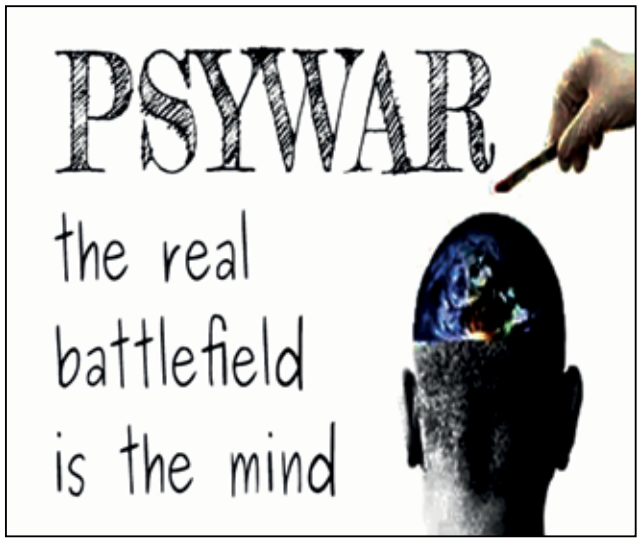
CENTRE FOR JOINT WARFARE STUDIES

SYNODOS PAPER | VOL - XII NO-23 / OCT 2018

INFORMATION WARFARE: REDEFINING NATIONAL SECURITY

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.- Qiao Liang and Wang Xiangsui, Unrestricted Warfare[1]



Introduction

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

[1]Qiao Liang and Wang Xiangsui, Chinese Air Force Officers,. Unrestricted Warfare. (Beijing: PLA Literature and Arts Publishing House. Feb 1999). Downloaded from the Internet. https://ia800201.us.archive.org/0/items/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui.pdf

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. Consequently, the need to defend one's own nation from 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.

Digital media penetration is increasing exponentially, therefore the capability to modulate public support and international opinion continues to increase. As we are aware, public pressures and international influence that impact national policies are largely guided by perceptions. The use of cyber networks in almost all aspects of daily life, transportation and financial services have opened avenues of digital manipulation. A vast number of people are being manipulated in a manner that make them the target as well as the weapon of Information Warfare. Knowingly or unknowingly their perceptions are manipulated and new age media enables them to transmit an opinion that they may not themselves have formulated or conceptualized, but they have become a cog in the wheel. We are victims of disinformation, propaganda, post-truth, fake news, or even real news cloaked in the personal conviction of the news anchor, we are also the weapon because we help create the Twitter storms without checking the veracity of the information, writes Lt Gen DS Hooda Retd[2]

> In this new battleground that is all pervasive and continuous, Information Superiority is the decisive element that determines National Security.

The National Security Construct. The capability of inimical forces to disrupt national networks of essential services and influence perceptions of key stake holders including the national and international population renders conventional concepts of National Security and the National Defence Architecture insufficient to deal with the emerging environment of conflict. The conceptual construct of National Security itself has undergone a transformation in the modern era.

It is therefore essential to redefine the concept of National Security and review the security systems in place to achieve security in the era of Information Warfare

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

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

are multifarious threats to economy and society in a complex and dynamic world order from both state and non-state actors. National security now concerns protection, preservation and furtherance of the Nation's core values in an 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 of hard 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.

Information as a Domain of Conflict. Security is a term that applies to both defensive and offensive measures in all domains, so just as military security implies the ability to ward off hostile actions as well as the capability to attack and capture enemy territory, Information Security has to be similarly seen as both defensive and offensive capabilities in the Information Domain. It is therefore clear that the connectivity and reach of the global information technology has spawned a 5th dimension of conflict in the Information Domain which involves offensive actions against the adversary's information as well as securing own information. There are several peculiarities of this battle of digital information which is permeable to inimical attacks with apparent anonymity and without evident breach of sovereignty of the target nation. Thus Information Warfare is a new domain of warfare that needs to be carefully woven into our National Security Architecture.

> The threats to cyber security and space security are expected to increase in the coming years. The growing digitalization of the financial activities and organizational processes and the race for the supremacy in space may pose serious security threats and warrant increased an allocation of financial and human resources in the coming five years.[3]
>
> ***Prime Minister Sh N Modi, Red Fort address, 15 Aug 2017***

Lead Agency for Info Warfare

Fifth Dimension Attacks could manifest on the national leadership, the social fabric of the nation, inciting communal violence, political turmoil, disrupt essential services, military surveillance, air defence, space systems and military command modules. The intensity could vary from Low - End threats : ransom ware, intelligence collection and mapping of own networks to a full blown Cyber War. It may be noted that the intentions and tools for low and high end attacks are indistinguishable, the difference is only in the scale of attack.

The response to an Info Warfare attack has to include defence as well as deterrence. While hardening of systems and repair capability will meet the defensive requirements, Offensive Capability has to be an integral part of Deterrence. The ability to inflict punitive damage on an adversary who launches a cyber attack on us has to be built in to our Info War design. The offensive capability has to include conventional attack capability, long range vectors, Special Forces, 4 GW attacks and the 5th Dimension attacks coordinated at the highest levels but executed

[3] Address to the nation by PM Modi, 15 Aug 2017. *https://www.jagranjosh.com/current-affairs/india70-pm-modis-vision-for-new-india-by-2022-the-challenges-ahead-1502952029-1*

by the military forces on the external enemy. In addition to the kinetic and non kinetic military attacks we can generate, we will need to incorporate economic and diplomatic measures into the military measures as a part of the national response. The escalation matrix would be rapid and seamless hence transfer of lead from MHA or MeitY to MoD in between the conflict will not be possible. It is therefore evident that MoD will have to take the lead in the Info Warfare structure for an effective counter strategy to be put in place.

The attempt to install a pure civilian detection and response for low end threats to be transferred to military for high end threat hence will be a fragmented approach that will prove sub- optimal in conflict. It is not a case of robbers being tackled by local police and terrorists with different forces. The same threat could be stealing, hacking or disrupting a national network, hence there is a need for a unified response system involving the military at all levels of the Info War. An analysis of the nature of the battle will reveal the structures needed and the capabilities to be integrated to wage the Info War. The threat is primarily external hence it is primarily a military mandate to respond within the overall arsenal available to the nation.

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 hostile[4].

The concepts of National Security are well defined in the **Russian National Security Strategy, December 2015**[5] which states that. National security includes the country's defense and all types of security envisioned by the Russian Federation Constitution and Russian Federation legislation. These have been further amplified and listed out in the document as under :-

State Security	Public Security
Informational Security	Environmental Security
Economic Security	Transportation Security
Energy Security	Individual Security.

Components of Security- Russan National Security Strategy

The emphasis placed on Informational Security by the Russians as far back as 2015 should be viewed in the context of the recent revelations of a possible Russian hand in the US Presidential Elections 2016. In a recent

decree signed by the Russian President[6], the Federal Guards have been charged with implementing "information warfare measures, detections, warnings and consequence management of computer attacks on Russian information resources."

---

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

[5]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 2018 at http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf..

[6] The Moscow Times News NEWS article dated Feb. 27 2018 "Putin Expands Power of Russia's Federal Guards to 'Information Warfare" accessed on 20 August 2018 at https://themoscowtimes.com/news/putin-expands-power-russias-federal-guards-information-warfare-60644

In a recent testimony before the Senate Intelligence Committee in February 2018, FBI Director Christopher Wray described information warfare as a whole-of-society problem that demanded a whole-of-society response[7]. Speaking before the Committee alongside the heads of other US intelligence agencies, Wray told Senators that China is using a host of methods to undermine American military, economic, cultural, and informational power across the globe that rely on more than just China's state institutions. Wray pointed to China's use of unconventional intelligence sources at US universities as a salient example of China's reach. He went on to specify that university students, researchers and members of the Confucius Institutes that the Chinese have across the globe serve as intelligence sources as well as projection points of Chinese soft power. All these are elements of Information Warfare(IW) that is used to undermine an adversary's capabilities and manipulate foreign societies without the use of kinetic force.

The nature of Information Warfare is all-encompassing and unrestricted in time space and scope as exemplified by the two famous Chinese Army Colonels in 1999[8]. The erstwhile rules of war, Geneva Conventions and other protocols no longer apply in this new domain of warfare.

International Law and its relevance to IW. International conventions and the UNO no longer use the term "WAR", and most nations are signatories to what are termed as the "LAWS OF ARMED CONFLICT" (LOAC). These laws are a 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 "armed force" and hence are difficult to apply to the Information Warfare 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 in a military attack and hence may not invoke measures under the LOAC. Under these circumstances, we cannot expect any international support in thwarting the Information Warfare attacks which we face, and therefore need to formulate our own responses as an intrinsic part of our National Security.

In the light of the above overwhelming evidence of the use of Information Warfare by both state and non- state actors, we need to review the components of National Security in the digital era correctly. If we have to respond to this very potent threat we must include Information Warfare in our conceptualization of National Security and thereon adapt our National Security Structures accordingly.

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

[7] Report by MICHAL KRANZ dated 14 FEB 2018 in Business Insider, https://www.businessinsider.in/The-director-of-the-FBI-says-the-whole-of-Chinese-society-is-a-threat-to-the-US-and-Americans-must-step-up-as-a-society-to-defend-themselves/articleshow/62908128.cms

[8] Qiao Liang and Wang Xiangsui, Chinese Air Force Officers,. Unrestricted Warfare. (Beijing: PLA Literature and Arts Publishing House. Feb 1999

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[9]. However, with the dark shadows of the cold war receding, one can now see that many conflicts are within nations rather than between nations[10]. The list of threats to human security is long, but most can be considered under seven main categories:-

• Economic security	• Food security
• Health security	• Environmental security
• Community security	• Political security.
• Personal security	

Threats to human security : UNDP Report on Human Development

Explanation of Personal Security. The UN report further goes on to amplify the nature of threats to personal security that loom large today. Human life is increasingly threatened by sudden, unpredictable violence that could take the following forms[11]:-

- Threats from the state (physical torture)
- Threats from other states (war)
- Threats from other groups of people (ethnic tension)
- Threats from individuals or gangs against other individuals or gangs (crime, street violence)
- Threats directed against women (rape, domestic violence)
- Threats directed at children based on their vulnerability and dependence
- Threats to self (suicide, drug use).

[9]HUMAN DEVELOPMENT REPORT of United Nations Development Programme (UNDP) New York Oxford University Press 1994 Pp 22

[10]UNDP Human Development Report op cit pp 22

[11]Op cit pp 30

Having seen some of the concepts related to Human Security and the enlarged scope of National Security in the new millennium, we need to analyse the components in the light of the changing threats generated by Information Warfare. We will look at some more views and writings on this subject by prominent experts in the field

Rajesh Basrur in his book ***"Security in the New Millennium"***[12] examines in great detail the context of security for a common citizen in the modern environment with particular reference to the specific issues confronting South Asian Nations. His analysis clearly shows how security today is viewed very differently from earlier times in the context of the changing environment and the rising aspirations of the people for an improved **Quality of Life**. He has described how ordinary people still depend primarily on the state for their security and that they depend on the state to :-

- *Secure them from **foreign military threats** by means of defence preparedness, if necessary with external assistance*
- *Carry out **appropriate economic policies** that maximize their material well being by shaping the domestic economy and by regulating the interaction between the domestic and the global economies.*
- *Manage the **environment** by means of domestic and interstate regulation;*
- *Protect and promote their **cultural identity** by regulating the linkages between the national community and the rest of the world; and*
- *Conserve and advance their **political identity and freedoms** by creating a firmly founded democratic political community that guarantees human rights*.

[12]Basrur, Rajesh, Security in the New Millennium, Regional Centre for Strategic Studies, Colombo, India Research Press New Delhi – 2001, pp 168-169

Defining of National Security Components

The components of National Security discussed above need to be reviewed in the context of the emerging Information Warfare threats and opportunities. We shall consider some of 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, to arrive at a comprehensive picture of National Security Components in the modern era.

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.

Political and Cultural Security in the Digital Era. Sovereignity and Independence of a nation need to be secured to retain cultural identity and sustain a stable democratic government. A critical issue here is the disruptive effect of globalised media connectivity and powerful transnational flows mentioned by Rajesh Basrur which challenge traditional cultures and social structures. The fissiparous tendencies emerging from this expanded connectivity have to be balanced against the economic advantages of the new age communications. The same speed that has helped unify the world has also brought many problems to our doorsteps with devastating suddenness. Drug dealers can launder money rapidly through many countries-in a fraction of the time it takes their victims to detoxify. And terrorists operating from a remote safe haven can destroy life on a distant continent and exacerbate ethnic divisions to create unrest in any part of the world.. Ensuring Political and Cultural Security therefore requires a robust Information Security capability of the Nation.

Redefining National Security. Having studied the changing security scenario and the various components of security it emerges that none of the elements of security can be achieved if we do not have Information Warfare Capabilities in the present context. In a recent development the US Army has given a major impetus to its cyber branch, giving it combat status akin to fighting formations like infantry[13] which indicates the importance of IW in the modern era and that developing both offensive and defensive IW capabilities is essential for us to win future conflicts. We therefore propose to include Information Security as an essential component of National Security. The other components as postulated by the National Defence College, New Delhi are retained with the exception of Food Security which is replaced by Economic Security.

[13]Article dated 10 December 2017 in Defence News, https://go.newsfusion.com/defense-news/item/5214183

Suggested Components of National Security	Components of National Security as per National Defence College, Delhi
➢ Military Security . ➢ Political Security. ➢ Community Security . ➢ Information Security. ➢ Energy Security.w ➢ Economic Security. ➢ Personal Security ➢ Environment Security. ➢ Health Security	❖ Military Security ❖ Political Security ❖ Community Security ❖ Personal Security ❖ Energy Security ❖ Food Security ❖ Environmental Security ❖ Health Security

Conclusion

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. We need to have a holistic understanding of Information Warfare along with a stated and declared policy, strategy and suitable structures to undertake info warfare campaigns in support of our National Interests. Including IW as an essential part of National Security is the first step towards waging the war in infospace, the Fifth Dimension of Warfare.

Major General Bipin Bakshi, VSM is a Paratrooper Engineer Officer who has commanded an Infantry Division on the Western Border, an Infantry Brigade on the Northern Border and a unit in the Kargil Sector. Presently in the NSG as the IG Training.