Aadhaar every month or go to its centres to update or correct information. The government is the biggest player in DI with several petabytes of data residing with various agencies. It is responsible for its security related issues.[12]

Indian Railways moves 23 million passengers and 3 million tonnes of freight every day, deploying more than 12,000 trains across 115,000 km and some 7,000 stations. Operation and monitoring of train movement is computerised and available on demand to users. Railways are for their operations gather and process huge approximately 100 terabytes of consumer data annually. Its passenger booking platform has 25 million users, who make some 800,000 daily transactions. It is collaborating with a number of private players to enhance customer experience. Google has collaborated with Railways to provide free wireless internet access under the 'G Station project'. Over 400 stations, starting with Mumbai Central, have been covered in the past four years, with users consuming an average of 300 mb per session. The company claims this boost to public Wi-Fi usage would have added 40 million incremental users and a $20 billion impact on GDP.[13]

11 Economic Times How Safe is Digital India sourcing PwC, UIDAI Data https://economictimes.indiatimes.com/news/economy/policy/how-safe-is-digital-india-indias-vast-data-pools-need-to-be-secured-with-tighter-de-risking-tools/articleshow/62489823.cms?from=mdr

12 Challenges and Risks of Privacy and Personal Information Security in Digital India V Karamchand Gandhi1, Dr M Suriakala2 International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

13 Indian Railways is emerging as a hub of innovation for service providers. As India's largest employer goes digital, it's beginning to acquire huge scale in a new dimension — data. By Rahul Sachitanand, ET Bureau| Updated: Jun 02, 2019, 01.39 PM IST https://economictimes.indiatimes.com/industry/transportation/railways/indian-railways-is-emerging-as-a-hub-of-innovation-for-service-providers/articleshow/69612576.cms?from=mdr

Problem with govt databases is that these are live, accessed by multiple users within the govt and outside. That multiplies the security challenge.[14]

Safeguards within Digital India

Cyberspace governance is an important function of the State. It is fountainhead that lays down a framework for enabling environment for use of the cyberspace in an orderly manner and shape the evolution of digital services according to shared norms. The structure of the cyber governance framework in India is spread across various departments and organisations functioning under four ministries namely the Prime Minister's Office (PMO), Ministry of Electronics and Information Technology (MeitY), Ministry of Communication and Ministry of Home Affairs (MHA).[15]

The PMO is the highest decision-making body and is the ultimate authority with respect to governing, coordinating and supervising cyber space in India. Under the PMO, the prominent organisations that deal with governance in cyber space are the National Technical Research Organisation (NTRO); National Information Board (NIB) and National Cyber Coordination Centre (NCCC).

The Ministry of Electronics and Information Technology (MeitY) works as an enabler in transforming the nation into a digital superpower. Many organisations operate under the MeitY. Among them CERT-In is the national agency in the area of cyber security that monitors, collects, analyses, coordinates and disseminates information. It takes exigency

14 Economic Times How Safe is Digital India sourcing PwC, UIDAI Data https://economictimes.indiatimes.com/news/economy/policy/how-safe-is-digital-india-indias-vast-data-pools-need-to-be-secured-with-tighter-de-risking-tools/articleshow/62489823.cms?from=mdr

15 Organisational Governance of Cyber Space In India E. Dilipraj and Ramnath Reghunadhan AIR POWER Journal Vol. 13 No. 1, spring 2018 (January-March)

measures in emergency situations.[16] CERT-In also functions to prevent and mitigate crises in various strategic and core sectors.

The Ministry of Communication plays a major role in providing services, issuing guidelines and taking necessary action with regard to infrastructure development for supporting the cyber space framework in the country. The Ministry of Home Affairs (MHA) issues security guidelines, assists and sensitises other ministries, departments and critical sector organisations with regard to securing and protecting Critical Information Infrastructures (CIIs). Indian Cyber Crime Coordination Centre under MHA facilitates online reporting of cyber offences. This together with CERT-In and other State agencies aims to strengthen the capabilities to deal with issues like cyber theft, social media terrorism, related recruitment and cyber espionage.[17]

In order to provide secure infrastructure, National Optical Fibre Network (NOFN) was initiated. It was envisaged as an information super-highway through the creation of a robust middle-mile infrastructure for reaching broadband connectivity to all the 2,50,000 Gram Panchayats. Based on NOFN experiences, successor BharatNet aims at a highly scalable network infrastructure accessible for all households and on demand capacity to all institutions. The objective is to facilitate the delivery of e-governance, e-health, e-education, e-banking, Internet and other services to the rural India.[18]

In order to utilise and harness the benefits of Cloud Computing, Government of India initiated project “GI Cloud” named ‘Megh Raj’. The focus of this initiative is to accelerate delivery of e-services in the

16 “CERT India”, available online at https://www.cert-in.org.in/

17 E. Dilipraj and Ramnath Reghunadhan Organisational Governance of Cyber Space In India, pp 115 AIR POWER Journal Vol. 13 No. 1, spring 2018 (January-March)

18 BharatNet http://vikaspedia.in/e-governance/digital-india/national-optical-fibre-network-nofn

country while optimizing ICT spending of the Government.[19] NIC Cloud Services offers variety of service model to meet requirements like 'Platform as a Service (PaaS)', 'Infrastructure as a Service (IaaS)' and 'Software as Services (SaaS)'. Among other services, 'Vulnerability Assessment Service' aids identifying the security vulnerabilities. 'Anti-virus Service' keeps applications and data safe from viruses, spyware and other malware threats. 'Backup Service' allows backing updata and application codes.[20]

In 2017 Ministry of Electronics and IT issued guidelines on setting up of IT infrastructure by government departments using cloud computing technology with a clause mandating that all data must be stored within the country. The guidelines for departments hiring cloud services abroad on contractual terms mandates clearly mentioning data location in the agreement with the service provider.[21] Localisation of data is a major step towards making data bases secure.

'Secure, Scalable and Sugamya' Website as a Service (S3WaaS) is a website generating and deployment product hosted on the National Cloud of National Informatics Centre (NIC). It leverages technology to generate secure websites using GIGW compliant templates which are highly customizable and can seamlessly be deployed on a scalable software defined infrastructure.Using the service, district administration can create and deploy their websites.[22]

19 MeghRaj Cloud initiative https://cloud.gov.in/about.php

20 26 ibid

21 Government data on Cloud must be stored in India: Ministry of Electronics and IT https://economictimes.indiatimes.com/tech/internet/government-data-on-cloud-must-be-stored-in-india-ministry-of-electronics-and-it/articleshow/58288014.cms

22 http://vikaspedia.in/e-governance/digital-india/s3waas-for-government-department-websites

The Domain name 'NIC.IN' is owned by National Informatics Centre (NIC) and the same can be allocated ONLY to Indian Government Entities. However, now NIC is the authorised registrar for 'GOV.IN' Domains and it is advised to all Government Departments (Central & State) to host their websites under 'GOV.IN' Domain names.[23] This measure is aimed at regulating websites and issues related to database integrity as well as security.

The "Cyber Swachhta Kendra " (Botnet Cleaning and Malware Analysis Centre) is a part of the DI initiative to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. This centre operates in close coordination and collaboration with Internet Service Providers and Product/Antivirus companies. This website provides information and tools to users to secure their systems/devices. This centre is being operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of Section 70B of the Information Technology Act, 2000.[24]

Breaches of Digital Platforms in India

Notwithstanding the measures inbuilt in DI initiative, many breeches are reported frequently. A few major ones are mentioned to illustrate vulnerability of pooled Databases.

In 2018, a data breach was recorded of Aadhaar database, one of the largest Government databases in the world. UIDAI revealed that

23 Government data on Cloud must be stored in India: Ministry of Electronics and IT Economic Times PTI|Apr 21, 2017, 12.27 AM IST https://economictimes.indiatimes.com/tech/internet/government-data-on-cloud-must-be-stored-in-india-ministry-of-electronics-and-it/articleshow/58288014.cms?from=mdr

24 Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra) https://www.cyberswachhtakendra.gov.in/

about 210 Government websites leaked the Aadhaar details of people on the internet. A Google search would reveal thousands of databases along with demographic data including Aadhaar numbers, names, names of parents, PAN numbers, mobile numbers, religion, marks, the status of rejection of applications, bank account numbers, IFSC codes and other information.[25]

The breaches and subsequent public discourse on social media led to a petition in Supreme Courtchallenging the need and validity of Aadhaar. The Court upheldits validity and its mandatory use for welfare schemes, filing of Income Tax (IT) returns and allotment of Permanent Account Number (PAN). However, the verdict restricted the use of Aadhaar authentication by private entities in the absence of a legal provision. Pursuant to Supreme Court of India's directive to take measures to enhance safeguards and privacy, UIDAI initiated a number of measures. The Authority offered offline verification tools like eAadhaar, masked Aadhaar and Quick Response (QR) code that leverage the unique ID without authentication or any access to biometrics. It initiated the process of deleting the authentication log beyond six months and confirmed no such records will be maintained beyond six months in future as well. "The apex court has also asked us that no illegal immigrant should be given Aadhaar, so we have started reviewing our own process on how we can make the scrutiny of the document more rigorous...We are taking a number of steps to implement the order to enhance safeguards," UIDAI CEO Ajay Bhushan Pandey said in communique.[26] It has been clarified that No bank account was compromised because of Aadhaar data leaks. For Aadhaar to be breached, access to biometrics is needed. This is a near impossibility

25 Indian School of Ethical Hacking Aadhaar Massacre https://www.isoeh.com/exclusive-blog-details-biggest-cyber-attacks-of-2018.html

26 India's digital journey to accelerate with stronger safeguards: UIDAI PTI New Delhi November 04, 2018 17:06 IST The Week https://www.theweek.in/news/biz-tech/2018/11/04/India-digital-journey-to-accelerate-with-stronger-safeguards-UIDAI.html

as they are securely encrypted and never shared with anyone. A large part of non-biometric information that Aadhaar captures is already there in public domain as people share voluntarily on social media platforms. Banks have been communicated that Aadhaar eKYC can be only used to authenticate beneficiaries of government subsidies and welfare schemes. For other customers, physical or electronic offline Aadhaar (in a masked form) can be used for verification so that such customers can be served digitally.

The personal data (including digital payment means used and nominee details) of 200,000 IRCTC passengers was made vulnerable to hacking through a bug which offered free and mandatory travel insurance, reports the Economic Times. It is unclear if any data was stolen, but the bug reportedly existed for nearly two years.[27]As per IRCTC's annual report for 2016-17, e-ticketing accounted for 62 percent of reserved railway tickets in India, with more than 573,000 tickets sold daily through the IRCTC website.

As per the information presented by the Indian Computer Emergency Response Team, over 493 websites were affected by malware propagation including 114 websites run by the government. healthcare data of India was left exposed without enough security measure. This mistake was found out during a regular security audit. The audit discovered that India based IP contained a data pack that's been left exposed without any security measures.[28]

In their paper, 'Challenges and Risks of Privacy and Personal Information Security in Digital India,' V Karamchand Gandhi and Dr M Suriakala mention, "The greatest threat to Digital India could arise

27 A free insurance bug caused data vulnerabilities on the IRCTC website and app Namita Singh ttps://www.medianama.com/2018/11/223-2lakh-rail-passenger-data-vulnerable-insurance-bug-irctc/

28 Major Cyber Attacks on Indiatestbytes Security Testing Thursday August 23, 2018 https://www.testbytes.net/blog/cyber-attacks-on-india/

from hackers residing anywhere in the world — state-sponsored or otherwise. About 20 years back, 40-bit encryption was considered high-tech. Today it can be breached in minutes and companies have moved to 128-bit and 256-bit encryption. Databases like Aadhaar are secured with 2048-bit encryption. That could take thousands of man hours or several years to break the fence. However, what appears impregnable today could succumb to quantum computing (QC) in just a few years. Today's encryption methods could be brought down with QC in minutes. It could become main stream in 8-10 years."[29]

As far as private sector is concerned, 69 per cent Indian companies are at most risk of cyber-attack. At least one third of organisations in these suffered at least one cyber security incident in the last 12 months.[30]A cyber-attack was carried in August 2018 on Cosmos Bank's Pune Branch by hacking the server. Over 22,000 websites were hacked between the months of April 2017 and January 2018. These are but a sample of many such breaches reported almost daily.

Serious threat that comes from lack of cyber-security among the citizenry. Use of smartphones that stores a lot of information and unrestricted use of apps that constantly pry on data poses a grave concern. Use of public printers or scanners to copy document linked to government database expose the individual. Networked community presents opportunities to hacker and information warrior to manipulate and exploit.

29 Challenges and Risks of Privacy and Personal Information Security in Digital India V Karamchand Gandhi1, Dr M Suriakala2 International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

30 69% Indian firms face serious cyber-attack risk: Study https://economictimes.indiatimes.com/tech/internet/69-indian-firms-face-serious-cyber-attack-risk-study/articleshow/69305216.cms

Conclusion

Cyberspace, advanced computing, mobile networks, unmanned systems, and social media present a revolution in information warfare. As information age technologies become more useful across all spheres of activity, vulnerabilities to disruption, deception, penetration, theft, and destruction increase as well.[31]Banking systems, railway and airlines networks, stock exchanges, strategic national security systems, communication networks and the like, are undeniably dependent on security of IT networks and structures. Many of the key systems are vulnerable due tolack of safeguards or redundancy.

The threats in cyber space will evolve in new forms with the emergence of the Internet of Things (IoT), cyber physical systems, cloud computing and other future technologies. The New "Net" monitors & controls critical Infrastructure. Its integrity & availability is critical for economy, public safety, & national security.[32]According to Dr VK Saraswat Member, NITI Aayog, "Critical infrastructure is prone to increased risks due to interconnectivity across sectors, proliferation of exposure points and concentration of assets."

Data sovereignty and localisation of critical data, enhancement of capability to produce systems within the country and have skilled skin-ware to operate and protect critical information infrastructure is the way ahead!

***Maj Gen Umong Sethi, AVSM, VSM (Retd)** is a Delhi based Defence Analyst

31 Information Warfare Past, Present, and Future Nick Brunetti-Lihach November 14, 2018 https://www.realcleardefense.com/articles/2018/11/14/information_warfare_past_present_and_future_113955.html quotingAmy Zegart, "Horns of a Dilemma: Even Cybersecurity is bigger in Texas," (Podcast), 2018, https://warontherocks.com/2018/03/horns-of-a-dilemma-even-cybersecurity-is-bigger-in-texas/

32 Presentation on Cyber Security by Dr VK Saraswat Member, NITI Aayog

‘JUGAAD’AND INFORMATION WARFARE MADE FOR EACH OTHER

Rear Adm Monty Khanna*, AVSM, NM

Information Warfare (IW) has existed in various avatars from time immemorial. Both Chanakya’s Arthashastra as well as Sun Tsu’s ‘Art of War’ dwell at length on this subject, particularly on the importance of deception. During the colonial era, the British used it to their advantage, perfecting the art of intrigue and subterfuge resulting in defections and fractionallised opponents that played a pivotal role in their victories and subsequent conquests. This was facilitated by a well-oiled intelligence network that leveraged technology such as wireless communications as well as telegraphy to constantly remain several steps ahead of the opposition they encountered.

As the industrial age gathered momentum, the mass production of increasingly capable military hardware changed the character of warfare. While IW mattered, the potential advantages of force asymmetry brought about by the industrial capacity to mass produce potent weapons gained ascendency. In these attrition-dominated battles, the focus of human endeavour shifted from information dominance to industrial efficiency and productivity. Sound management practices backed by engineering skills became the new mantra of winning conflicts. These skills were not only applied to the accretion of assets but also in their employment. New disciplines such as ‘Net Assessment’ and ‘Operational Research’ with all their mathematics and probability theorems played a dominant role in subjugating adversaries, a vivid

example of which is the manner in which the Battle of the Atlantic was played out during the Second World War.

Post conflict, the victorious allies translated this war-winning strategy to other walks of civilian life. The dominant theme in the new world was productive efficiency. Management and engineering became the professions of choice in a highly rule based world that prioritised efficiency over everything else. Processes were streamlined to iron out uncertainties and bring about much greater predictability which in turn,once again contributed towards enhanced productivity thereby creating what may best be summed up as a constantly elevating virtuous spiral. Management practices such as '*Just in Time*' owe their genesis to this environment as they are rooted in certainty and predictability regarding the delivery of inventory just prior to its requirement. In this world, countries that adapted themselves rapidly in terms of equipping their people with requisite skills and creating the required infrastructure to support these best management practices prospered. They outdistanced themselves from the rest of the developing world where the yoke of uncertainty was too heavy to shed.

There has, however, been a consequence of living in a highly developed predictable society. Generations brought up in such an environment have gradually lost the art of coping with uncertainty. Deviations of any nature in these rule bound societies are frowned upon and take time to resolve. The intent is more often than not, to seek systemic long-term solutions to problems even where prompt quick fix solutions will suffice.

Let me quote you a mundane example to drive home this point. During my tenure as the Naval Attaché in Washington D.C. about a decade ago, I had the Naval Chief visiting the United States. The United States Navy at their efficient best churned out a draft programme two months prior to the visit. At their persistent urging, the programme was frozen about a month in advance. Once finalized, getting even the

smallest of changes to the agreed programme was neigh impossible. Changes after all bring uncertainty which is despised in their society. Fast forward to five years later where I am the Assistant Chief of Naval Staff for Foreign Cooperation and Intelligence (ACNS FCI) at Naval Headquarters in New Delhi. We have the chief of the Australian Navy in Delhi and he is making his official call on the Chief of Naval Staff on a Monday morning. In accordance with his programme, he is scheduled to depart for Mumbai the next morning by service aircraft. Because of my designation, I happen to be sitting-in during the official call in CNS chambers. As the conversation drifts, the Chief asks his guest if he has been to the Taj Mahal. On receiving a negative response, he expresses surprise as to why he didn't ask to have it put in his itinerary. Knowing where this conversation is leading, I am starting to feel uncomfortable. The next sentence comes as no surprise, "You can't leave India without seeing the Taj. FCI, please fix that". I scrambled out of the office in haste. My staff and I spent the better part of the day obtaining necessary approvals, amending flight plans and resolving protocol issues. To cut a long story short, the Australian Navy Chief and his spouse did get to see the Taj Mahal and get a most memorable photograph taken sitting on a bench with this astounding creation of love and devotion in the background.

What makes us so different in this respect from western cultures? To my mind, having been brought up in an environment of uncertainty makes us agile at the personal level and to some extent at the organisational level too. While things may have changed in some respects today, the vast majority of my generation has been brought up in an uncertain world. We were uncertain about even basic requirements such as power, communications, transportation, running water and what have you. What did we do to adapt? - 'Contingency planning!' What if…..? is a question that comes to us naturally. We are constantly and involuntarily planning for hypothetical problems that could rapidly become real. Since we are likely to be confronted by so many of them, the preference is for the 'quick fix' or '*jugaad'* approach

rather than a long term holistic response. While this may be detrimental in a process dominated shop-floor of a production plant, it may not be so in tomorrow's information dominated world.

Force asymmetry brought about by productive efficiency has undoubtedly played a key role in the wars of yester-years. The Japanese learnt this the hard way during World War 2. While common sense told them that with the bulk of the U.S.N. fleet sunk in Pearl Harbour on the seventh of December 1941, the United States government would seek an accommodation with them, they failed to factor in the industrial might of this nation and the consequent capacity to regenerate lost assets. In a matter of a year, the tide began to turn and in less than three years the remnants of the Imperial Japanese Navy were being decimated at Leyte Gulf in the Philippines by a humongous U.S. Navy that outnumbered them many times over.

Since World War 2, the world has witnessed another revolution centred on rapid strides that have been made in the field of Internet and Communications Technology (ICT). The consequent information explosion powered by an exponential increase in internet connectivity and ubiquitous mobile devices have brought about big changes in all facets of life including the manner in which we conduct war. The hitherto predominance of asset-based asymmetry in combat is being challenged by the effects that can be produced by highly targeted disinformation campaigns that leverage the modern era'sspeed and reach of information dissemination.

How does information warfare differ from traditional means of engaging in hostilities? Firstly IW is non-kinetic. Not being bound by the traditional 'Laws of Armed Conflict', its conduct is not restricted to the formal declaration of hostilities. In a sense, it gets to be played persistently 24 X 7 X 365. Secondly, it requires a totally different skill set. The efficient and process based approach of problem solving so

critical to industrial manufacturing are not designed to keep up with the agile twists and turns of rapidly evolving IW campaigns. We have witnessed this in several recently fought wars against shadowy outfits like Al-Qaeda and ISIS. Using speed and nimbleness, they have succeeded in putting large, well-trained and robustly resourced armies on the back foot. While one may make the argument that they have eventually been defeated, the heavy handed approach used in doing so has created deep fissures and cleavages in society which is exactly what these organisations intended to do – so victory is questionable. Thirdly, IW campaigns require a deep and nuanced understanding of the character and culture of people they are targeted against. So while traditional warfare has been biased towards engineers and technicians, IW favours psychologists and anthropologists. Even an innate understanding of these subjects without formal schooling is adequate. Further, as human character varies significantly from place to place, regional players are better equipped to practice it as against distant expeditionary powers. Fourthly, traditional warfare thrives on cutting edge weapons, the development of which are enabled by large R & D outlays. It therefore comes as no surprise that developed countries with considerable capital and human resources tend to be good at it. IW on the other hand largely rides on existing technology that has widespread civil use. As a consequence, organisations with even modest budgets are capable of crafting highly effective IW campaigns.

From the above, it can be seen that IW is the proverbial equalizer in the conduct of modern day warfare. Advantages that developed nations have accrued for themselves through sustained investment into sophisticated technologies essential for designing and building modern day weapons can be significantly eroded through thoughtful IW campaigns. Undoubtedly, this too requires skills and resources, but as mentioned earlier, these are at considerable variance from those demanded by the military industrial complex which has been a dominant factor in wars hitherto.

IW is a manpower intensive discipline that thrives on grabbing fleeting opportunities as they present themselves. It requires tremendous agility and dexterity to retain control of the information narrative as the opposition attempts to fight back. The single-minded focus has to be on speed and seeking rapid solutions to situations as they present themselves; many of which have to be devised on the fly. As mentioned earlier, this is an environment much more attuned to the average Indian where we thrive on finding quick fix solutions to problems that constantly present themselves in our daily lives. The culture of *Jugaad* is thus a perfect fit for the information warrior.

We are also well placed in some other ways. India has the largest pool of IT trained professionals in the world. Our strength in the field is amply demonstrated by the fact that most of the IT majors have vast numbers of Indian professionals on their pay-roles. The ability to circumvent technical hurdles and find innovative solutions is therefore resident in country. It is also well recognised that in today's world the internet is the primary medium of moving information. Here too we are advantaged. We have leapfrogged land line connectivity and embraced mobile devices as few nations have. Data rates in the country are currently the cheapest in the world by far and as per December 2018 data, the number of internet users in the country has risen to 566 million and is projected to cross 627 million by end 2019. Deep familiarity and a high comfort level with the virtual world amongst our youth is a resource that has important connotations in IW. All we need is an institutional approach to put all these moving parts together and convert them into capabilities that would make us dominant in the control and exploitation of information.

In conclusion, it may be said that we are extremely well poised to embrace IW as a force multiplier for meeting our strategic goals. All the building blocks to do so are available in our country. The need of the hour is, therefore, to create the requisite structure and assign responsibility along with accountability. Existing organisations engaged

in the field could be subsumed, amalgamated or simply brought under a well thought through structure so as to ensure that we operate in a synchronised manner. While doing so we would need to be careful that the primary tenets of successful IW; speed and responsiveness, are not compromised. Having missed the bus for industrial warfare in the past, we need to ensure that we don't meet the same fate as this opportunity presents itself. We need to leverage our culture of *jugaad* to excel in Information Warfare.

***Rear Adm Monty Khanna, AVSM, NM** is an Assistant Chief of Naval Staff for Foreign Cooperation and Intelligence (ACNSFC) at Naval Headquarters, New Delhi

CYBER SPACE – A TOOL FOR INFLUENCE OPERATIONS

Air Mshl Anil Chopra, PVSM, AVSM, VM, VSM (Retd)*

In the aftermath of the Indian Air Force (IAF) Balakot air strikes of February 2019 and the Pakistan Air Force (PAF) riposte of 27 February began a propaganda and perception war. The battle had the public of both the nations not only as an audience but also active participant in the information war that followed. This was many steps ahead of Indo-Pak Cricket wars. Information operations are an integral part of cyber warfare. Today rhetoric and imagery are as important as weapons as decisive elements in warfare. They are essential for constructing the good and the bad, legitimatizing one's actions and influencing the events. Era of perception management is now here as a part of war. Interestingly drawing the line between preparations for cyber war and the actual fighting is difficult. So this is a gray area between war and peace. Cyberspace has been a battleground in all recent major conflicts, yet it is difficult to say how and to what extent this activity influenced the conflicts' results. The intelligence communities actively use cyberspace to collect and manipulate information. Information operations (IO) not only influence public opinion; they also influence what we hold as true in any relationship that involves information exchange. The higher the level of political decision making using information, the more substantial the effect of information manipulation will be.

Cyber Era and Information Warfare

The cyber era has widened the battlefield to cover entire societies, and has made the global public into an active participant. Today, controlling information flows is very complex and difficult. Any form of information, fact or rumor, spreads much quicker and more freely in the cyber domain. Information operations, the vector for manipulating perceptions, are integral to cyber warfare. Manipulating perceptions is being combined with intelligence and cyber espionage, military deception, and disruptive or destructive cyber operations to advance a nation's goals. Subtle information operations try to persuade the target audience to view this information in a positive light. Perceptions determine how each actor chooses to act. If one can affect the opponent's policy goals by manipulating perceptions, it can have a great influence over the battlefield. Recently Russia fought and won an "information war" during the run-up to the Crimean vote[1]. Information operations exist not only to advance one's own message, but also to block or disrupt the flow of opposing ideas.

Manipulating Public Opinion

In the 1960s, Daniel Moynihan had said that everyone was entitled to their own opinions but not to their own facts[2]. The internet allows people to have their own facts. Social media amplifies this trend. Face book has become the primary source of news for many around the world. Russia, Iran, and China fear the effect of social media on their own societies, yet the Russians have been astute in using it to shape Western views, while the Chinese use it to impose a conformity in discussion and opinion in their own population. Many countries use internet trolls to shape social media narrative in ways favorable to their regimes and damaging opponents. Over time, the primary mode for organizing cyber troops has gone from involving military units to strategic communication firms that take contracts from governments for social media campaigns.

Social Media Soldiers and Fact Check

"Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation" by Samantha Bradshaw[3], concludes that cyber troops are a pervasive and global phenomenon. 'Social media soldiers' are today actively advancing national goals on social platforms associated with the free exchange of information among private citizens. Social media has provided opportunities for 'citizen journalism', and they have no less weight than the major content producers and established media personalities. Unfortunately any information, irrespective of the source may be manipulated or given a tilt. Many websites and cyber handles have now come up for 'fact-checking', so as to help the public know the truth, but they are not being able to keep pace. Social Media may not influence or change the outcome of the on-going conflict, but it puts perception pressure on decision makers, puts doubts in the minds of public and affects the morale. Some countries like Pakistan are skillful in successfully automated trolling though the use of 'chat bots'.

Psychological Warfare

It is a broad term for directing the emotional aspect of strategic communication. When specific information involving psychological components is delivered to a defined target audience, this audience experiences a shift in its emotions and outlook. As a result, there is a shift in the target audience's behavior, tarnishing its ability to reach the goals it has set for itself. It could also create conditions for the ending fighting or of surrender, encouraging defection and so forth. Information has the potential to evoke an emotional response in those exposed to it, especially if this information comes from war zones. Psychological warfare operations can be executed both during war and peace.

Influence Operations

For a successful influence operation, the planning includes, goal creation, target audience definition, scheme outline, group leader's influence, information sources, intellectual attitudes, alternative information sources, advocating change, and quantity of transmitted information. Disseminating specific information to a distinct target audience to control its responses is important. Influence operations are usually identified with technological capabilities from the world of computers, but in effect, each of its operations that combines elements of trickery and deceit would be considered an act of Information Warfare (IW).

Fifth Generation Networks

5G cellular network technology which has started unfolding since late 2018 provides much faster broadband access. The first fairly substantial deployments were in April 2019. As it replaces current 4G networks, it promises to accelerate cellular data transfer speeds from 100 Mbps to 10 Gbps and beyond. 5G radio hardware is already in the market. In 5G, the 'air latency' target is 1-4 milliseconds estimated to be 60 to 120 times faster than average 4G latencies. 5G is crucial for Internet of Things (IoT). Large quantity of new spectrum will have to be added for 5G. The frequency band most widely being used for 5G in this range is around 3.5 GHz. Meanwhile there are concerns related to interference with passive remote sensing and weather and earth observation satellites. US DoD has cautioned harmful impacts to national security due interference. Because of espionage fears on foreign users by Chinese equipment vendors, several countries have taken actions to restrict or eliminate the use of Chinese equipment in their respective 5G networks. Also it had stoked fear that 5G radiation could have adverse health effects. Belgium and Switzerland had blocked a 5G trial because of radiation laws[4]. 5G will become a faster tool for IW.

Artificial Intelligence and Cyber Weapons

Nations which have greater resources, are developing Artificial Intelligence (AI) based cyber weapons. Elsa Kania, an American expert on Chinese military talks of Chinese efforts to transform 'informatized' way of warfare into 'intelligentized' warfare by using AI[5]. The AI based cyber weapons would be far more destructive as they could manoeuvre to exploit vulnerabilities or even would be able to create new vulnerabilities.

International Conflict in Cyberspace

A Center for Strategic and International Studies (CSIS) report of September 2018[6] has brought out how information technology is reshaping international security. It is helping new resurgent powers to upset the status quo in the existing world order. Internet, which was to create a world without borders and without external interference has now become a tool for external interference and conflict. Cold War was bipolar, but new conflict is multi-polar. Wars between big, heavily-armed states are expensive and risky, so cyberspace has become the preferred battleground, taking advantage of the 'grey area' that is neither peace nor war. Internet lends itself to coercion, anonymity, deniability, and has instant global reach. Cyber-attacks can produce effects similar to kinetic weapons. The strategic goal is to affect morale, cohesion, political stability, and, ultimately, diminish the opponent's will to resist. The intent will be to degrade 'informational advantage' in warfare by attacking communications and ISR assets and capabilities, to slow and damage decision making and operations, and to create political uncertainty, turmoil, and dissent. The 'rules of war' themselves have changed significantly, nonmilitary options have come to play a greater role in achieving political and strategic goals.

Responses to Information Warfare and Influence Operations (IWIO)

Sun Tzu, wrote that "The supreme art of war is to subdue the enemy without fighting", and that best suits IW and IO. By definition, IWIO take place without kinetic violence, and are below any threshold of armed conflict. There are no noncombatants. Every individual in the adversary's population is a legitimate target. Cyber-enabled IWIO strongly leverage the capabilities of modern computing and communications technologies. When an adversary uses kinetic weapons, a country usually knows that it has been attacked, as it may cause death or destruction. A cyber campaign may not be detected if its effects were intended to be kept secret. The rapid emergence of large numbers of automated social chat bots promulgating similar political messages could signal the start of a concerted campaign. Investigation could point to national affiliations of parties operating such bots. When legitimate institutions are under attack, it is an indication. Coordination among intelligence-gathering agencies will improve capabilities for detecting IWIO campaigns. Defensive measures against IWIO require measures to help people resist the operation of IWIO weapons targeted at them, and measures to degrade, disrupt or expose an adversary's arsenal of IWIO weapons.

International Fact-Checking Network (IFCN)

First step to degrade, disrupt or expose the arsenal of weapons being leveraged against a target population, is to run fact checkers at organizational level. IFCN has been set up to promote excellence in fact-checking and accountability in journalism[7]. Responsible media must make commitments to nonpartisanship and fairness; transparency of sources, and funding. Face book is already committed to providing fact-checking services to Face book users. Face book has also introduced a button that makes it much easier for users to signal that they regard a given story as fake news. Google has decided to prevent its advertisements from appearing on fake news sites, thus depriving

them of revenue. For political advertising on Face book are required to include information about who paid for them. In future IWIO threats would focus on forensics to detect forged email, videos, audio and so on. Visual and audio information associated with specific events once had dispositive value for authenticating events, conversations and other exchanges, but with advanced Photoshop and audio and video editing software widely available this assumption of certitude is simply no longer valid, and the authenticity of images and recordings will be increasingly debated rather than automatically trusted.

United States Cyber Command (USCYBERCOM)

USCYBERCOM was created in mid-2009 at the Nation Security Agency (NSA)[8]. It cooperates with NSA networks. While originally created with a defensive mission in mind, it has increasingly been viewed as an offensive force. On 04 May 2018 USCYBERCOM was elevated to the status of a full and independent unified combatant command. It operates on two levels: tactical, and strategic. On the tactical level, it sends teams of IW experts to interface with globally positioned U.S. joint task forces, in accordance with the requirements of the Joint Chiefs of Staff. On the strategic level, It serves as an IW authority for all U.S. Department of Defense (DoD) agencies.

Russian Military Approach

Russian military has adopted an approach by which tactical military field operations, and political, diplomatic strategy across various international forums are integrated and interwoven components of the systemic concept. Cyber warfare and IO are combined efforts that include systemic attacks on digital networks, psychological warfare, fraud, misdirection and disinformation. Russia's goals contributes not only to weakening the opponent, but also to empowering Russia's image. The heavy reliance on IW stems from Russia's acknowledgment of its military and economic inferiority, in comparison to the U.S. and China.

Israeli Approach

Israel has three military entities operating in the fields of strategic communications and IO with various populations. The Center for Consciousness Operations was established in 2005[9], and coordinates with the Operations Branch and Military Intelligence Directorate. In Operation Cast Lead, the center mounted psychological warfare in the Gaza Strip against Hamas fighters and civilian populations. Most of these messages were delivered through newscasts broadcast across different types of media. Israeli C4I Corps is primarily tasked with launching IW against the enemy. The PR branch of the IDF manages operations directed towards various overseas audiences. The branch initiates and organizes visits to Israel by key figures (foreign military personnel, government officials, academics, etc.), coordinates PR missions for a variety of overseas conferences and helps pen studies overseas written about the IDF. These activities are performed under the premise that creating a pro-Israel stance overseas will propel foreign leaders to adopt a friendlier stance towards Israel. Israel supports websites, Face book pages, video segments, radio broadcasts and Twitter feeds, all in accordance with IW guidelines.

China Major Cyber Threat

After the Chinese cyber-attack on Google's computer systems in December 2009, China has been classified as a major Cyber threat. Hundreds of thousands have been employed in this state sponsored Cyber warfare. All are specially trained and most are English proficient. People's Liberation Army (PLA) Unit 61398[10] has been very active in cyber espionage and cyber-attacks. The unit is located in Pudong area of Shanghai. Pudong also happens to be location of the main undersea cable between China and the United States. They have reportedly stolen hundreds of terabytes of data though an extensive network of computers spread across the world. The attack on Google was essentially to steal intellectual property rights, and assess and

use the near 500 million Google user passwords. Major targets are strategic industries, defence establishments, weapon and military technology companies. China's IWIO efforts are focused primarily on its own population and Chinese emigrants. Chinese propaganda has persuaded the world of its inevitable economic ascendancy. Chinese doctrine for the military use of cyber operations is more conventional. It focuses on disrupting weapons performance and command functions. China has undertaken cyber operations to gain access to U.S. weapons systems to understand their operational limits, copy them, and to prepare to interfere with their operations in combat. China works on cyber operations combined with electronic warfare, anti-satellite attacks, informational campaigns and other unconventional tactics and weapons.

Chinese Electronic Hardware Threat

India's heavy reliance on imported equipment and mobile apps pose a serious security challenge. Indian intelligence agencies have warned that China was collecting data from India through popular Chinese mobile apps. The Chinese Xiaomi smart phones and notebooks are suspected to be transmitting personal data to the servers located in China. China is exporting devices equipped with backdoor surveillance tools. Huawei and ZTE are notorious in this sphere[11]. China also purchases companies dealing with computer network with this intention. The Chinese company Lenovo, which bought IBM' PC business in 2004, was reportedly shipping laptops with 'superfish' malware which undermines basic security protocols. The threat from imported equipment would significantly increase if we continue to rely on imported equipment for 5G network as well as that may have back door surveillance system based on Artificial Intelligence.

Pakistani and Jihadi Approach

Pakistan seems to have realised that for a Cyber attack one does not talk about "death by 1000 cuts" or attacking critical infrastructure to produce a "cyber Pearl Harbor". Since Pakistan is at a deep disadvantage in terms of conventional military power, it leverages asymmetric options like terrorism, and IWIO supplemented by AI. They create realistic fake videos, or "deep fakes," which appear authentic. Use India's internal social cleavages, which heightens such a risk. Pakistan has mastered the craft of proxy war over the last three decades in Afghanistan and Kashmir. A group of Pakistani hackers, who specialize in surveillance software have been hired by the Pakistani ISI to create spyware versions to target key government officials in India. Pakistan Inter Services Intelligence (ISI) supports jihadi terror organisations to use cyber space for collection of sensitive information and spreading misinformation to change the rational thought process of youth. ISI is using smart-phone malware embedded gaming, music apps to spy upon military personnel. Pakistan military is also using radio and TV channels for spreading anti-India propaganda. Jihadi groups are using websites to incite the youth to take to arms. Most communal incidents in India were preceded by intensified circulation of fake videos to incite people to resort to violence.

Cyber Attacks on India

According to a study by CERT-IN the cyber-attacks in India[12] almost 40% originated from China, 25% from US, 13% from Pakistan and 9% from Russia. The attacks from Pakistan and North Korea are on the increase. The targets were financial networks, Government websites, power plants, oil refineries, oil and gas pipe-lines, and telecom and defence networks. There are large 'leakages' of huge data from MNCs which are increasing in scale and frequency. The Cambridge Analytica firm was suspected to have harnessed data from almost 87 million Face book users, out of which over half a million were Indians,

and leveraging them for political campaigns. Similarly, Microsoft has routinely shared the financial details of Indian bank customers with intelligence agencies in the United States. The Chinese website of official newspapers like Global Times and People's Daily contain anti-India articles.

India's IWIO Strategy

India is gradually realizing the significance of IWIO but a lot needs to be done in this field. India established the National Information Board (NIB) in 2002[13] and is chaired by National Security Adviser. The NIB is the highest policy making body for cyber security and IW and periodically reports to the Cabinet Committee on Security headed by the Prime Minister. The Indian Armed Forces are also represented in it. However, the NIB's capabilities for countering IWIO needs to be enhanced significantly. An independent National Fact Checking Organisation needs to be established for not only checking facts in a transparent manner but also to formulate a code of principles for fact checking which would help media to check authenticity of news. The need for making citizens aware of misuse of social media platform to exploit our fault lines and cultural differences is important. India must find indigenous telecom solutions and equipment to ensure its safety. An effective system of providing incentives to Indian telecom entrepreneurs should be established. India needs to devise time-sensitive rapid government response to adversary IWIO campaigns. Immediate steps must be taken to check the narratives built by our adversaries to influence our population and weaken democratic institutions. The NIB must engage best professionals in the field to counter IWIO. It is a round the clock activity. Government needs to work closely with all social platforms and electronic and print media to counter IWIO. There is a need to make citizens and security personnel aware of misuse of social media platform to exploit our fault lines, and also include this subject in the educational institutes. The newly formed tri-service Defence Cyber Agency (DCA) will work in conjunction with

the National Cyber Security Advisor. Its focus will be towards offensive and defensive military cyber-issues. It would include as many as 1000 personnel from all three branches, the Army, Navy and the Air force. The National Cyber Security Policy was adopted by the Government of India in 2013 to ensure a secure and resilient cyberspace for citizens, businesses and the government. DCA is meant to combat the current threat from China and Pakistan. The Agency will have smaller teams, spread around the country. It will position dedicated officers in major headquarters of the forces to deal with emerging cyber security issues. DCA highlights the threat to cyberspace and cyber as a tool of modern warfare. DCA must find indigenous solutions and equipment. There should also be an effective national cyber strategy so that all stakeholders can work as one force.

***Air Mshl Anil Chopra, PVSM, AVSM, VM, VSM (Retd)** is a Delhi based Defence Analyst

Notes

1. https://lithub.com/russia-is-winning-the-information-war/

2. https://www.brainyquote.com/quotes/daniel_patrick_moynihan_182347

3. http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf

4. https://in.reuters.com/article/swiss-5g/switzerland-to-monitor-potential-health-risks-posed-by-5g-networks-idINKCN1RT15J

5. https://www.uscc.gov/sites/default/files/June%207%20Hearing_Panel%201_Elsa%20Kania_Chinese%20Military%20Innovation%20in%20Artificial%20Intelligence.pdf

6. https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace

7. https://accountablejournalism.org/ethics-codes/international-fact-checking-network-fact-checkers-code-of-principles

8. https://www.cybercom.mil/About/History/

9. https://www.haaretz.com/israel-news/with-eye-on-hearts-and-minds-israeli-army-sets-up-consciousness-ops-1.5888362

10. https://in.reuters.com/article/china-military/chinese-military-force-to-take-lead-on-cyber-space-defence-idINKCN0V71AI

11. https://www.theverge.com/2018/5/2/17310870/pentagon-ban-huawei-zte-phones-retail-stores-military-bases

12. https://www.hindustantimes.com/india-news/cyber-attacks-becoming-more-frequent-in-india/story-8Os6AtCrHzL6QCBinVQuSM.html

13. https://www.medianama.com/2016/04/223-indias-cyber-security-agencies/

AN INTEGRATED APPROACH TO INFORMATION WAR - INDIAN CONTEXT

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

> 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.

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. 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 area 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.

The Basic Features of Information Warfare

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.

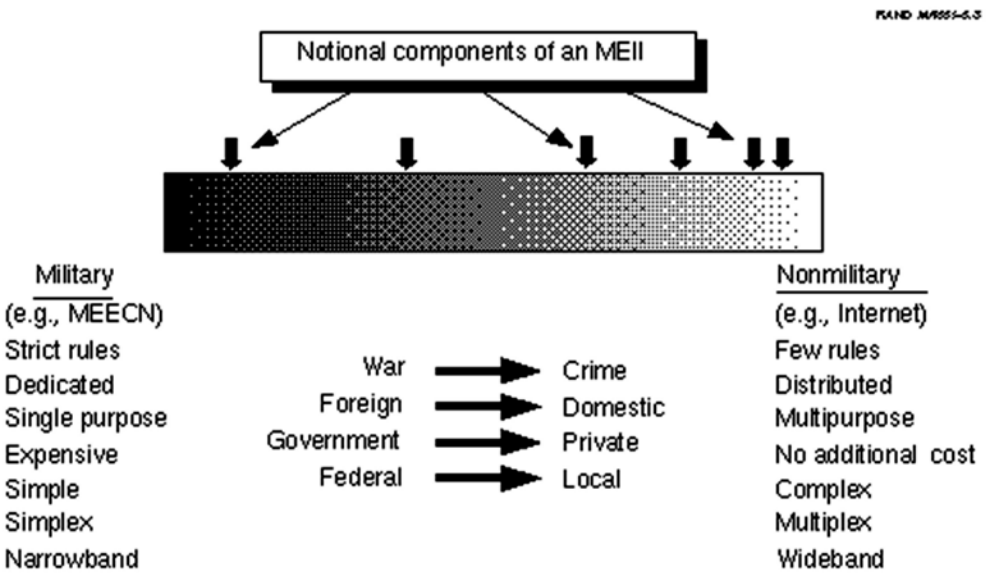
A new strategic intelligence challenge: Poorly understood strategic IW vulnerabilities and targets diminish the effectiveness of classical intelligence collection and analysis methods. A new field of analysis focused on strategic IW may have to be developed.

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.

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 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.” 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. 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:-



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. 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.

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 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.

***Lt Gen Vinod Bhatia, PVSM, AVSM,SM (Retd)** is a former DGMO and now Director CENJOWS, New Delhi

DETAILS OF PUBLICATIONS 2018-19: CENJOWS

S No.	Author	Nomenclature	Remarks
Book			
1.	Brig (Dr) Rajeev Bhutani (Retd)	Sino-Indian Equation: Competition + Cooperation – Confrontation	Feb 2019
Monographs			
1.	Shri R Chandrashekhar	China-Pakistan Economic Corridor: Furthering the Initiative and Progress on Projects	Jan 2018
2.	Shri R Chandrashekhar	Gilgit Baltistan – Political Control Under Pakistan Occupation & Recent Developments	Jun 2018
3.	Shri R Chandrashekhar	Pakistan Occupied Kashmir	Jul 2018
4.	Col Arvind Sharma	Analyzing The Training Methodology of Special Operations Forces (SOF) of Foreign Armies & Recommendations for Conduct of Special Forces (SF) Training	Oct 2018
5.	Dr Manabrata Guha & Prof David J Galbreath	The Multi-Domain Battle Concept: A Preliminary Assessment	Dec 2018
6.	Brig (Dr) Rajeev Bhutani (Retd)	Geopolitics to Geo-Economics to The New Era of Geo-Technology	May 2019
7.	Team CENJOWS	Interim Budget 2019-20 Analysis	May 2019
8.	Shri R Chandrashekhar	XINJIANG	Jul 2019
9.	Brig Navjot Singh Bedi	5G, IOT & IT's Relevance for the Armed Forces	Jul 2019
Issue Briefs			
10.	Shri R Chadnrashekhar	China Pakistan Economic Corridor: Furthering the Initiative and Progress on Projects	Jan 2018
11.	Shri R Chadnrashekhar	India's Armed Forces in the National Military Security Matrix-Need for 'Comprehensive' Integration	Apr 2018
12.	Brig (Dr) RK Bhutani (Retd)	Profile: China's President Xl Jinping	May 2018
13.	Gp Capt GD Sharma, VSM (Retd)	Examin Role for India in the Indo-Pacific Region	Jun 2018
14.	Brig Ranjit Singh	Pragmatic Approach to Counter Chinese Juggernaut in the 21st Century	Feb 2019
15.	Air Vice Marshal D Choudhury, AVSM, VM, VSM	Joint Approach to Warfare: Concept of Operations	Feb 2019

S No.	Author	Nomenclature	Remarks
16.	Capt (IN) KK Agnihotri	High Technology Developments in China: Leveraging for Military Effectiveness	Mar 2019
17.	Col Arvind Sharma	Analysing Indo-Afghan Relations: Pakistan's Strategy of Interference & Lessons from US Intervention in Afghanistan	Apr 2019
18.	Brig Saurabh Tiwari	Defending/Explaining EM Spectrum Against for Cyber Warfare	Jun 2019
19.	Brig (Dr) Navjot Singh Bedi	RF Spectrum Allocation Process in India	Jun 2019
20.	Lt Gen PR Kumar, AVSM, VSM (Retd)	A Strategic Perspective of the Continental Defence of India: Pivotal Constituent of the Multi Domain Competition Environment	Jul 2019
Occasional Paper			
1.	Maj Gen (Dr) PK Chakravorty, VSM (Retd)	Manoeuvre Warfare	Apr 2018
2..	Shri R Chandrashekhar	The India Myanmar Trilateral Highway: Present Status"	May 2018
3..	Lt Gen Sunit Kumar, AVSM (Retd)	Cyber-Alike Nontraditional Wars (Combined)	Jun 2018
Synodos Paper			
1.	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)	Revisiting Maldives_ India's Military Intervention	No2/Feb 2018
2.	Lt Gen Rameshwar Yadav, PVSM, AVSM, VSM (Retd)	CPEC: Fundamental Negative Paradigms	Feb 2018
3.	Lt Gen (Dr) NB Singh, PVSM, AVSM, VSM (Retd)	Mission Engineering the FICV	Mar 2018
4.	Shri R Chandrashekhar	India-Asean Relations: Way Forward	Mar 2018
5.	Lt Gen Vinod Bhatia, PVSM, AVSM, SM (Retd)	Post Wuhan – Imperative to ensure peace & Tranquility along the Line of Actual Control (LAC)	May 2018
6.	Col Harpreet Singh	Minimising Casualties in Counter Insurgency/Counter Terrorism Operations	May 2018
7.	Air Cmde T Chand (Retd)	Artificial Intelligence (AI) and its Applications for Defence & Security Forces	June 2018
8.	Rear Admiral Monty Khanna, AVSM, NM	A Case for Eliminating Permanent Commission at the Entry Level	June 2018
9.	Col Shyamji Yadav	Asean Discord in South China Sea	Jul 2018
10.	Rear Adm Monty Khanna, AVSM, NM	The Indian Air Force & Theaterisation-Misplaced Apprehensions	Jul 2018
11.	Col Arvinder Singh	Security Challenges in the Indian Ocean Region	Jul 2018
12.	Col Sumit Rana	Defence Production Policy 2018: Opportunities & Challenges	Jul 2018

S No.	Author	Nomenclature	Remarks
13.	Brig HS Cheema	India-Bangladesh Relations A Way Ahead	Jul 2018
14.	Rear Adm Monty Khanna, AVSM, NM	Merger of Public Sector Shipyards-A Crying Necessity	Jul 2018
15.	Col Harpreet Singh	Blockchain: Military Applications	Jul 2018
16.	Rear Adm Monty Khanna, AVSM, NM	How Does China Build its Warships at a Fraction of our Cost?	Aug 2018
17.	Lt Gen K Surendra Nath, PVSM, AVSM, VSM (Retd)	Re-Attire, Re-Skill; Re-Serve; Enabling a Second Career to Veterans	Sep 2018
18.	Lt Gen Rajesh Pant, PVSM, AVSM, VSM (Retd)	Cybertronic Warfare-Beware the Monk!	Sep 2018
19.	Rear Adm Monty Khanna, AVSM, NM	It is Time We Raised Our Own Maritime Militia	Oct 2018
20.	Lt Gen (Dr) NB Singh, PVSM, AVSM, VSM (Retd)	Equipment Capability Planning.	Oct 2018
21.	Gp Capt Ashish Singh, VM, VSM	The Two Forms of Reforms	Oct 2018
22.	Maj Gen Bipin Bakshi, VSM	Information Warfare: Redefining National Security	Nov 2018
23.	Brig (Dr) Navjot Singh Bedi	Social Media & The Armed Forces	Dec 2018
24.	Shri R Chandrashekhar	The Gilgit Baltistan Order- 2018	Jan 2019
25.	Lt Gen AB Shivane, PVSM, AVSM, VSM (Retd)	IBG: Powering The Future Ready Force VOL-XIII No-2/Mar 2019	Mar 2019
26.	Brig Gurmeet Kanwal (Retd)	Cooperative Security in the Indo-Pacific: Managing China's Rise Vol-XIII No.3/Mar 2019	Mar 2019
27.	Brig Deepak Mehra, KC, VSM	Russia and Pakistan: Strange Bedfellows Vol-XIII No 4	Apr 2019
28.	Lt Gen (Dr) SP Kochhar, AVSM**, SM, VSM (Retd	Mainstreaming Cyber Org & Trainings for Army Vol-XIII No 5	Apr 2019
29.	Lt Gen AB Shivane, PVSM, AVSM, VSM (Retd)	Leveraging Space for National Defence "Capabili-ties, Strategic Outlook and Recommended Framework" Vol-XIII No 6	Apr 2019
30.	Air Cmde T Chand (Retd)	Virtual Reality (VR) – Likely Military Applications Vol XIII No 7	Jun 2019
31.	Brig HS Cheema	Doctrinal Direction Towards Reforms and Modernisation of PLA Vol XIII No 8	Jun 2019
32.	Rear Adm Monty Khanna, AVSM, NM	Managing Threats to Maritime Stability Vol XIII No 9	Jun 2019
33.	Lt Gen Balbir Singh Sandhu, AVSM, VSM (Retd)	India's Look/Act East Policy: A Comprehensive Review	Jul 2019 Vol-XIII

CENJOWS

CENTRE FOR JOINT WARFARE STUDIES

(Web site: www.cenjows.gov.in - Email: cenjows@cenjows.gov.in)

APPLICATION FOR LIFE/ ANNUAL MEMBERSHIP

To,
The Director
Centre for Joint Warfare Studies (CENJOWS)
Room No. 65, Kashmir House
Rajaji Marg, New Delhi 110011

Dear Sir,

1. Please register me as a Life ☐ /Annual ☐ member of the Centre for Joint Warfare Studies (CENJOWS).
2. I undertake to abide by the Rules and Bye Laws of the Institution.
3. My particulars are given below:-
   (a) Name in full …….....
   (b) Address:-
      (i) Office/Unit…….....
      Pin Code …… Phone No …….....
      (ii) Permanent/Residential …….....
      …….....
      Pin Code…..... Phone No.....
      Mobile No (Optional)…….....
      (iii) Email …….....

Optional Fields

(a) Parent Service Army/Navy/Air Force/Civil Services …….....

(b) Rank/ Designation…..…….…. (c) Decorations ……...…. …….….

(d) Appointment ……..... (e) Personal Number …...……

(f) Date of Commission ……..…..... (g) Serving/Retired……..…..

4. Areas of expertise or interest:-

(a) ……. …….....

(b) …….....

(c) …….....

5. Any other information that may be of interest to the CENJOWS (including important exposures):-

……

……

6. Proof of my identity (Copy of passport/ voters ID Card/ PAN Card/ Iden Card) will be produced after approval of membership.

7. The following are enclosed:-

(a) Demand Draft/Cheque in favour of CENJOWS payable at New Delhi.

(i) DD/Cheque No……..……. dated…….....

(ii) Amount …….....….....….

(iii) Drawn on ……. Bank.....

(b) Two stamp sized photographs for membership card.

Place : …….....……

Yours faithfully,

Date : …….....……..

FOR OFFICE USE ONLY

Identity Card/Document No: …….. To be verified by Secretary.

New Delhi

Date …..... ……. Secretary, CENJOWS

Accepted/Rejected

Membership Number …… …….

Place: New Delhi

Date:.....…….... Director CENJOWS

Note:-

1. Life membership is open for all serving and retired personnel of the Armed Forces, Government Ministries, Academia, members of other think tanks and others interested in studying defence and military strategy.

2. Membership Fees:-

(a)	Life Membership:-		
	(i) Serving/Retired Officers	-	Rs 1,500/-
	(ii) Civilians	-	Rs 10,000/-
(b)	Annual Membership	-	Rs 1,000/-