An Analysis on Information Warfare Space on a Regular Collusive Nature of Transborder Proxy War and Hybrid Warfare

Dr. Rajesh Kumar, Associate Professor, Department of Defence Study, Govt. College Ateli (Mahendergarh) , Haryana, India
Email ID: dr.rajeshsaini70@gmail.com

ABSTARCT

In the modern era of hybrid warfare, governments have switched to the unorthodox use of information warfare to impose their national will on an adversary with apparent anonymity and without breaking international laws on other nations' sovereignty.To wage the fight in infospace, the Fifth Dimension of Warfare, information security must be a crucial component of national security.Electronic warfare, psychological operations, cyberwarfare, military deception, and operational security are all possible elements of information warfare.The current situation calls for a comprehensive strategy for operationalizing a mix of psychological warfare, cyber operations, and electronic warfare, which are the well-established elements of information warfare. Since proprietary software that runs information systems, control over numerous apps providing essential services, and massive data collection giants like Google and Facebook have colonized us in a NeoColonial way, Third World nations, including India, will have to work hard to offset the information advantage of the First World.The world is only now becoming aware of the Internet Giants' immense power as a result of the information they possess and their amazing ability to sway people's ideas, choices, and outcomes of events. The Cambridge Analytica discoveries and a number of other instances of information warfare in action highlight the importance of information superiority in the modern day.

In information warfare, which has elevated the idea of information security to a new level, information serves as both the weapon and the target.This conflict is distinct from those fought in the physical domains of land, sea, air, and space since it is fought in the virtual infospace.Edward Waltz, a former Manager for Information Understanding Programs at The Environmental Research Institute of Michigan, was one of the first well-known authors on the subject. He claimed that information warfare encompasses three crucial characteristics of conflict at the national level: information dominance, information protection, and information attack2 in his groundbreaking work, released in 1998. Since then, there has been a significant evolution in the doctrines and conceptions of information warfare as the notions he proposed were put into action. The idea of information warfare (IW) was first established and articulated under US military doctrine before being subsequently adopted in various versions by several countries.Since the early 2000s, the Indian Army has also employed officers in information warfare positions. IW encompasses the fields of electronic warfare, cyber warfare, and psychological operations, as can be seen from the various doctrines and studies that have been published in the USA over a period of time. These three major components are also a part of er Warfare, which consists of computer network attack, defense, and exploitation.

KEYWORD: Social Sciences, Social Sciences General, Information Warfare, Transborder

INTRODUCTION:

In information warfare, which has elevated the idea of information security to a new level, information serves as both the weapon and the target.This conflict is being fought in an informational virtual world.This distinguishes it from the four physical domains of land, sea, air, and space.One of the first well-known Edward Waltz, who formerly served as the Manager for Information Understanding Programs at The Michigan Environmental Research Institute. He wrote in his ground-breaking book, released in 1998, that Three crucial facets of national conflict are covered by information warfare: information hegemony Information Attacks And Information Protection2. There has been significant advancement in the ideas and theories of information warfare.

Information Warfare : American Concepts and Components

The term Information Warfare can be traced to one of the first instances of its use by the Office of Net Assessment, USA where in the 1970s, Dr. Rona described the competition between competing control systems in the cybernetics field as "Information Warfare"3. Subsequently the US military has used the term Information Warfare (IW) for a considerable period before expanding it to include a wider range of activities in Information Operations(IO). Daniel Kuehl explained the relationship between IO, IW and CNA(Computer Network Attack) in his paper published for a US Naval War College Publication in 2002, wherein he states that IW is to be performed primarily by the military in a specific conflict while IO involves the military and civilian agencies. By and large the activities envisaged in IW and IO are the same, with IW being practiced at the Military level in a specific conflict and IO at the National level across the PeaceConfilct Peace continuum. Daniel Kuehl, in his writings, has extracted three important definitions from the US doctrinal publications as under :-

Information-Psychological Warfare which is conducted under conditions of natural competition, i.e. permanently; and affects the personnel of the armed forces and the population of the adversary

Information-Technology Warfare Which is conducted during wars and armed conflicts to affect technical systems which receive, collect, process and transmit information

It may be seen that both US and Russian thinking on IW is beginning to connect Psychological Manipulation with use of Technology to jointly operate in the Information Domain for waging Information Warfare. While terminologies vary, the focus on use of various IW means to achieve Information Dominance and influence the outcome of peaceful competition as well as military conflict is evident. A study of Russian actions in Crimea has reinforced this synergy between Electronic Communication and Psychological Messaging. One study propounds that future Russian military adventures may include a far higher and frequent level of coordinated EW and Psyops. Much as conventional military communications are the vector by which orders and plans are transferred into action, civilian telecommunications are the vectors by which Psyops are conveyed12. The Russian concepts, strategies and structures reflect this skilful use of Military and Civilian infrastructure and manpower in a synchronised manner to achieve national goals. There is ample evidence of the success of the Russian approach in Ukrane, Crimea, Europe and America, so much so that American Information Warfare practitioners have started focussing a lot of effort to counter Russian IW attacks and also to design IW offensives against Russia. IW Transformations in the UK Information Manoeuvre Command The United Kingdom has recognised the evolution of warfare from Air- Land- Sea Manoeuvre to Information Manoeuvre. They have created an Information Manoeuvre Command that intertwines three domainsVirtual, Physical & Cognitive for decisive advantage. Some of the key points from a presentation by the British speakers during a seminar13 at Delhi in June 2018 and July 2017 are Information is the Lifeblood of the Battlefield Whoever wins in the Infospace wins Info Manoeuvre replaces Air- Land Sea Manoeuvre.

“From a computer room or from the trading floor of a stock exchange a lethal attack on a foreign country can be launched from anywhere. In such a world is there anywhere that is not a battlefield? Where is the battlefield? It is everywhere.”

The importance of information as an enabler for state affairs, and as a tool for inter and intra state conflict was always understood by statesmen and military thinkers since time immemorial. However the process of disrupting the thought process and paralyzing the internal functioning of an adversary with non- kinetic means, using elements of information and technology in various forms has developed more recently into a distinct form of warfare, namely Information Warfare. Waging Information Warfare (IW) during peace, competition and conflict spectra has enlarged the scope of actions a Nation needs to take in pursuit of National Security. such warfare and developing the capability to strike back in similar coin is a domain of human endeavor that merits analysis and study. Non traditional bodies like terrorist groups, contending factions within nation states and even individual private citizens are wielding influence across national boundaries and are playing significant roles in world politics. Hybrid threats have emerged exploiting the Revolution in Military Affairs, emerging technologies (infotech, nanotech, biotech and Social Media) which have begun to shape doctrine, strategy and tactics of Defence Forces around the Globe. Fourth and Fifth Generation Warfare has been spawned along with the emergence of the Super-Empowered Individual (SEI). These new trends have led to the emergence of new methods of violating sovereignty and achieving objectives without using conventional armed forces.

The Concept of National Security

As outlined above the concept of security itself has evolved beyond mere defence of land borders in an interstate conflict. Today there are multifarious threats to economy and society in a complex and dynamic world order from both state and non-state actors. National security now environment which imposes both internal and external threats in various dimensions, many of which do not involve the use of force.

Significance of Information Security

The battle of the mind is increasingly fought over digital media hence securing our infospace is of increasing importance. The storage and flow of information is shifting to digital form today while traditional forms of storing and sharing information are being pushed into oblivion. Therefore the importance of Print, Radio and Television in the context of information media and ofhard copies of files, minutes of conferences and records of discussions is reducing. Physical security of a HQ, a power station or electric sub station today does not prevent digital manipulation that can completely disrupt the functioning of the facility by manipulation of the digital systems involved in its operation today. It is axiomatic that the means of securing our critical information and infrastructure needs to be accordingly adapted to meet the new challenges in the digital age.

Impact of Information Warfare on National Security.

The components of National Security need to be analysed to put them into context and analyse the impact of Information Warfare in almost all domains of human conflict. Further the need to transform the conceptual construct as well as our structures.

Components of National Security

The concept of National Security today encompasses elements beyond the military forces needed to ensure territorial integrity. While this study will recount the views of several authors and thinkers on the subjects of National Security and Information Warfare, it is observed that both these concepts have generally been analysed separately. In certain countries the importance of the Information Domain as a key component of its military capability has been recognized, however it is felt that Information as a Domain of Warfare and Security needs to be integrated at the conceptual level in a more holistic manner. Therefore this study will attempt to derive the Components of National Security as given in the box on the left while those that have been postulated by the National Defence College, New Delhi are in the box on the right:-
India is facing challenges in the Information Warfare space on a regular basis be it concerning the collusive nature of proxy war and Hybrid Warfare or spread of radicalism and terrorist ideology. These challenges are all manifesting on a daily basis in electronic, print and social media and other means of public diplomacy. The internal and external vectors challenging our security and impeding our pursuit of National Interests will be identified. Some of these are competition with China, Proxy War waged by Pakistan, Transnational Terrorism and threats to our economic growth.

Methodology and the review of the literature

The research work has employed the descriptive, explanatory and analytical method. It is a method in which the researcher has attempted to analyze and interpret both the primary and secondary sources. The useful literature for this research work are books and articles in journals and periodicals written with varying degrees of relevance on National Security and on Information Warfare as available in the open domain.

INDIA'S NATIONAL SECURITY IN THE MODERN ERA

Concepts of National Security

A renowned expert, Barry Buzan states that security is taken to be about the pursuit of freedom from threat and the ability of states and societies to maintain their independent identity and their functional integrity against forces of change which they see as hostile8 . This may be analysed in the light of Section 1.2 wherein National Security is seen to have expanded in scope beyond the use of military power to secure or expand territory. In the last three decades we have seen the increasing potency of non state actors and transnational terror groups who are exploiting ethnic, religious and cultural fault lines to exacerbate divisions and further their inimical designs. These organisations operate with impunity across International Boundaries riding on the improved global connectivity and they have scant respect for national or international laws. These radicalised groups have harnessed Information Technology and Social Media effectively to propagate their extremist ideology, and therefore comprise a rising and ominous threat to human security which did not exist, at least in this form and potency, in earlier times. The UN Report on Human Development also mentions in this context that the main threats to security are those that travel across international borders in the form of terrorism, drugs, HIV/AIDS, climate change and illegal migration9 . There have been recent instances of Nation States exploiting Social Media to influence elections in another state, which is also a violation of sovereignty. Thus the natureof the threats to National Security have been transformed by the dawn of the Information Era. Security is evidently required in several domains including the information domain and not just military security in the erstwhile limited context of interstate conflict. In view of these changes in the threat landscape, there is a need to incorporate Information Warfare as a critical component of National Security in the Information Age.

International Law and its relevance to IW

International conventions and the UNO and most nations are signatories to what are termed as the compendium of agreements and understandings which include the basic principles of military necessity, humanity, proportionality and chivalry. However LOAC do not address hostile efforts by a party to impose its will on another without using spectrum. The type of damage that such attacks may cause may be significantly different from the kind of physical damage caused by traditional warfare. Bombs and bullets are visibly destructive, however, the disruption of information systems may cause intangible damage, such as disruption of civil society or government services. The intangible damage the attacks cause to civilian or military targets may not be the sort of injuries against which the humanitarian law of war is designed to protect non-combatants. Finally, the ability of technology to operate trans-border results in intangible violation of national borders that may not comprise traditional violations as in a military attack and hence may not invoke measures under the LOAC. The attacks riding on the Information Domain are capable of physical damage and disruption, but cannot be classified as an armed attack as defined under international conventions. Under these circumstances, we cannot expect any international support in thwarting the Information Warfare attacks which we face, and therefore, we need to formulate our own strategies, structures and responses as an intrinsic part of our National Security.

Components of National Security

United Nations Development Programme Human Development Report has sought to put the individual, not the state, at the centre of the picture, and to focus on his or her interests at the expense of the traditional state-centric approach. The report states that the concept of security has for too long been interpreted narrowly: as security of territory from external aggression, or as protection of national interests in foreign policy or as global security from the threat of a nuclear holocaust. It has been related more to nation-states than to people.16. However, with the dark shadows of the cold war receding, one can now see that many conflicts are within nations rather than between nations.

Defining of National Security Components

The various components of National Security discussed above will be studied in the context of the emerging Information Warfare threats and opportunities. We shall include the elements mentioned in the Russian National Security Strategy, the UNDP report, the writings of Rajesh Basrur, and other security experts as well as those included in the curriculum of the National Defence College, New Delhi, India.

Military Security :

The Security of Frontiers defined on Land, Sea, Air and Space are prime components of National Security. In the evolving era, protection against foreign military threats continues to be the cornerstone of security, however the need for collaboration in achieving this aim is gaining greater importance in South Asian nations as analysed by several experts. Military Security is graduating to Space Warfare very rapidly with anti satellite weapons being developed on space platforms as well as ground based weapons having the capability to destroy or disable the satellites of an adversary. Military Forces all over the world are maintained to counter these threats as well as to provide the host nation the capability to respond with military force against its adversaries in a conflict. Information Warfare also affects the military in all four dimensions just as it affects the civilian infrastructure, civil society and the national leadership and it is the military that has taken the lead in developing offensive as well as defensive Information Warfare capabilities. However Information Warfare needs a wider response that may not be restricted to the Armed Forces alone, but need a whole of nation , and even a whole of society approach. Therefore Information Security is a domain that includes, but is not restricted to, military measures to wage the Information War.

Environmental Security is crucial to the quality of life. It encompasses.

Availability of basic needs such as clean water and air; Freedom from the vicious cycle of poverty, deforestation, soil erosion, flooding, and receding water tables; Judicious environmental management with regard to the exploitation. Concerns relating to the potential degradation of the environment as a result of armed conflict be it nuclear, conventional, or low intensity. Externally, the state has to engage in inter-state negotiation to preserve the environment and at the same time combat protectionist pressures ope for collaboration among South Asian countries

CONCLUSION

It has been discussed how the absence of a National Security Strategy to include the Information Security Strategy is a serious lacuna in the Information Age where warfare has shifted to the 5th Dimension. We can neither escape from the relentless attacks that are being launched in Infospace on a 24x7 basis nor can we continue to deny ourselves the capability for offensive IW and deterrence against such attacks. The importance of adapting our strategies, structures and staffing patterns to achieve security in the age of Information Warfare has emerged in the course of this research. The ongoing Information War that we are facing cannot be won by old fashioned forces and structures, which are likely to be degraded by the information attacks unless we reorganise, restructure and conceptualise our actions to manage the Information Domain in the context of conflict with other nations and with nonstate actors. This assumes greater importance and urgency in view of the looming China coupled with the perpetrated by inimical forces. This 2 ½ front threat is further compounded by the Information Warfare threat from all over the globe that threatens our Core Values, our National Integrity and, indeed, our very existence as a Nation- State. In the information domain there are no clear demarcations of threats and capabilities unlike the other 4 domains of Land, Sea, Air and Space. All the Information Warfare agencies and the adversaries are riding on the same medium, whether for espionage, sabotage or crime, whether for financial purposes or for securing or degrading National Security. Therefore there are numerous overlaps in the activities of all these agencies leading to duplication of effort, cyber jostling, possible fratricide, compromise of access gained to adversary systems, conflicting approach to the same targets and a host of other coordination issues. A study of the existing apex level structures suggests that a formal relationship between the decision making authorities, the advisory bodies and the executing authorities is lacking. The NSCS and the related organs have no direct control over the ministries who are actually dealing with the threats and challenges for which these organisations are providing policy directions and recommending future courses of action. There is also a separation of these prime advisory bodies from the decision making body that is the CCS, owing to a structural filtration of the NSCS advice through the NSA or the Cabinet Secretary. The apex advisory organs are supposed to service the NSC and hence have no access to the CCS. This kind of separation of advisors from decision makers and the executing ministries runs across all organs involved in Intelligence, National Security and Cyber Security, and there is a further separation due to the existence of the National Security Council in addition to the Cabinet Committee on Security. This framework is quite unique and is now being reorganised for greater synergy and effectiveness to include a revamp of the NSCS and the setting up of the Defence Planning Committee. Attempts are under way to streamline and synchronise these multifarious stake holders. For example the independent wings of Army Navy and Air Force are being amalgamated to function under a Joint Service Organisation under the Chairman Chiefs of Staff Committee while the Public Information and Information Warfare structures of the Indian Army will be merged, upgraded and enhanced to a new Director General Information Warfare. The tendency to raise multiple structures with overlapping charters continues as does the malaise of posting general duty officers for limited tenures in highly specialised appointments. At no level do we see a holistic approach to Psychological Warfare, Cyber Operations and Electronic Warfare which are the established components of Information Warfare The integration of efforts of these multiple organs continues to pose challenges even as more and more new structures are being created to function in Infospace. As we can see above some steps are being taken to improve the capability to respond to the ongoing threats in the Information Domain, however a review of the above structures in the light of the scope and extent of virulent Information Warfare attacks will reveal that there is inadequate integration of existing structures and a lack of focus on certain elements like Psychological Warfare. The battle in the Information Domain needs to be fought in a synchronised manner as most nations have already become adept at this new form of Hybrid the word. Fragmented organisations working separately in the Cyber and Cognitive dimensions will be quickly overwhelmed and defeated in this new form of warfare which is ongoing today. The manner in which Information Warfare strategies and structures are being designed, evolved and employed by other nations varies greatly according to their political dispensation, threat perception and emphasis on information as a domain of conflict. However the important aspects of the study done above include the need to integrate the three dimensions of Information Warfare, Cognitive, Technical and Physical at one level and the Military, Academic and Civilian components of the nation at another level. Separation of all these elements is likely to result in a fragmented development of concepts, strategies and doctrines as also a sub- optimal execution of Information Operations which will be detrimental to the future of the nation. With a number of adversaries or competitors adopting a more integrated approach to Information Warfare, those nations which choose to ignore this critical aspect are bound to face losses and defeats in peace, conflict and war, and will remain unable to pursue their National Interests. The need for integrated and focussed structures, both for conventional wars and Information Warfare may be seen to have emerged clearly from this study. The Lead Agency for Information Warfare has been recommended as Ministry of Defence which must play a critical part in waging Information Warfare, particularly against adversaries operating from areas outside our land boundaries. A suitable organisational structure for Information Warfare in India needs to be formulated by drawing relevant lessons from other nations described in the study. The conceptual underpinning needs to be a synchronisation between the Information-Technical and Information-Psychological Dimensions of Information Warfare to influence the Cognitive Dimension. The structures and concepts of the Information Manoeuvre Command of UK would be a good model to study and the es Public Relations Directorate, the Chinese Strategic Support Force and the Russian Spetsnaz. formulate a Draft National Security Strategy is a significant step towards a revamp. To this end the contents of this research may be submitted for appropriate consideration in the process of formulation of the future strategies and structures. The staffing patterns and structures of the apex level entities also need considerable revamping which would flow from the National Security Strategy and some pointers could be taken from this research in this regard.

REFERENCE

Qiao Liang and Wang Xiangsui, Chinese Air Force Officers,. Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House. Feb 1999, available at. https://ia800201.us.archive.org/0/items/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui/Unrestricted_Wa rfare_Qiao_Liang_and_Wang_Xiangsui.pdf

2Maj Gen Bipin Bakshi, VSM, Information Warfare : Redefining National Security, Article in Centre for Land Warfare Studies (CLAWS) Oct 2018 Edition

3 Lt Gen DS Hooda , Retd, In Info Warfare, Common People Are Not Just Victims But Also Weapons, Article in News 18,dated January 17, 2018, available at https://www.news18.com/news/opinion/opinion-in-social-media-warfarecommon-people-are-not-just-victims-but-also-weapons-1634529.html

5 Brig Rahul K Bhonsle, Transforming to the Information Warfare Paradigm, published by Ocean Books Pvt Ltd 4/19,Asaf Ali Road, New Delhi 110002, p 7

Address to the nation by PM Modi, August 15, 2017. available at https://www.jagranjosh.com/currentaffairs/india70-pm-modis-vision-for-new-india-by-2022-the-challenges-ahead-1502952029-1

8Barry Buzan. New Patterns of Global Security in the Twenty-First Century. International Affairs (Royal Institute of International Affairs), Vol. 67, No. 3. (Jul., 1991) p. 432

United Nations Development Programme (UNDP) Human Development Report (New York Oxford University Press 1994) p 24

10 Russian National Security Strategy, December 2015 Full-text Translation issued under Presidential Edict 683 signed by President V Putin on 31 Dec 2015, accessed on 15 Apr 2018at http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy31Dec2015.pdf.

Report by MICHAL KRANZ dated Feb 14, 2018 in Business Insider, https://www.businessinsider.in/The-directorof-the-FBI-says-the-whole-of-Chinese-society-is-a-threat-to-the-US-and-Americans-must-step-up-as-a-society-todefend-themselves/articleshow/62908128.cms Qiao Liang and Wang Xiangsui, Chinese Air Force Officers,. Unrestricted Warfare. (Beijing: PLA Literature and Arts Publishing House. Feb 1999)