

THEME: INFORMATION WARFARE IMPACTING

CONCEPT NOTE

Information about the adversary is critical and pivotal to glean the right intelligence for successful conduct of any operation. Information has been essential to wage a war irrespective of the strength of the forces one possessed since the advent of warfighting. It is hence natural that opponents have continued to compete with each other to gain an upper hand in the domain of information gathering and exploitation by setting up intelligence networks. While this was dependent on information collection by adopting multifarious means during ancient times, it has evolved to exploiting technology as well in the modern age. Since, no amount of information is ever enough or adequate, the process of gathering information and intelligence is perpetual. One, however, cannot limit to information gathering about an adversary, but has to ensure that own information is also not obtained by the adversary.

Information Warfare (IW), therefore, includes activities undertaken by one against their adversary to achieve 'information dominance' by gathering information about them while denying the adversary similar dominance. It includes activities aimed at feeding misleading information into the enemy systems to subterfuge them. Information warfare may be defined as actions taken to achieve "information superiority by adversely affecting the adversary's information, information-based processes, information systems, and computer-based networks whilst simultaneously protecting one's own information, information-based processes, information systems and computer-based networks and the psychological domain as well". However, the term remains loosely defined and some choose to define Electronic Warfare (EW), cyber warfare and psychological warfare as separate domains while others may include some or all of them under information warfare. For effective and successful operations, availability of timely and accurate information to the commanders is the key to success. It makes the Command and Control (C2) structures and processes more efficient and shortens the Observe, Orient, Decide, and Act (OODA) loop. At the same time, it provides opportunities to strike Command, Control, Communication, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) structures and processes of the adversary.





THEME: INFORMATION WARFARE IMPACTING JOINT WARFIGHTING

CONCEPT NOTE

Information Warfare is not a new process and has been practised since ancient times and so has been the component of misinformation to deceive or confuse the opponent. An example of it is found in the Mahabharat wherein, during the battle of Kurukshetra, Yudhishtir announced the death of Ashwatthama, the elephant, misleading Drona to believe that it was his son. This stopped the carnage of Drona and enabled the Pandavas to bring him down. Using IW, nations have been resorting to information warfare to gather information about the adversaries, protecting their own information and information systems, for executing military operations, for propaganda in other nations, spreading narratives to justify their own actions and inaction within and outside their countries, interfering in election processes of other nations, affecting regime changes and more. It is a powerful tool that can be used to achieve desired effects and objectives even without bloodshed or by violent action most of the times.

With continuous advancements in technology, the process of information gathering has also been evolving. The multiple types of sensors and their employment on various kinds of platforms (surface, sub-surface, air and space) has left virtually no area on the Earth hidden to humans. The information gathered also feeds the kinetic tools of war such as precision weapon systems. The tools of cyberwarfare can attack a nation's infrastructure without warning and trace, collapsing critical services that can shake the entire country including its economy. Social media engineering can play havoc with the democratic processes of countries and shape an entire population's opinion in the desired way. Technology has not only invented newer methods of executing information warfare but has also made it more dangerous and pervasive. It has brought a sea change in the concepts of warfighting and assists the practitioners in shaping the battle space in all domains of warfare. With the national infrastructures and military organisations becoming more and more technology driven and interconnected, the danger and vulnerability to cyberattacks has also increased manifold. Information warfare has become a tool for non-state actors as well to further their ideologies, turn people in their favour, and carry out planning and execution of offensive activities as well.

The tools of information warfare are used by various organs of the government towards achievement of common national goals and aims. In the age of integrated armed forces where operations are conducted jointly, the components of information warfare are also to be exercised in a manner that enhances the efficiency and efficacy of the operations towards achievement of the national objectives. Like military operations, which require synergistic application of force by synchronised use of assets of the services, information operations too need to be conducted synergistically to cover the entire ambit of activities required to achieve the desired outcome. The shaping of the battlefield is also a function executed in the information domain to soften the target psychologically. The transformation of a joint force towards integrated cross-domain operational capabilities is intrinsically enabled by the information domain. Therefore, information systems need to achieve convergence at tactical, operational, and strategic levels. A joint force's objective to achieve information dominance in multi-domain operations will ask for the utilisation of



THEME: INFORMATION WARFARE IMPACTING JOINT WARFIGHTING

CONCEPT NOTE

complex new approaches and tools in information warfare as part of a wider ecosystem of information resources and information power. Information warfare conducted by a joint force will need to be coordinated more closely with partners, for example, mounting deception and cyber operations and indeed even with fake news and propaganda campaigns.

Information Warfare is vital to a joint force's operational and C2 effectiveness, particularly in a combat cloud-enabled environment. The deployment and employment of military power in the future will require the joint force's planners and operators to be more situationally aware, more collaborative and more dependent on partners in the information environment if they are to go beyond traditional 'in house' approaches and generate the optimum solutions for IW effects.

It is to this effect that CENJOWS invites papers for the next edition of its Synergy journal covering subjects, though not limited to the following aspects with special focus on joint warfighting:-

- · Information Warfare: A Historical Perspective.
- · Impact of Technology on Information Warfare.
- Recommended Joint Information Warfare Structure for Indian Armed Forces.
- Information Warfare through electronic warfare.
- IW through Psychological Operations.
- IW through Cyber.
- IW through Military Deception.
- · IW through Operational security.
- IW for Defence.
- · IW for Offense.
- IW for Exploitation.
- $\bullet \;\;$ Information Warfare and the Changing Face of War.
- $\bullet \quad \hbox{Cyber-Enabled Information Warfare and Information Operations}.$
- Challenges for India due to IW onslaught by China.
- $\bullet\,\,$ Challenges for India due to IW on slaught by Pakistan.
- IW in Russia-Ukraine War: Lessons for India.
- · Future of information warfare in an AI-powered world.
- · Disinformation as an IW tactics.
- · Perception management.



THEME: INFORMATION WARFARE IMPACTING
JOINT WARFIGHTING

CONCEPT NOTE

- Ethical, Political, Legal and Social Issues relating to Information Warfare/Operations
- · Information Warfare Techniques.
- Role of cyber operations in IW
- · IW and its impact on National Security.
- · Philosophical perspective of IW.
- · How IW has shaped wars A historical perspective.
- · Information Warfare: Hype Or Reality? .
- · IW in modern political theory

GUIDELINES

- ➤ Research papers of 3000-4000 words, Font Size 12, Font Style Arial, 1.5 Spacing and Chicago Style Referencing is mandatory for review. A short abstract of 200-250 words must be submitted with the paper.
- > Refer to: Guideline for Contributors and Write for Us
- >Appropriate Honorarium will be paid for articles selected for publications after peer review.
- \succ Deduction of INR 500 if repetitive AI and Plagiarism check has been done by CENJOWS.
- \succ 12 to 15 papers for the SYNERGY Issue will be printed and other selected papers will be published on the CENJOWS Website.
- ➤ MI or Equivalent Clearance submission is mandatory for serving Officers of the Indian Armed Forces.
- \succ Though the last date of article submission is 30 September 2024, earlier submission will be appreciated.
- \succ Prospective contributors are requested to seek further details and submit their papers to:

Email: cenjows@cenjows.in
Contact: Dr Ulupi Borah
Senior Fellow, CENJOWS
9599316101