SHODH SAMAGAM

ISSN : 2581-6918 (Online), 2582-1792 (PRINT)

Information Warfare : Capabilities and Operations Paradigm

V. Vishal, Research Scholar, Defence & Strategic Studies Department
Jiwaji University, Gwalior, Madhya Pradesh, INDIA
Girish Sharma, Ph.D., Research Guide, P. G. Department & Research Center, Military Science
Govt. Science College, Gwalior, Madhya Pradesh, INDIA

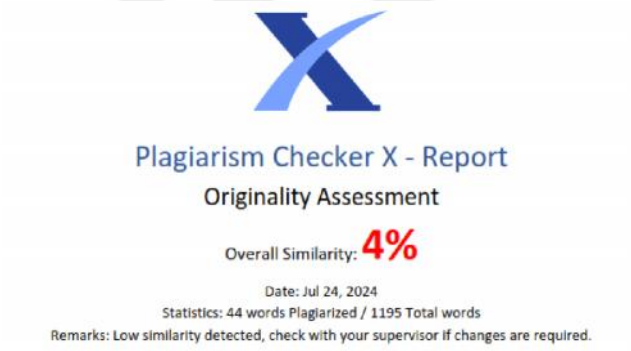
ORIGINAL ARTICLE

Authors

V. Vishal, Research Scholar
Girish Sharma, Ph.D.
E-mail : v.vaibhaw@gmail.com

shodhsamagam1@gmail.com

Received on : 31/05/2024
Revised on : 23/07/2024
Accepted on : 01/08/2024
Overall Similarity : 04% on 24/07/2024



ABSTRACT

Recently India has been victim to numerous information warfare attacks, mostly in the cyber domain due to the vulnerabilities in the active infrastructure. There have been a many incidents where sensitive Government and defence forces systems have been compromised and information has been stolen. A group called Pakistan Cyber Army hacked the Central Bureau of Investigation's website in December 2010. The same group hacked into the Bharat Sanchar Nigam Limited's website a few months later. In 2012, after the Assam violence social media was used to spread hate messages which caused the mass departure of North East people from Bangalore and other major cities in India. Such incidents have always raised fear over the security setup and defence machinery of the nation to react to new ways of fighting war in the recent times. Joint information operations by Indian forces with advanced technologies, better structures and a comprehensive doctrine can considerably reduce such incidents and result in a positive outcome.

KEY WORDS

Information Warfare, Security, Cyberspace, Psychological Operations (PsyOps), Deception, Countermeasure.

INTRODUCTION

"Successful warfare is all about and has always been all about – acquiring and exploiting information."
Richard P Hilton, Air Power Historian

On 19 Jul 2024, whole world was grappled by a problem created by one company and the operations of many international firms, Banks, and other reputed

institutions came to a grinding halt. This was due to a small software glitch by company name Crowdstrike in which provide security updates for Microsoft systems. An IT outage was witnessed by the entire world and it showcased that the capabilities of Information Warfare. Information Warfare is the cost effective solution for non-linear and exponential results. Back in 2007, Estonia, a tiny former Soviet republic, was targeted and faced new type of warfare and attacks. Some unknown bunch of techies, far away from the mainland started targeted and concentrated cyber-attack on its IT systems which caused stoppage of critical sectors such as banking and power. It continued for three days and essential systems halted. It was a perfect example of Information Warfare wherein one country made a deliberate attack on the critical systems of other country known as a Deliberate Denial of Service (DDoS). It showcased the world the effectiveness of Information Warfare. Both the above cases showcased the capabilities of Information Warfare. It is now possible to address the question of what capabilities are integrated by Information Warfare. These capabilities will be further categorised as either core, supporting or related.

Core Capabilities

These are those capabilities which are essential to the conduct of IW by providing critical operational effects or preventing the adversary from doing so. The core capabilities of Psychological Operations (PSYOP), Military Deception (MILDEC), Operations Security (OPSEC), Electronic Warfare (EW), Space Operations, Cyberspace Operations (CO) and Computer Network Operations (CNO) form the foundation for IW. While not every activity conducted within these capabilities is Information Warfare (IW), they all contribute to the achievement of IW objectives.

Psychological Operations (PSYOP)

PSYOPS are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behaviour of foreign Governments, organisations, groups and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behaviour favourable to the mission's objectives. Role of media is also essential in the PSYOPS. Every action is now scrutinised in front of live camera on a 24-hour basis. The media reporting of the 26/11 Mumbai attack is a case in point. During the Kosvo operations, in addition to protecting their tactical forces, the Serbs used deception to influence the media reporting on the conflict. Examples of such manipulation included the Serbs escorting reporters to non military targets hit by NATO aircraft but not to military targets in an effort to discredit the NATO success.

Military Deception (MILDEC)

It consists of actions executed to deliberately mislead adversary military decision makers as to own military capabilities, intentions and operations. Thus it causes the adversary to take specific actions that will contribute to the accomplishment of own mission. Deception is to limit the access and manipulate information.

Operations Security (OPSEC)

This can be defines as the identification of own or friendly information, knowledge of which can be of importance to the enemy. The measures that impact OPSEC are:

- Counter-Intelligence.
- Information Security (INFOSEC).
- Transmission Security (TRANSSEC).
- Communication Security (COMSEC).
- Signal Security(SIGSEC).

Electronic Warfare (EW)

EW is a process of using electromagnetic spectrum for own/ friendly benefit and devoid enemy of the same. The three sub-divisions within electronic warfare are as follows:

Electronic Counter Measure(ECM)

Electronic Countermeasures are the actions taken to prevent or reduce the enemy's effective use of the electromagnetic spectrum. Two major actions of ECM are jamming and deception.

Electronic Counter Counter Measure (ECCM)

ECCM is the part wherein usage of electronic warfare done to prevent own and friendly systems from effects of enemy deployment of electronic warfare that reduces the own/friendly combat capability.

Electronic Support Measure (ESM)

Electronic Support Measure is that part of electronic warfare in which actions are taken to search, intercept, locate, record and analyse electromagnetic waves, to exploit those EM waves for friendly operations.

Cyberspace Operations

Cyberspace is a world-wide sphere within the information environment. Cyberspace Operations is the usage of cyberspace with the aim to gain advantage and restrict others using the medium of cyberspace.

Space Operations

Space capabilities are a significant force multiplier when integrated with joint operations. Space capabilities have caused apparent shrinking and dissolving of boundaries, compression of time and near instantaneous insight into the happenings around the globe. Space operations support IW through the space force enhancement functions of intelligence, surveillance, and reconnaissance, missile warning, environmental monitoring, satellite communications, and space-based positioning, navigation, and timing. These core capabilities are supported by five additional or Supporting Capabilities which provide additional, though less critical, operational effects. These are Counterintelligence (CI), Combat Camera (COMCAM), Physical Attack, Physical Security, and Information Assurance (IA). Finally, three additional Related Capabilities of Public Affairs (PA), Civil-Military Operations (CMO), and Defence Support to Public Diplomacy (DSPD) contribute to the accomplishment of the IW mission. These activities often have regulatory, statutory or policy restrictions and limitations regarding their employment which must be observed.

CONCLUSION

Information has been recognised as a strategic resource which must be effectively managed to maintain a competitive and evolutionary advantage. It has critical role in reducing uncertainty, structuring complexity and generating greater situational awareness. Any action taken in the information domain can leverage tremendous effects in the physical domains of resources such as material, personnel and finance as well as more abstract domains such as belief systems. It also extends the range of new options for a planner or decision maker. The use of communications and information technologies will allow fast operations either in a region or globally. Yet although information is increasingly critical for success, all the information in the world is useless unless it contributes to effective decision making in combat. As information is becoming more and more available in a digital format, ever increasingly powerful computational processes permits completely new forms of military endeavours that will require new organisations, activities, skills and mandates.

REFERENCES

1. CBI website hacked by 'Pakistani Cyber Army'", *Times of India* 04 Dec 2010
2. Christopher, Paul (Year) Information Operations: Doctrine and Practice, Praeger Publishers Inc, USA, p. 99.
3. Crowdstrikes shuts down Worlds Windows for Hours" Times of India, 20 Jul 2024
4. Johnson, Mark (Year) USMC, Military Deception: Hiding The Real – Showing The Fake, Joint Forces Staff College, USA, p. 04.

5. Landler, Mark (2007) "Digital Fears Emerge after Data Seize in Estonia", *The New York Times*, 29 May 2007
6. Paul, Christopher (2012) *Information Operations: Doctrine and Practice,* KWPublishers Pvt Ltd, India, p. 178.
7. Poduval S, (2009) *NCW: How We Think, See and Fight in The Information Age,* Defence Department, USA, p 02.

****