CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 191 September 2019

The Importance of Information and Time in Strategy

Nikita Kohli is a former Research Assistant at the Centre for Land Warfare Studies (CLAWS). Her primary focus of research was terrorism.

Introduction

War and warfare are undergoing a major change. Concepts, weapons, the nature of adversaries have changed considerably since the end of the Second World War, when these terms and ideas had clear, defined attributes. With the growing centrality of technology, information, backed by the absolute salience of the cyber domain, there are a number of "bumper-sticker" terms that are being used in various military circles. Fifth generation warfare, algorithmic warfare, hybrid war, grey-zone war—the list goes on. While defining these terms and concepts, especially those which pertain to warfighting remains important, the reality is that "much of the debate over future force structure, command and control, and strategy writ large is littered with unexplored assumptions and muddled thinking, often cloaked in buzzwords that members of an organization become obligated to use once their leadership has adopted and promulgated them as guidance."[1]

Key Points

1. Information in warfare differs significantly from information warfare (IW), with the latter focusing on the confidentiality, integrity, and availability of information, as well as confidence that the information has not been tampered with.
2. IW consists of offensive, defensive, and influence operations across the three domains of cyber, electromagnetic, and psychological operations. IW is focused more on the Tactical Battle Area (TBA), whereas Information Operations (IO) is larger in scope and focuses on the whole-of-nation approach.
3. IW is not limited by the use of special technologies, or by the idea of slowing down the enemy's OODA loop. While this forms a part of it, these two aspects remain epiphenomenal correlates. It is the information itself, as well as the timing which remain most important—you win by knowing when to give out, when to keep it and when to extract it from your adversary.

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent think-tank dealing with national security and conceptual aspects of land warfare, including conventional and sub-conventional conflict and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

CLAWS Vision: To establish as a leading Centre of Excellence, Research and Studies on Military Strategy & Doctrine, Land Warfare, Regional & National Security, Military Technology and Human Resource

Website: www.claws.in Contact us: landwarfare@gmail.com

The Importance of Information ...

But when you are talking about warfare—the conduct of which would certainly have a large and direct impact on a large section of humanity—you need to have clear concepts and understanding of the terms being used. In the present scenario, one of the most oft-used concepts is information warfare. Despite its importance and growing centrality, there remains little consensus as to what it means and what it doesn't. While not exploring the full depths of the topic, this paper dissects and analyses the meaning of information warfare, information in warfare, and elaborates as to the reasons why information and time are two of the most crucial factors in modern-day warfare.

Information in Warfare and Information Warfare (IW)

Information warfare in recent past has become one of the fixtures in all strategic thinking, discussions, and forums. The centrality of information in warfare as well as of information warfare is not without reason. Information in warfare refers to the use of particular information about yourself and the adversary, especially as they relate to the way the adversary thinks, strategises, places troops in different locations, places reserves, and most importantly, about how they think what they know about you and your information. Information warfare refers to the use and manipulation of data—raw data or information. It is, in essence, the fight over keeping your data clear, dependable, confidential, and updated, while making sure that the enemy does not have access to it. It also means that you want access to the clear, confidential data of your adversary or allow them access to your manipulated data in a manner such that what they think they know is true is actually false, and what they think they know to be false is actually true.

The complicated nature of information in warfare as well as information warfare has confounded many. While the centrality of information can be ascertained by many, the planning for and conducting of information warfare has consequently not been discussed in detail. Different facets of it—data breaches, meddling in national elections, putting malware in another country's grid—are all being talked about separately. Consequently, talking about information warfare has become the case of blind men feeling different parts of the elephant and describing it differently!

Information warfare, put simply, is the warfare over information. In this, "the confidentiality, integrity and availability (CIA) of information are three of the cornerstones of information assurance, but there is a fourth factor to consider in information operations as well. That fourth factor is confidence."[2] It is not about meaning of information. That is, IW pertains to the war between adversaries over access, use of, and confidentiality of information available with them. Its aim is certainly to affect the meaning of the information available with a state. It is about questions being raised with regard to knowing the truth and believing what you see, know, and hear to be true are actually true. This is achieved by three kinds of operations: offensive, defensive, and influence operations.

The three types of operations are expected to work in tandem across three domains: cyber, electromagnetic, and the psychological. The collective impact of conducting offensive attacks, say the shutting down of a country's electrical grid and messing with its financial and military networks, defensive attacks, including maintaining cybersecurity of essential networks, low electrical emission in the tactical battle area (TBA), and influence operations, where you focus on the mind of your soldiers, the domestic population *and* the international perception in your favour—together comprises Information Warfare.

Due to the complexity of the concept, added on to by the involvement of various areas and issues such as electromagnetic warfare and cyber narrative dominance, the concept of IW has lent itself into various sub-fields and buzz-terms. One particular buzz-phrase is of slightly more importance. This is—"Information Warfare is primarily about slowing down of your enemy's OODA loop and using advanced technology to overpower the adversary." While this phrase is not entirely incorrect, it is not absolutely true either.

Looking first to the aspect of slowing down of the enemy's OODA loop, we see a resurgence of a time-old concept being revived to explain something that has, quite frankly, little to do with the modern-day concept of information warfare. The OODA loop stands for Observe-Orient-Decide-Act loop, and was developed by John Boyd (US Air Force) to express an approach to tactical engagement, which was later expanded to incorporate broad strategic action.[3] While certainly expressing an important aspect of military decision making, especially as it pertains to air-to-air battles, the concept of OODA loop should not carry much weight in discussions pertaining to modern-day information warfare.

As discussed above, information warfare has to do with the use of and manipulation of data in a manner that helps you in your decision making at the tactical and strategic levels, while denying the enemy the same advantage. In certain cases, it can mean creating and giving false information to the enemy in a manner that would lead them into a trap. Inessence—deception. Despite such functions of deceptions being regularly carried out by militaries worldwide—especially with regard to movement and placement of troops and reserves, details of ammunition holds and nuclear stockpile, to more simple facets of manoeuvre and maintaining strategic autonomy—it is often being ignored while discussing information warfare. In such situations when militaries develop and use techniques of deception, it becomes paramount that the adversary believe that such information is true. It is only when they believe that the information that they have is true, uncorrupted, and bankable, would they then engage in those areas. Therefore, in such situations, your aim is to hasten or fasten up your enemy's OODA loop, ensuring that they believe in having a small window to exploit the situation—thereby falling for the deception laid out for them by you. In other similar situations (think deception based on infiltration), it may very well be important to ensure that the enemy does not have or use the concept of OODA loop at all! Clearly, IW is not solely about slowing down your enemy's OODA loop.

A similar case is that of technology exploitation being one of the central focuses for information warfare. Such an understanding is based on two areas: cyberspace and electromagnetic spectrum. While IW extensively uses both these sectors, it is not restricted to it. The proponents of cyberspace centrality are looking at the increasing use of the domain for exploitation of data and breaches, as well as to the cyberattacks which are being carried out by both state and non-state actors with complete impunity. The anonymity guaranteed by cyberspace has certainly made it a favourite for many disruptive actors, and is consequently being used extensively in conducting information warfare operations—offensive, defensive and influence. A similar case can be made for electromagnetic spectrum warfare (EW). EW is a field, which despite being extremely technical, has found many proponents. EW is based on the control and manipulation of the electromagnetic spectrum—something that all cyber operations, radars and radio transmissions rely on. With militaries the world over relying on the electromagnetic spectrum, electronic attack measures such as jamming, deceiving, chaffing, radar reflection and other stealth techniques have gained importance in inter-state warfare. Other measures such as electronic support and electronic protection measures, which are designed to protect your own equipment from being meddled with, while providing information and "listening in" devices are necessary in any TBA. As can be imagined, EW too has been thought of as one of the most important areas of IW.

As in the case of the OODA loop, Cyber Warfare and Electronic Warfare are important components of Information Warfare. But they are not central to it. To assume that the central focus of information operation should and does lie in cyberspace operation or EW betrays the importance of human intelligence and psychological operations. Technology and technological exploitation make an important part of IW, but are not the essence of it.

Importance of Time in Strategy

The essence of any military operation is time. This remains true even for information warfare—be it offensive, defensive, or influence operations. In the military classic, *A Book of Five Rings,* Musashi notes, "From the outset you must know the applicable timing and the inapplicable timing, and from among the large and small things and the fast and slow timings find the relevant timing, first seeing the distance timing and the background timing. This is the main thing in strategy."[4]

In the context of information warfare as well, timing is the most important. In this strange battlefield of IW that stretches from physical area to the fourth dimension of electromagnetic spectrum to influencing the minds of people over the cyber and physiological domains (TV adverts, news, etc.)—you win by knowing when to give out information, when to keep it and when to extract it from your adversary. Put another way, you need to know the timing of advance of your enemy, its location of forward troops as well as of reserves, its plans and its order of battle (ORBAT). Simply knowing your enemy's area of influence and area of interest is of little use unless you know how they are going to gain access to it, and more particularly, when they are going to gain access to it. Knowing your enemy's timing by exploitation over cyberspace as well as electronic communication and non-communication relays, you can effectively plan your strategy—your timing.

Think about it this way—you have the most perfect cyberweapon ready. This cyberweapon can gain access to information, it can change your information stored or your documents in subtle yet significant manner, and it can even destroy the system—and never be found. The dream cyberweapon. But if you use it in the first place in a manner that can destroy the entire system of computers linked to it, would you have achieved your goal? Would you have sufficiently altered the course of events being planned by your adversary—when you did not get the full details? Could you have simply changed and confused them by making subtle changes in a manner that they can no longer trust their command and control? Does destroying the enemy computer system solve everything?

Conclusion

In information warfare, the fight is over the credibility, integrity, confidentiality, and access to information. IW is not about destroying information or even about *meaning* of information—the latter is narrative warfare. IW is therefore not concerned with slowing down the enemy's OODA loop or about exploiting technology in a more efficient way. It is war over information—raw data. This raw data is important for two reasons. One, the missing information must matter. That is, an actor would change its course of action if it had access to the missing information. Second, when there is incomplete and asymmetrical information available with one actor, they must have the incentive to misinterpret it or lie about it. Otherwise, you could have simply told your adversary what you know.

Information warfare is about gaining access to the information available with the adversary while protecting your own. It is bigger than information in warfare. It is, at its core, about timing—the timing of the use of that information. In the new battlespace which is undefined, IW done properly allows you to anticipate your opponent's moves and devise countermeasures. With more information, that is, raw data, you, that is, the winner, can plan one step ahead of the opposition, and show your winning hand after them. It is about making sure that you surprise them, and that they don't surprise you.

Notes

1. Dave 'Sugar' Lyle, "Fifth Generation Warfare and Other Myths: Clarifying Muddled Thinking in Our Current Defense Debates," *Over the Horizon*, December 4, 2017.
2. Patrick D. Allen, *Information Operations Planning*, Artech House, 2007, p. 4.
3. For a great in-depth analysis of Boyd's OODA loop, see Clay Chun and Jacqeline E. Whitt's piece, "John Boyd and the OODA loop," *War Room*, US Army War College, January 8, 2019; at https://warroom.armywarcollege.edu/special-series/great-strategists/boyd-ooda-loop-great-strategists/
4. Miyamoto Musashi, *A Book of Five Rings*, translated by Victor Harris, The Overlook Press, 1974, p. 48.

The contents of this Issue Brief are based on the analysis of material accessed from open sources and are the personal views of the author. It may not be quoted as representing the views or policy of the Government of India or Integrated Headquarters of MoD (Army).

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Tel.: +91-11-25691308, Fax: +91-11-25692347, Email: landwarfare@gmail.com
Website: www.claws.in
CLAWS Army No. 33098