172-184

THE FATAL TROUBLE OF INTANGIBLE SCUFFLE: INFORMATION WARFARE IMPACTING JOINT WAR FIGHTING

Lt Varun Bajiya

Abstract

The paper makes an effort to develop an understanding and renewed perspective about the role and implications of Information, in the changing nape of conflicts, which is Information Warfare (IW) and Information Operations (IO). It achieves this through empirical analysis of historical and contemporary conflicts, pertaining to diplomacy, military, as well as intelligence. The paper also argues that there is a necessity for revision in the Indian defence organisational structure, engagement doctrines and culture, aimed at giving birth to a new paradigm of jointness, wherein not only governmental components and tri-services, but inter alia even the private sector is incorporated.

INTRODUCTION

IW and IO are commonly misconceived to be a sixth-generation warfare facet. However, information being used as a non-kinetic means of warfare has its origins dating back to historical conflicts.

Traces of IW dates back to 18th century, wherein pioneers such as Frederick-II, the monarch of Prussia, probed travellers from variegated nation-states for information pertaining to strategic culture, tactics, armaments, and battle plans used by their enemies.[1] This would facilitate them in profiling generals and emperors of such inimical states.[2] The veracity of such information was compounded by a meticulous web of

Prussian spies carefully planted into such nations.[3] However, it was soon realised that information, which acted as a 'force multiplier', had another side to it. Despite earnest endeavours to limit damage from subterfuge, vulnerability of information from being exaggerated and erroneous could not be ruled out. This scepticism was also harboured by Carl von Clausewitz in his academic texts.[4]

As stated above, IW is not novel and has been practised since ancient times. So have been the components of 'misinformation', which was targeted to deceive or confuse the opponent. An example of it is found in the excerpts from early texts, such as Kautilya's Arthashastra, which shows traces of principles being implemented in today's hybrid warfare. Spies were tasked to find out and report the rumours circulating among the people of enemy state, and those vulnerable to subversion within the enemy state were to be won over by conciliation and gifts. Those who were not prone to subversion were to be subjected to use of force. Furthermore, aids and counsels to the king within one's own nation-state were to propagate favourable sentiments for the incumbent rulers.[5] Similarly, in Mahabharata, in the battle of Kurukshetra, Yudhishtira declared the demise of Ashwatthama, an elephant. This intentional ambiguity in the information being dispersed misled Drona into believing that it was his son Ashwatthama who has died, leading to cessation of war waged by Drona, thereby enabling the Pandavas to defeat him.[6]

WORLD WAR I

Traditional narratives of World War I generally overlooked and misunderstood an important part of the conflict, that is IW. Entente powers early on recognised the importance of information as a 'force multiplier' and diplomatic tool, thereby greatly influencing the vox populi by controlling entertainment platforms such as radio, films and music. They directed the producers to portray the war positively and keep civilian spirits high.[7]

SUBTERFUGE IN WORLD WAR II

- **Fortitude North and Fortitude South**. Evolving its complexities by the advent of World War II, IW had advanced exponentially. Fearing that if the Germans obtained actionable intelligence, their overwhelming firepower and numerical superiority could defeat the Allied thrust, a complex subterfuge was engineered in the form of a fictitious Fourth Army in Edinburgh, Scotland, and fictitious First United States Army Group (FUSAG) under Fortitude North and Fortitude South, respectively. Superfluous radio traffic and decoy military assets such as inflatable tanks and fake landing crafts were used to portray preparations for an invasion at Pas de Calais.[8]

- **Operation Zeppelin**. Similarly, under Operation Zeppelin, the Germans were duped into believing that three British army components were stationed in Egypt, preparing for an invasion of Crete. Owing to this, even weeks after the Normandy landings, the German High Command continued believing that an attack was imminent in the Strait of Dover. This compelled the Germans to not only deploy their troops over several suspected landing sites but also procrastinated mobilisation of their reinforcements to Normandy. This serves as a prime example of how subterfuge under IW strayed the Germans off course by firstly convincing the German leadership that the disposition of attacking Allied components was larger than they were in reality, and secondly, by convincing them that there were multiple landing sites namely Norway and Calais in France.

- **Operation Graffham, Op Royal Flush and Op Vendetta**. The British succeeded in duping the Germans into believing that there was a likely invasion of Norway by staging communiqué with Sweden. In these communiqués, they made supplications for the right to fly, land and refuel Allied military aircrafts on Swedish territory. Additionally, they convinced the Germans that Sweden would discontinue being a neutral state by joining the Allied forces. This resulted in the Germans stationing nearly 400,000 troops in

Norway as a contingency. Similarly, Spain, a neutral nation, was portrayed through fabricated physical evidences as soon to join Allied members, in order to convince the Germans that France was under threat of an Allied invasion.[9]

WORLD WAR II AND RADIO PROPAGANDAS

- **Axis Propaganda**. In Nazi Germany, under the infamous German propaganda minster, Joseph Goebbels, German propagandists made herculean efforts to transmit almost 12 hours of propaganda a day just a few months after the outbreak of World War II. Goebbels justified radio as the 'eighth great power' and these programs delivered propaganda to occupied territories and enemy states. The objective was to weaken pro-British sentiments, germinate apprehensions, and exploit fears of conflict among British, Canadian, Australian and American troops, as well as capitalists and Jews. These targeted listeners heard selected music, virtues of Axis causes, Allied defeatist propaganda and Axis victories. The troops popularly gave epithets to the voices they heard over radio, such as 'Tokyo Rose' from Japan and those from Germany as 'Axis Sally', 'Lord Haw-Haw' and 'Home sweet Home'.

- **Allied Propaganda**. Lagging not far behind, the Americans used their 'you technique' programs to implant or psychologically transport targeted listeners into scenarios of battle or being captives in military camps by addressing them personally. IW through radio programs played a pivotal part in the war effort for both the Allied and Axis powers.[10]

- **Kargil War**. During the build-up to Kargil in 1998, the Research and Analysis Wing (R&AW) submitted to the government that Pakistan, owing to the economic regression, was not capable of engaging in conflict. However, indicators on ground by March 1999 were indicating a significant accumulation of Pakistani troops and armaments in Pakistan Occupied Kashmir. Yet, R&AW continued to maintain that engagement in full-scale conflict was impractical for Pakistan owing to their financial limitations. This

is a prime example of the significance of information being sine qua non in warfare and the mammoth failure on behalf of Indian intelligence agencies. Pakistan's multilinear engagement on a political, strategic, and tactical level took India by utter surprise. This indicated a gapping insufficiency in the system of gathering, reporting, and assessing information by Indian intelligence agencies owing to which India sought external support by turning to Israel during the Kargil War.[11]

- **Operation Enduring Freedom**. The US Army suffered a major setback when 'Strava', an application that can be used on various devices - including smartphones and fitness trackers, released a visualisation map of heat data gathered from its users in the year 2015 and November 2017. The map showed every single activity ever uploaded to Strava, including extremely sensitive information about a subset of Strava users, namely military operatives on active service. This revelation compromised their operational security by revealing the internal layout of their military bases.[12]

CHANGING NATURE OF WAR

- **From Industrial Era of Conflict to Multilinear Warfare**. The conventional interpretation of 'war' is one where physical violence or kinetic means are resorted to for establishing dominance over another nation-state. However, we are experiencing a change in the methodology of warfare, moving ahead from an 'industrial era of conflict', wherein strength in numbers and fire power dominance played an indispensable role. The transition has happened towards Multilinear Warfare, disrupting conventional understanding of conflict. Furthermore, with the advent of 21st century, there would be amalgamation of civil, military and political spheres in conflicts, which is unprecedented. 'Proxy and Hybrid Warfare', as witnessed in Yemen, are not just examples of how ideologically distinct nations such as Saudi Arabia and Iran are exploiting foreign soils for conflict, without any iota of geographical or tangible participation or kinetic military involvement.

- **Modes of Multilinear Warfare**. The aforementioned is achieved through means of disrupting economy, participating via non-state actors, instigating insurrection, financing terrorism, aiding insurgency, misinformation, cyber-attacks and most importantly for our discussion, through IW and IO. The Russia-Ukraine conflict in which the Russians initiated the offensive with cyber-attacks to disrupt internet connectivity in Ukraine and incapacitate its command & control centres, missile systems, electronic warfare (EW) systems, radar and communications systems, are alarming observations and a wakeup call for military academicians worldwide. It compels us to appreciate the ever-evolving nature of warfare with clarity, especially in the technological era, where the tactical advantage provided by technology and IW to the first mover cannot be underestimated. Today, instruments of force such as IW and advanced technology (including precision attack systems, loiter munitions, hypersonic missiles, edge and quantum computing, swarming drones etc.) are formidable challenges for military strategists, accustomed to traditional warfare concepts.

CONTEMPORARY RELEVANCE

Epiphenomenon of Low Intensity Conflicts

Since India has, for the past few decades, been engaged in low intensity conflicts (such as suppressing secessionist tendencies in Jammu & Kashmir and in the North East), its military is plagued with technological stagnation, leading to an informational disadvantage. Therefore, it is crucial to introduce structural, doctrinal and organisational adaptations within the armed forces. These include incorporating the study of Information Technology into curriculum of armed forces personnel, particularly for assessments such as the Part B examination. Increasing the presence of Information Technology platforms in defence acquisitions, investing in indigenous innovation of Disruptive Technologies, conducting training exercises involving Non-Kinetic Military Participation, executing intelligence based offensive actions, and deploying lethal autonomous weapons in regions affected by

hybrid warfare (such as Union Territory of Jammu & Kashmir), are essential steps. Additionally, integrating AI based weapons and defence systems should be a priority. Economic and Information Technology hubs or agglomerations, modelled after initiatives like GIFT (Gujarat International Finance Tec-City) should be established for defence sector. These hubs should focus on research, innovation, academia, applied tests and manufacturing. Such economic hubs would ensure flawless supply connectivity, technology spill over, common research facilities, an improved technical skill pool, readily available capital, special purpose vehicles, customised policy making and tax relaxations. In other words, this would incentivise domestic (both private and public) entities, as well as international entities, to enter the market of defence research, innovation and production market. This shall be tantamount to being the genesis of a new paradigm of 'jointness', wherein not only governmental components and tri-services, but inter alia even the private sector are integrated. The Uttar Pradesh Defence Industrial Corridor (UPDIC) and the Tamil Nadu Defence Industrial Corridor (TNDIC) are steps towards this objective. This would enable us to be self-sufficient rather than being interdependent on technology transfers with countries such as Israel, France and China which in turn makes us vulnerable to IW. However, for any of the aforementioned to be materialise, it is imperative that gross expenditure on defence sector be increased incrementally, followed by equitable distribution of resources across tri-services, academia, research & development, industry & businesses and the government enterprises.[13]

QUANDARY AT ADOPTING INFORMATION TECHNOLOGY

As of today, the Indian Army finds itself in a conundrum. On one hand, it is restricting the use of emerging technologies, information technology and cyber tools to limit the vulnerability to weaponised offensive cyber interference and IW by adversaries or non-state actors. On the other hand, with the seismic shift in paradigm of armed conflicts by information and technological revolution, the Army is also desperate to incorporate technology into their routine operations, training institutions, and organisational reforms. Therefore, it is essential that defence

organisational structure, engagement doctrines and culture be revised. Simultaneously, we must dedicate resources towards establishing an equilibrium between maintaining security and embracing technological evolution.

ONGOING INITIATIVES

The Indian Army has shown dedicated efforts towards transformation and upgradation into a modernised army by dedicating 2023 and 2024 as the 'Year of Transformation'. Gargantuan changes are underway, including:

- **Maritime Capability Perspective and Indian Naval Indigenisation Plan**. The Indian Navy is incorporating state-of-the-art maritime defence technology and augmenting indigenous innovation to their infrastructure. In furtherance of this, the Innovation and Indigenisation Organisation, in general, and the Technology Development Acceleration Cell of the Indian Navy, in particular, are in process of recognising innovation industry partners, incorporating advanced technology through the private sector, encouraging indigenous innovation, and facilitating participation from academia.[14] These are prime examples of new paradigm of 'jointness', where not only governmental components and tri-services but also the private sectors are being incorporated to a great extent.
- **Drones**. The seamless incorporation of precision & swarming drones, as well as counter-drone systems, within present structures.
- **Policy Changes**. Policies now permit Lt Col specialising in Artificial Intelligence, automation, mechanisation, information technology etc., to continue in their respective fields even upon being promoted to the rank of Col.
- **Dedicated Corpus Facilitating Indigenous Production**. In the Union Budget for 2020-21, Rs 8,000 crores were dedicated under National Mission on Quantum Technologies & Applications

(NM-QTA).[15] Indigenous development includes weapon systems such as ASMI and the remodelling of the INSAS rifle into a bullpup configuration, the development of an electronic warfare system for all three services by DRDO and proposed production of air droppable gun tower, counter IED mechanised system, electromagnetic weapon system for avionics, RADARS, drones and next generation mine grid.

- **Command Cyber Operations Support Wing.** This wing intended to augment Indian Army's information and cyber capabilities, moulding specialised officers, including cyber experts, through civil and military collaboration.

INDIAN ARMY AND RECOMMENDED JOINT IW AND IO STRUCTURE

- **Changing Nature of Warfare**. With ever-increasing geopolitical instability and the rising number of hybrid warfare scenarios across the globe, it is essential that India, as a nation state, equips itself not just for today, but tomorrow's IO and IW. Ongoing conflicts in the Middle East, Korean Peninsula, West Asia, China-Taiwan and Russia-Ukraine war clearly demonstrate that wars can no longer be interpreted through a conventional lens. Observing, recognising, deliberating on, and acting upon the changing nature of warfare warrants a major overhaul in the defence policy, strategy and infrastructure.

- **Joint Operations**. To achieve this, the understanding of joint operations must be expanded beyond the scope of the tri-services and traditional interpretations. A conscious thrust towards amalgamating not just the defence, but non-defence organisations and even the private sector needs to be systematically planned. Currently, the tri-services are constrained by their parochial focus on capitalising on the 'Human Centric Operational Edge' rather than relying on informational & technological facets. Our interpretation of IO and IW is limited to the defence sector, which is deeply flawed. From a national security perspective, various components of the government and private sector are equally crucial.[16]

MEANS AND OBJECTIVES OF IW

Novel Means

Due to the novel means of IO and IW, such as 'command and control warfare' where the enemy's functionality is disrupted to compromise their effectiveness through electronic warfare (including radars, jammers, ciphers and 'hack ware') or 'intelligence-based warfare' where technology is used to augment military operations, it has become obsolete and ineffective to rely solely on conventional defence tactics. In fact, one might already be subjected to IO and IW without even realising it, especially when subjected to 'psychological warfare' through propaganda. Worse still, individuals can be demoralised and instigated towards social disorder through 'economic information warfare', wherein financial institutions are destabilised through non-kinetic means of warfare.

MULTIDIMENSIONAL OBJECTIVES

IO and IW compound the complexity of preparing our defences against such attacks as they can have multiple objectives. These could include collecting tactical information on the enemy, ascertaining its veracity, and propagating disinformation about the inimical state in order to demoralise and manipulate the 'vox populi' against the incumbent regime (as discussed above in Mahabharata and Arthashastra). IO/ IW could also be aimed at compromising the integrity of the enemy's information data base, thereby disabling their command and control. Similarly, it could be used within one's own people through perception management (as demonstrated in radio propaganda campaigns of Axis powers).[17]

CHALLENGES FOR INDIA

India is increasingly facing the onslaught of IO and IW on different fronts.

- **Türkiye and Pakistan**. Colluding on the Kashmir issue by publishing findings bearing malo animo (ill intent), such as calling armed insurrections 'non-armed state groups' and levying allegations of human rights and international law violations against the Indian state, are prime examples of IO and IW.[18]

- **China**. Staging misinformation campaigns against India by fabricating news to discredit the government.[19] Similarly, Chinese manufactures such as Huawei and ZTE pose tremendous cyber threats, and China's compromise of INSAT-4B using the 'Stuxnet worm', are alarming concerns.[20]

WAY FORWARD

It is undeniable that IO and IW are inevitable - if they have not already metastasised to an advanced stage. Therefore, it is imperative that India deliberates upon the following aspects of IO and IW:

- **Scope.** The scope of IO and IW is strategic and geographically limitless.
- **Nature.** The nature of IO and IW is such that they are not bounded by the traditional constrains of time in terms of initiation and cessation. Rather, they are ongoing campaigns, unfettered by shackles of duration.
- **Entities.** IO and IW encapsulates non-traditional entities, including diplomatic, economic, and military components.
- **Tangible Implication of Intangible Warfare.** Lastly, and most importantly acknowledge and act upon the 'The Fatal Trouble of Intangible Scuffle'-the realisation that, though an intangible conflict, IO and IW, like conventional kinetic warfare have extreme physical and tangible implications, which might go undetected until it's too late to contain the damage.[21]

CONCLUSION

The growing importance of IO and IW is characterising today's landscape of warfare. This necessitates a significant level of shift in how the nations prepare for and engage in conflicts. Historically, it has been observed that information played a crucial role in the warfare. In terms of New Delhi, the threats posed by IO and IW are multifaceted in nature.

To address these challenges, the Indian Armed forces will have to emphasis on jointness, while incorporating the three components:

governmental, non-governmental and the private sector. Investment in technology remains one of the core mitigations along with restructuring of defence doctrines.

Furthermore, enhancing cyber resilience along with information integrity should remain the priorities of New Delhi.

Such shifts in India's policies would not only address the IO and IW threats but would position India as a leader in terms of adapting to the changing nature of warfare.

★★★

Lt Varun Bajiya is an alumnus of Officers Training Academy (OTA), Chennai. The officer got commissioned into Judge Advocate General's (JAG) branch of Indian Army in September 2023. He is currently serving his attachment with the 7th Battalion of 8th Gorkha Rifles in Srinagar.

NOTES

1 *Vanya Eftimova Bellinger, "Carl Von Clausewitz — the Bridge," The Strategy Bridge, June 12, 2023, https://thestrategybridge.org/the-bridge/tag/Carl+von+Clausewitz.*

2 *Christopher Duffy, The Army of Frederick the Great (New York: Hippocrene Books, Inc.*

3 *Ibid.*

4 *Carl Von Clausewitz, "Intelligence in War," in On War, ed. Michael Howard, trans. Peter sity Press, 1976), 117. Also refer Nathaniel D. Bastian, U.S. Government, and Nathaniel D. Bastian, "INFORMATION WARFARE AND ITS 18TH AND 19TH CENTURY ROOTS," THE CYBER DEFENSE REVIEW,season-03,2019,31–33, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Fall%202019/CDR%20V4N2-Fall%202019_BASTIAN.pdf?ver=2019-11-15-104103-203#:~:text=Some%20historians%20hold%20that%20information,of%20wireless%20and%20telephone%20communications.*

5 *Kautilya's Arthashastra: A Timeless Frand Strategy Defence Technical Information Center https://www.claws.in/espionage-in-kautilyas-arthashastra-a-case-study-of-1971-india-pakistan-war-and-intelligence/*

6 *Shyam Bhat and Shyam Bhat, "Ashwathama Is Dead - Dr Shyam Bhat," Dr Shyam Bhat - Holistic Psychiatry, Integrative Medicine, Self-Actualization, Meditation (blog), November 14, 2018, https://www.shyambhat.com/ashwathama-is-dead/.*

7 *Information Warfare (IW) in World War I1 Winkler, Jonathan Reed. The Journal of Military History; Lexington Vol. 73, Iss. 3, (Jul 2009): 845-867.*

[8] *Imperial War Museums, "D-Day's Parachuting Dummies and Inflatable Tanks," n.d., https://www.iwm.org.uk/history/d-days-parachuting-dummies-and-inflatable-tanks.*

[9] *D-day Info, "Operation Bodyguard, the Diversion Plan for D-day - D-day Info," August 2, 2021, https://d-dayinfo.org/en/preparation/operation-bodyguard/.*

[10] *"Radio Propaganda in World War II | Historical Spotlight | News | Wargaming," n.d., https://wargaming.com/en/news/radio_propaganda/.*

[11] *Roopashree Sharma, "Explained: Role of Technology and Communication in Kargil War," Jagranjosh.Com, July 26, 2024, https://www.jagranjosh.com/general-knowledge/amp/kargil-chronicles-the-role-of-technology-and-communication-in-the-kargil-war-1721480440-1.*

[12] *Alex Hern, "Fitness Tracking App Strava Gives Away Location of Secret US Army Bases," The Guardian, April 14, 2018, https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.*

[13] *Rajeswari Pillai Rajagopalan, ed, Future Warfare and Technology: Issues and Strategies, (New Delhi: ORF and Global Policy Journal, 2022) https://www.orfonline.org/research/future-warfare-and-technologies-issues-and-strategies.*

[14] *Ibid.*

[15] *Byjus's, (National Quantum Mission), URL: https://byjus.com/free-ias-prep/national-mission-on-quantum-technologies-applications-nm-qta/#:~:text=The%20NM%2DQTA%20was%20first,years%20in%20the%20Budget%202020.&text=Objective%3A%20The%20aim%20is%20to,quantum%20technology%20within%20the%20nation.*

[16] *Dan Kuehl and Institute for National Strategic Studies, "Joint Information Warfare: An Information-Age Paradigm for Jointness," STRATEGIC FORUM, vol. Number 105, March 1997, https://apps.dtic.mil/sti/tr/pdf/ADA394384.pdf.*

[17] *Saulius Griškėnas and Saulius Griškėnas, "What Is Information Warfare (IW)? With Real Examples," NordVPN,July5,2024,https://nordvpn.com/blog/information-warfare/?srsltid=AfmBOopc8fhcgxbnILHrTo8MxEo5_C_laH3BtWQXofbWeewGAFDxYC9z.*

[18] *"India's War Crimes in Kashmir: Violence, Dissent and the War on Terror," SW Investigations, 20 January, 2022, https://www.swiunit.com/post/india-s-war-crimes-in-kashmir-violence-dissent-and-the-war-on-terror.*

[19] *Pradip R. Sagar, "How China Has Unleashed a Misinformation War on India," India Today, October 18,2023https://www.indiatoday.in/amp/india-today-insight/story/how-china-has-unleashed-a-misinformation-war-on-india-2450656-2023-10-18.*

[20] *Vaasu Sharma, "Information Warfare (IW) Against India - the China Angle," WION, September 13, 2022, https://www.wionews.com/opinions-blogs/information-warfare-against-india-the-china-angle-515617/amp.*

[21] *Graham Fairclough, A Persistent Fire, Chapter 09 https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2004078/9-the-ethical-challenge-of-information-warfare-nothing-new/.*