AMOGHVARTA

ISSN : 2583-3189

Hard Reality of Soft Power : Information Warfare

ORIGINAL ARTICLE

Authors
V. Vishal
Research Scholar
Defence & Strategic Studies Department
Jiwaji University
Gwalior, Madhya Pradesh, INDIA

&

Dr. Girish Sharma
Guide / Professor Military Science
P. G. Department & Research Center
Govt. Science College
Gwalior, Madhya Pradesh, INDIA

Abstract

The last few decades of the 20th century saw a quantum development in methods and technologies which assisted management of information. Cutting edge technologies like the microchip, computers, miniaturisation, digital communication, satellites etc made it likely to handle great volumes of data at incredible speeds and also present processed information in formats which assisted decision making. Thus, there was an increased dependence on information infrastructure and management of information. Information infrastructure is the term used to describe the totality of inter-connected computers and networks and the essential information flowing through them. Thus, societies which placed great reliance on information systems became increasingly vulnerable to any disruption of such systems.

Key Words

Information, Technology, Management, Dimension, Warfare, Operations.

Introduction

"Those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations." *-Sun Tzu, The Art of War*

Today, with the help of the Internet, it is feasible to access information across the world. Such thorough accessibility has made it possible to assault information infrastructure and information related systems from outside the geographic boundaries of any nation. The primary perpetrator may be an individual, an organisation, a non-state actor, or a nation-state. The change has been the swiftness at which information could be handled in all phases of its processing, acquisition, coalition, synthesis, analysis, dissemination, storage and denial. This awareness of the susceptibility of information systems gave rise to the idea of information warfare. It can be executed with precision and lethality both during peace and war. Chinese military officers have written that knowledge war and information operations clearly provide a way that weaker forces can compete with stronger forces in future.

What is Information Warfare?

The concept of term "Information Warfare" is enormous. Information warfare is hostile activity concentrating against any part of the knowledge and belief systems of an adversary. Different authors of Information Warfare related publications will probably produce different definitions of what constitutes information warfare. Some will probably substitute information warfare for terms such as information operations, information-age warfare, cyberwar, network and knowledge warfare or knowledge-based warfare. In the Indian Air Force doctrine, Information Warfare is defined as, "The effective use and protection of the information infrastructure from adversaries' attack and the capability of degrading, corrupting and destroying the information infrastructure of the adversary."

Information Warfare seeks to influence the behaviour of target decision-makers or audiences through the use of information and information systems. Conversely, it also seeks to shield or defend friendly decision-makers or audiences from being unduly influenced by a target's use of information or information systems. This is no different from the exercise of the other forms of national power, be diplomatic, military or economic. In this instance the means is information, but the resulting outcome is the same. This use of information is frequently referred to as "soft-power" or "non-kinetic" as contrasted with the military use of kinetic means to physically attack a target. However, Information Warfare also covers activities to disrupt, degrade or destroy enemy information systems. This includes physical destruction. Isolating an enemy decision-maker by eliminating his ability to command and control his forces is certainly a means of influencing his behaviour. The focus of Information Warfare (IW) is on "adversary decision-makers" or "adversary decision-making processes."

Today, information is itself a weapon and target. The ability to Observe, Orient, Decide and Act (OODA) faster and more effectively than an adversary is a key part of the equation. Often times affecting the target's decision cycle is a means of influencing target behaviour. Reducing an adversary's ability to make timely and efficient decisions will degrade his use of initiative or his response to friendly military action. Action must also be taken to protect friendly information and information systems from disruption. Any network-enable force relies on these systems to maintain situational awareness and to command and control its forces. These protective actions are not planned to prevent the unrestricted flow of information vital to the organisation. They are intended to prevent a target's manipulation power of information or attacks on information systems from being effective. Information Warfare is like a mental chess game. It involve anticipating an opponent's moves to manipulate our information centers of gravity while at the same time attempting to protect our own centres of gravity.

Information Environment

All Information Warfare activities occur within the broader context of an information environment. It is the aggregate of individuals, organisations and systems that collect, process, disseminate or act on information. This environment consists of three interrelated dimensions, which continuously interact with individuals, organizations and systems. This environment recognises the critical role that information and information systems play in today's advanced societies. This environment pervades and transcends the boundaries of land, sea, air and space. Within this environment exist three conceptual dimensions namely physical, information and cognitive.

- The physical dimension is the tangible real world. It is composed of command and control systems, key decision makers and supporting infrastructure that enable individuals and organizations to create effects. It is the dimension where military operations take place within the land, sea, air and space environments. Information and communications systems exist within this dimension to enable these operations to take place.
- The information dimension is where information is created, manipulated, shared and stored. This joins the physical real world with the human consciousness of the cognitive dimension both as a source of input and to convey output.

- The cognitive realm includes the thought process of those who delivers, receive and react to or act on information. Here is where the individual processes the ascertained information in relation to a set of rules, beliefs, culture and ethos. These attributes act as a human perception to arrange the information and provide a sense of meaning. The information is evaluated and to form decisions which are communicated back through the information dimension to the physical world. It should be noted that the cognitive dimension cannot be directly attacked but must be influenced indirectly through the physical and information dimensions.

The friendly decision cycle can be made in relation to the target using these three domains. However, this will require ISR of adversary and management of own decision cycle. The actions require to execute both these activities, targeting adversary information system and protecting own information system is information operations.

- **Intelligence, Surveillance, and Reconnaissance (ISR):** ISR are those operations of sensors, assets and processing, exploitation and dissemination systems to gain information and knowledge concerning a target. The focus is strictly on target information and information systems.
- **Information Management (IM):** IM activities seek to provide the right information to the right individual at the right time in a usable form to facilitate situational understanding and decision-making. The focus is on friendly information and information systems.
- **Information Operations (IO):** The third type of activity relates to both friendly and target decision cycles. These activities are Information Operations (IO).
- Considering these three sets of activities as a whole yields Information Superiority which, when achieved, results in a degree of dominance in the information domain permitting the conduct of operations without effective opposition.

Conclusion

Information has long been a key part of human rivalry. Those with a better ability to collect, understand, control and use information have always had a considerable advantage on the battlefield. From the initial recorded battles to the most recent military operations, history is full of examples of how the right information at the right time has influenced military struggles. Now information is becoming more accessible in a digital format, and it entails increasingly powerful computational processes which allows completely new forms of military activities that will require new organizations, activities, skills and mandates. Some military theoreticians and practioners claim that information has emerged as fourth factor in addition to the three traditional operational factors. Information war is the emerging theatre. The information war has the ability to act as a force multiplier to change conventional superiority and gaining absolute information dominance. The defence establishment and the society as a whole, is moving rapidly to take benefit of the new opportunities presented by the current changes.Therefore, information must be fully considered by commanders and leaders, in every sphere, at all levels.

References

1. Deakin, Richard S (2010) *Battlespace Technologies: Network Enabled Information Dominance, Artech House Publishers,* Boston (USA), p. 243.
2. Hall, W.M. (2003) *Stray Voltage: War in the Information Age, Naval Institute Press,* Annapolis Maryland (USA) p. 97.
3. Information Operations Primer, Nov 2008, US Army War College.
4. Paul, Christopher (2008) *Information Operations: Doctrine and Practice,* Praeger Publishers, California (USA), p. 27.

5. Poduval S, (2012) *NCW: How We Think, See and Fight in The Information Age,* KW Publishers, New Delhi, p. 168.
6. Sharma, M.K. (2016) Criticality Analysis and Protection of National Critical Information Infrastructures, *Air Power Journal*, Vol. 11, Spring, p. 100.
7. Svetoka, Sanda (2016) *Social Maedia as a Tool of Hybrid Warfare,* NATO Strategic Communications Centre of Excellence, p. 17.
8. The Indian Air Force Information Warfare Doctrine, p.13.

––==00==––